kaspersky

Kaspersky Endpoint Detection and Response

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 3.7.0.713

kaspersky

Содержание

kaspersky

Об этом руководстве

Обозначение документа: 643.46856491.00113-01 90 01

Этот документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия Kaspersky Endpoint Detection and Response. Руководство адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Endpoint Detection and Response, а также специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Endpoint Detection and Response.

В этом руководстве вы можете найти информацию о настройке и использовании Kaspersky Endpoint Detection and Response.

Также из этого руководства вы можете узнать об источниках информации о программе и способах получения технической поддержки.

В этом разделе

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком "Пример".
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.

Пример текста	Описание условного обозначения
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком "стрелка".
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

kaspersky

Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection and Response (далее также "KEDR") – решение (далее также "программа"), предназначенное для защиты компьютеров локальной сети организации и своевременного обнаружения таких угроз, как, например, *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "*APT*"). Программа разработана для корпоративных пользователей.

Программа Kaspersky Endpoint Detection and Response является функциональным блоком решения Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform включает в себя два функциональных блока:

- KEDR, обеспечивающий защиту компьютеров локальной сети организации
- Kaspersky Anti Targeted Attack (далее также "KATA"), обеспечивающий защиту периметра IT-инфраструктуры предприятия.

KEDR лицензируется отдельно от KATA.
Для активации функциональности KEDR нужно использовать отдельный ключ.

Программа может получать и обрабатывать данные следующими способами:

- Интегрироваться с программой Kaspersky Endpoint Agent и получать данные с отдельных компьютеров, входящих в IT-инфраструктуру организации и работающих под управлением операционной системы Microsoft® Windows®. Kaspersky Endpoint Agent осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.
    - Компонент Endpoint Agent может устанавливаться на отдельные компьютеры и получать данные с этих компьютеров.
    - Kaspersky Endpoint Detection and Response может интегрироваться с программой "Лаборатории Касперского" Kaspersky Endpoint Security для Windows (далее также "KES").

      Вы можете получить подробную информацию о Kaspersky Endpoint Security для Windows из *Справки Kaspersky Endpoint Security*.
- Интегрироваться с внешними системами с помощью интерфейса REST API и проверять файлы на этих системах.

Программа использует следующие средства анализа угроз (Threat Intelligence):

- Инфраструктуру облачных служб Kaspersky Security Network (далее также "KSN"), предоставляющую доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.
- Интеграцию с программой "Лаборатории Касперского" Kaspersky Private Security Network (далее также "KPSN"), предоставляющую пользователю возможность получать доступ к репутационным базам KSN, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров.
- Интеграцию с информационной системой "Лаборатории Касперского" Kaspersky Threat Intelligence Portal, которая содержит и отображает информацию о репутации файлов и URL-адресов.
- Базу угроз "Лаборатории Касперского" Kaspersky Threats.

Программа может предоставлять пользователю результаты своей работы и анализа угроз следующими способами:

- Отображать результаты работы в веб-интерфейсе серверов Central Node, PCN или SCN.
- Интегрироваться с внешними системами с помощью интерфейса REST API и по запросу отправлять данные об обнаружениях программы во внешние системы.
- Публиковать информацию об обнаружениях компонента Sandbox в локальную репутационную базу Kaspersky Private Security Network.

Пользователи Старший сотрудник службы безопасности и Сотрудник службы безопасности могут выполнять следующие действия в программе:

- Осуществлять мониторинг работы программы.
- Просматривать таблицу обнаруженных признаков целевых атак и вторжений в IT-инфраструктуру организации, осуществлять фильтрацию и поиск обнаружений, просмотр и работу с каждым обнаружением, выполнять рекомендации по оценке и расследованию инцидентов.
- Просматривать таблицу событий, происходящих на компьютерах и серверах, входящих в IT-инфраструктуру организации, осуществлять поиск угроз, фильтрацию, просмотр и работу с каждым событием, выполнять рекомендации по оценке и расследованию инцидентов.
- Выполнять задачи на хостах с компонентом Endpoint Agent: запускать программы и останавливать процессы, скачивать и удалять файлы, помещать объекты на карантин на компьютерах с компонентом Endpoint Agent, копии файлов в Хранилище программы, а также восстанавливать файлы из карантина.
- Настраивать политики запрета запуска файлов и процессов, которые они считают небезопасными, на выбранных хостах с компонентом Endpoint Agent.
- Изолировать отдельные хосты с компонентом Endpoint Agent от сети.
- Работать с индикаторами атак Indicators of Attack (IOA) для классификации и анализа событий.
- Работать с пользовательскими правилами Targeted Attack Analyzer TAA (IOA) и YARA: загружать правила, по которым программа будет проверять события и создавать обнаружения.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах с компонентом Endpoint Agent и в базе обнаружений.
- Добавлять правила TAA (IOA), предоставленные специалистами "Лаборатории Касперского", в исключения из проверки.
- Работать с объектами на карантине и копиями объектов в Хранилище.
- Управлять отчетами о работе программы и отчетами об обнаружениях.
- Настраивать отправку уведомлений об обнаружениях и о проблемах в работе программы на адреса электронной почты пользователей.
- Работать со списком обнаружений со статусом VIP, с белым списком данных, наполнять локальную репутационную базу KPSN.

Пользователи Локальный администратор и Администратор могут выполнять следующие действия в программе:

- Настраивать параметры работы программы.
- Настраивать серверы для работы в режиме распределенного решения и multitenancy.
- Производить интеграцию программы с другими программами и системами.
- Работать с TLS-сертификатами и настраивать доверенное соединение сервера Central Node с сервером Sandbox, а также серверов программы с внешними системами.

- Управлять учетными записями пользователей программы.
- Осуществлять мониторинг работоспособности программы.

Программа обнаруживает следующие события, происходящие внутри IT-инфраструктуры организации:

- На компьютер локальной сети организации был загружен файл или была предпринята попытка загрузки файла.
- На компьютере локальной сети организации была открыта ссылка на веб-сайт.
- На компьютере локальной сети организации были запущены процессы.

Kaspersky Endpoint Detection and Response оценивает события и рекомендует пользователю обратить внимание на каждое обнаруженное событие (*обнаружение*) в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера, по опыту "Лаборатории Касперского". Пользователь Kaspersky Kaspersky Endpoint Detection and Response самостоятельно принимает решение о дальнейших действиях над обнаружениями.

О Kaspersky Threat Intelligence Portal

Для получения дополнительной информации о файлах, которые вы считаете подозрительными, вы можете перейти на веб-сайт программы "Лаборатории Касперского" Kaspersky Threat Intelligence Portal, которая анализирует каждый файл на содержание в нем вредоносного кода и отображает информацию о репутации этого файла.

Доступ к программе Kaspersky Threat Intelligence предоставляется на платной основе. Для авторизации на веб-сайте программы на вашем компьютере в хранилище сертификатов должен быть установлен сертификат доступа к программе. Кроме того, у вас должны быть имя пользователя и пароль доступа к программе.
Подробнее о программе Kaspersky Threat Intelligence Portal см. веб-сайт "Лаборатории Касперского".

kaspersky

Комплект поставки

В комплект поставки Kaspersky Endpoint Detection and Response входят следующие файлы:

1. Образ диска (файл с расширением iso) с установочными файлами операционной системы CentOS 7.7, подготовленной для развертывания компонентов Sensor, Central Node.
2. Образ диска (файл с расширением iso) с установочными файлами компонентов Sensor, Central Node.
3. Образ диска (файл с расширением iso) с установочными файлами операционной системы CentOS 7.7, подготовленной для развертывания компонента Sandbox.
4. Образ диска (файл с расширением iso) с установочными файлами компонента Sandbox.
5. Образы дисков (файлы с расширением iso) операционных систем Windows XP SP3, 64-разрядной Windows 7 и Windows 10, в которых компонент Sandbox будет запускать файлы.
6. Файл с информацией о стороннем коде, используемом в программе.
7. Комплект поставки программы Kaspersky Endpoint Agent (ранее Endpoint Sensors), в который входят следующие файлы:

Таблица 2. Комплект поставки Kaspersky Endpoint Agent

Файл	Назначение
`agent\endpointagent.msi`	Инсталляционный пакет Kaspersky Endpoint Agent.
`agent\endpointagent.kud`	Файл для создания инсталляционного пакета Kaspersky Endpoint Agent с помощью Kaspersky Security Center.
`agent\klcfginst.msi`	Инсталляционный пакет плагина управления Kaspersky Endpoint Agent для Kaspersky Security Center.
`agent\kpd.loc\en-us.ini`	Конфигурационный файл, необходимый для создания инсталляционного пакета англоязычной версии Kaspersky Endpoint Agent с помощью Kaspersky Security Center.
`agent\kpd.loc\ru-ru.ini`	Конфигурационный файл, необходимый для создания инсталляционного пакета русскоязычной версии Kaspersky Endpoint Agent с помощью Kaspersky Security Center.
`agent\en-us\ksn.txt`	Файл, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Security Network на английском языке.
`agent\en-us\kmp.txt`	Файл, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Managed Protection на английском языке.
`agent\en-us\license.txt`	Файл, с помощью которого вы можете ознакомиться с Лицензионным соглашением и Политикой конфиденциальности на английском языке.
`agent\en-us\release_notes.txt`	Файл, с помощью которого вы можете ознакомиться с Информацией о выпуске для Kaspersky Endpoint Agent на английском языке.
`agent\ru-ru\ksn.txt`	Файл, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Security Network на русском языке.

Файл	Назначение
agent\ru-ru\kmp.txt	Файл, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Managed Protection на русском языке.
agent\ru-ru\license.txt	Файл, с помощью которого вы можете ознакомиться с Лицензионным соглашением и Политикой конфиденциальности на русском языке.
agent\ru-ru\release_notes.txt	Файл, с помощью которого вы можете ознакомиться с Информацией о выпуске для Kaspersky Endpoint Agent на русском языке.

Аппаратные и программные требования

Для настройки и работы с программой через веб-интерфейс на компьютерах должен быть установлен один из следующих браузеров:

- Google Chrome™ для Windows версии 80 или выше.
- Google Chrome для Linux версии 80 или выше.
- Mozilla™ Firefox™ версии 73 или выше.
- Microsoft Edge версии 80 или выше.
- Safari версии 13.0 или выше.

Минимально возможное разрешение экрана для работы в веб-интерфейсе: 1366x768 пикселей.

Для развертывания программы на виртуальной платформе должен быть установлен гипервизор VMware ESXi™ версии 6.5.0 или 6.7.0.

Конфигурация серверов с компонентами Central Node и Sandbox зависит от объема данных, обрабатываемых программой, а также от пропускной способности канала связи.

Аппаратные требования к компонентам Central Node и Sandbox приведены в Руководстве по масштабированию (см. раздел "Руководство по масштабированию" на стр. 88).

В этом разделе

kaspersky

Требования к компоненту Endpoint Agent

У компонента Endpoint Agent есть предустановленные параметры, которые определяют влияние компонента Endpoint Agent на производительность локального компьютера в сценариях получения информации и взаимодействия с компонентом Central Node.

Если версия программы Kaspersky Endpoint Detection and Response (Kaspersky Anti Targeted Attack Platform) на серверах Central Node несовместима с версией компонента Endpoint Agent (см. раздел "Совместимость версий компонента Endpoint Agent (Endpoint Sensors) с версиями Kaspersky Anti Targeted Attack Platform" на стр. 27) (ранее Endpoint Sensors), установленного на компьютерах локальной сети вашей организации, возможны следующие ограничения в работе программы: IOC-проверка файлов на компьютерах с Endpoint Agent, а также работа с задачами и политиками, созданными на компьютерах с Endpoint Agent, могут быть недоступны с серверов Central Node.

Программные требования к компьютерам для установки компонента Endpoint Agent

Для работы компонента Endpoint Agent на компьютерах должна быть установлена одна из следующих операционных систем:

- Windows 7 SP1 Home / Professional / Enterprise 32-разрядная / 64-разрядная.
- Windows 8.1.1 Professional / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS3 (версия 1703) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS4 (версия 1803) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS5 (версия 1809) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS6 (версия 1903) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 19H2 (версия 1909) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows Server 2008 R2 Foundation / Standard / Enterprise 64-разрядная.
- Windows Server 2012 Foundation / Standard / Enterprise 64-разрядная.
- Windows Server 2012 R2 Foundation / Standard / Enterprise 64-разрядная.
- Windows Server 2016 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 Essentials / Standard / Datacenter 64-разрядная.

При использовании компонента Endpoint Sensors версии 3.6 в составе Kaspersky Endpoint Security поддерживается меньше операционных систем, чем в программе KES версии 11.1.1 без встроенного компонента Endpoint Sensors.
При использовании компонента Endpoint Sensors версии 3.6.1 в составе Kaspersky Endpoint Security поддерживается меньше операционных систем, чем в программе KES версии 11.2 без встроенного компонента Endpoint Sensors.

Для работы компонента Endpoint Agent с программой Kaspersky Security для виртуальных сред Легкий агент в виртуальной инфраструктуре должен быть установлен один из следующих гипервизоров в зависимости от платформы виртуализации:

- Платформа Microsoft Hyper-V: гипервизор Microsoft Windows Server 2016 Hyper-V (в полном режиме или в режиме Server Core) со всеми доступными обновлениями.
- Платформа Citrix Hypervisor: гипервизор Citrix XenServer 7.1 LTSR.
- Платформа VMware vSphere:
  - Гипервизор VMware ESXi 6.7.
  - Гипервизор VMware ESXi 6.5.
- Платформа KVM (Kernel-based Virtual Machine): гипервизор KVM на базе одной из следующих операционных систем:
  - Ubuntu Server 18.04 LTS.
  - Ubuntu Server 16.04 LTS.
  - Red Hat Enterprise Linux Server 7.5.
  - CentOS 7.5.

Если вы используете компонент Endpoint Sensors в составе программы Kaspersky Endpoint Security, учитывайте совместимость версий программ:

- Компонент Endpoint Sensors программы Kaspersky Anti Targeted Attack Platform версии 3.6.1 входит в состав KES версии 11.2.
- Компонент Endpoint Sensors программы Kaspersky Anti Targeted Attack Platform версии 3.6 входит в состав KES версии 11.1.1.
- Компонент Endpoint Sensors программы Kaspersky Anti Targeted Attack Platform версии 3.0 входит в состав KES версии 10 SP2 MR3 и версии 11.0.

Аппаратные требования к компьютерам для установки компонента Endpoint Agent

Минимальная конфигурация:

- Процессор: 2 ГГц и выше с поддержкой инструкций SSE2.
- Объем оперативной памяти: 2 ГБ.

  Для корректной работы компонента Endpoint Agent требуется 40 МБ свободной оперативной памяти.
- Дисковая подсистема: 2 ГБ свободного пространства.

  Для установки компонента Endpoint Agent требуется 100 МБ свободного пространства.
- Один сетевой адаптер со скоростью передачи данных 1 Гбит/с.

При интеграции с программой "Лаборатории Касперского" Kaspersky Endpoint Security программа Kaspersky Anti Targeted Attack Platform имеет ограниченную функциональность, если на сервере с программой KES установлена операционная система Windows Server 2008 SP2 x64.

kaspersky

Совместимость версий компонента Endpoint Agent (Endpoint Sensors) с версиями Kaspersky Anti Targeted Attack Platform

У компонента Endpoint Agent есть предустановленные параметры, которые определяют влияние компонента Endpoint Agent на производительность локального компьютера в сценариях получения информации и взаимодействия с компонентом Central Node.

Если версия программы Kaspersky Anti Targeted Attack Platform на серверах Central Node несовместима с версией компонента Endpoint Agent (ранее Endpoint Sensors), установленного на компьютерах локальной сети вашей организации, возможны следующие ограничения в работе программы: IOC-проверка файлов на компьютерах с Endpoint Agent, а также работа с задачами и политиками, созданными на компьютерах с Endpoint Agent, могут быть недоступны с серверов Central Node.

Информация о совместимости версий компонента Endpoint Agent (Endpoint Sensors) с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Таблица 3. Совместимость версий компонента Endpoint Agent (Endpoint Sensors) с версиями Kaspersky Anti Targeted Attack Platform

Версия Endpoint Agent (Endpoint Sensors)	Тип Endpoint Agent (Endpoint Sensors): отдельный или в составе KES	Совместимость с Kaspersky Anti Targeted Attack Platform 3.0	Совместимость с Kaspersky Anti Targeted Attack Platform 3.5	Совместимость с Kaspersky Anti Targeted Attack Platform 3.6 и 3.6.1	Совместимость с Kaspersky Anti Targeted Attack Platform 3.7
Endpoint Sensors версии: 3.1.414 3.1.422	Отдельный компонент	Да	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221); события (см. раздел "Поиск угроз по базе событий" на стр. 251); задачи (см. раздел "Работа с задачами" на стр. 299) (только **Восстановить файл из карантина**).	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221); события (см. раздел "Поиск угроз по базе событий" на стр. 251); задачи (см. раздел "Работа с задачами" на стр. 299) (только **Восстановить файл из карантина**).	Нет

Версия Endpoint Agent (Endpoint Sensors)	Тип Endpoint Agent (Endpoint Sensors): отдельный или в составе KES	Совмести-мость с Kaspersky Anti Targeted Attack Platform 3.0	Совместимость с Kaspersky Anti Targeted Attack Platform 3.5	Совместимость с Kaspersky Anti Targeted Attack Platform 3.6 и 3.6.1	Совместимость с Kaspersky Anti Targeted Attack Platform 3.7
Endpoint Sensors версии: 3.1.414 3.1.422	В составе KES версии: 10 SP2 10 SP1 MR3 10 SP1 MR4	Да	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221); события (см. раздел "Поиск угроз по базе событий" на стр. 251); задачи (см. раздел "Работа с задачами" на стр. 299) (только **Восстановить файл из карантина**).	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221); события (см. раздел "Поиск угроз по базе событий" на стр. 251); задачи (см. раздел "Работа с задачами" на стр. 299) (только **Восстановить файл из карантина**).	Нет
Endpoint Sensors версии 3.1.406	В составе KES версии 11.0	Да	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221); события (см. раздел "Поиск угроз по базе событий" на стр. 251); задачи (см. раздел "Работа с задачами" на стр. 299) (только **Восстановить файл из карантина**).	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221); события (см. раздел "Поиск угроз по базе событий" на стр. 251); задачи (см. раздел "Работа с задачами" на стр. 299) (только **Восстановить файл из карантина**).	Нет
Endpoint Sensors версии: 3.5.0.X 3.6.X	Отдельный компонент	Да	Да	Да	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221) (только ТАА); события (см. раздел "Поиск угроз по базе событий" на стр. 251). Действия по реагированию на угрозы недоступны.

Версия Endpoint Agent (Endpoint Sensors)	Тип Endpoint Agent (Endpoint Sensors): отдельный или в составе KES	Совмести-мость с Kaspersky Anti Targeted Attack Platform 3.0	Совместимость с Kaspersky Anti Targeted Attack Platform 3.5	Совместимость с Kaspersky Anti Targeted Attack Platform 3.6 и 3.6.1	Совместимость с Kaspersky Anti Targeted Attack Platform 3.7
Endpoint Sensors версии 3.5.1.X	В составе KES версии 11.1	Да	Да	Да	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221) (только TAA); события (см. раздел "Поиск угроз по базе событий" на стр. 251). Действия по реагированию на угрозы недоступны.
Endpoint Sensors версии 3.6.X	В составе KES версии: 11.1.1 11.2	Да	Да	Да	Доступная функциональность: мониторинг (см. раздел "Мониторинг работы программы" на стр. 174); обнаружения (см. раздел "Таблица обнаружений" на стр. 221) (только TAA); события (см. раздел "Поиск угроз по базе событий" на стр. 251). Действия по реагированию на угрозы недоступны.
Endpoint Agent версии 3.7.1.X	Отдельный компонент	Нет	Нет	Нет	Да
Endpoint Agent версии 3.7.1.X	В составе KES версии 11.3	Нет	Нет	Нет	Да

Версия Endpoint Agent (Endpoint Sensors)	Тип Endpoint Agent (Endpoint Sensors): отдельный или в составе KES	Совмести-мость с Kaspersky Anti Targeted Attack Platform 3.0	Совместимость с Kaspersky Anti Targeted Attack Platform 3.5	Совместимость с Kaspersky Anti Targeted Attack Platform 3.6 и 3.6.1	Совместимость с Kaspersky Anti Targeted Attack Platform 3.7
Endpoint Agent версии 3.8	Отдельный компонент	Нет	Нет	Нет	Да
Endpoint Agent версии 3.9	В составе KES версии 11.4	Нет	Нет	Нет	Да Для Kaspersky Endpoint Detection and Response версии 0.1

Если вы одновременно используете **Endpoint Sensors версии 3.6.X в составе KES** и **отдельный компонент Endpoint Agent версии 3.8 или 3.9**, Kaspersky Anti Targeted Attack Platform получает данные и объекты на проверку от обоих компонентов:
• От Endpoint Sensors версии 3.6.X поступают данные об обнаружениях Kaspersky Endpoint Security, но Endpoint Sensors версии 3.6.X не совместим с обновленными технологиями Sandbox Kaspersky Anti Targeted Attack Platform версии 3.7, и Sandbox-обнаружения не создаются по полученным объектам.
• От Endpoint Agent версии 3.8 или 3.9 не поступают данные об обнаружениях Kaspersky Endpoint Security
Рекомендуется выполнить одно из следующих действий:
• Перед обновлением программы Kaspersky Endpoint Agent до версии 3.8 или 3.9 отключить использование Kaspersky Endpoint Agent в составе Kaspersky Endpoint Security и только после этого выполнять обновление программы. Иначе отключится использование и старой, и новой версии Kaspersky Endpoint Agent.
• Перед обновлением и после обновления программы Kaspersky Endpoint Agent до версии 3.8 или 3.9 в политике Kaspersky Endpoint Agent отключить использование версии 3.6.X.

Совместимость версий компонента Endpoint Agent (Endpoint Sensors) с версиями Kaspersky Endpoint Security

Информация о совместимости версий компонента Endpoint Agent (Endpoint Sensors) с версиями Kaspersky Endpoint Security приведена в таблице ниже.

Таблица 4. Совместимость версий компонента Endpoint Agent (Endpoint Sensors) с версиями Kaspersky Endpoint Security

Версия Endpoint Agent (Endpoint Sensors)	Совмести мость с KES 10 SP1 MR3	Совмести мость с KES 10 SP1 MR4	Совмести мость с KES 10 SP2 MR2	Совмести мость с KES 10 SP2 MR3/MR4	Совмести мость с KES 11.0.0	Совмести мость с KES 11.0.1	Совмести мость с KES 11.1 KES 11.1.1	Совмести мость с KES 11.2 KES 11.3	Совмести мость с KES 11.4
Endpoint Sensors версии: • 3.6 • 3.6.1	Да	Да	Да	Да	Да	Да	Нет	Да В составе KES	Нет

Версия Endpoint Agent (Endpoint Sensors)	Совместимость с KES 10 SP1 MR3	Совместимость с KES 10 SP1 MR4	Совместимость с KES 10 SP2 MR2	Совместимость с KES 10 SP2 MR3/MR4	Совместимость с KES 11.0.0	Совместимость с KES 11.0.1	Совместимость с KES 11.1 KES 11.1.1	Совместимость с KES 11.2 KES 11.3	Совместимость с KES 11.4
Endpoint Agent версии 3.7 (для программы Kaspersky Sandbox)	TBD	TBD	TBD	TBD	TBD	TBD	TBD	Да В составе KES	Нет
Endpoint Agent версии 3.8 (отдельный компонент)	Нет	Нет	Нет	Да	Нет	Да	Да	Да	Да
Endpoint Agent версии 3.9	Нет	Нет	Нет	Да	Нет	Да	Да	Да	Да В составе KES

Если вы одновременно используете **Endpoint Sensors версии 3.6.X в составе KES** и **отдельный компонент Endpoint Agent версии 3.8 или 3.9**, Kaspersky Anti Targeted Attack Platform получает данные и объекты на проверку от обоих компонентов:
• От Endpoint Sensors версии 3.6.X поступают данные об обнаружениях Kaspersky Endpoint Security, но Endpoint Sensors версии 3.6.X не совместим с обновленными технологиями Sandbox Kaspersky Anti Targeted Attack Platform версии 3.7, и Sandbox-обнаружения не создаются по полученным объектам.
• От Endpoint Agent версии 3.8 или 3.9 не поступают данные об обнаружениях Kaspersky Endpoint Security
Рекомендуется выполнить одно из следующих действий:
• Перед обновлением программы Kaspersky Endpoint Agent до версии 3.8 или 3.9 отключить использование Kaspersky Endpoint Agent в составе Kaspersky Endpoint Security и только после этого выполнять обновление программы. Иначе отключится использование и старой, и новой версии Kaspersky Endpoint Agent.
• Перед обновлением и после обновления программы Kaspersky Endpoint Agent до версии 3.8 или 3.9 в политике Kaspersky Endpoint Agent отключить использование версии 3.6.X.

Совместимость компонента Endpoint Agent с другими программами

Рекомендуется использовать сертифицированную версию Kaspersky Endpoint Security для Windows, не требующую установки отдельного компонента Endpoint Sensors или гарантировано совместимую с отдельным компонентом Endpoint Sensors.

Совместная работа Kaspersky Endpoint Detection and Response с программами, не указанными в этом разделе, не предусмотрена.

Совместимость компонента Endpoint Sensors версии 3.5 с программами "Лаборатории Касперского"

Вы можете использовать Kaspersky Endpoint Security для Windows версии 10 SP2 MR3 или 11.0 и отдельный

компонент Endpoint Sensors версии 3.5 на одном компьютере. Для этого выполните следующие действия:

1. Отключите компонент Endpoint Sensors в составе программы KES.

   Подробнее о том, как отключить компонент Endpoint Sensors в составе программы KES см. в *Справке Kaspersky Endpoint Security* https://help.kaspersky.com/KESWin/11.1.1/ru-RU/132664.htm.

2. Установите отдельный компонент Endpoint Sensors версии 3.5 на все компьютеры сети вашей организации, на которых вы хотите использовать компонент Endpoint Sensors.

Совместимость компонента Endpoint Sensors версии 3.6 с программой Kaspersky Endpoint Security для Windows (KES)

Информация о совместимости компонента Endpoint Sensors версии 3.6 с программой KES приведена в таблице ниже.

Программа Kaspersky Endpoint Security версии 11.1.1 совместима только с компонентом Endpoint Sensors, входящим в состав программы KES. Установка программы KES версии 11.1.1 и отдельного компонента Endpoint Sensors на одном компьютере невозможна.

Таблица 5. Совместимость компонента Endpoint Sensors и программы KES

Версия программы "Лаборатории Касперского"	Режим совместимости	Установка отдельного компонента Endpoint Sensors после установки другой программы	Установка другой программы после установки отдельного компонента Endpoint Sensors	Поддерживаемые операционные системы
• KES10 SP1 MR3 (Endpoint Sensors в составе KES версии 1.0) • KES10 SP1 MR4 (Endpoint Sensors в составе KES версии 1.0)	Совместная работа. Работа компонента Endpoint Sensors в составе KES **не поддерживается**.	Стандартная процедура установки.	KES, устанавливающийся поверх отдельного компонента Endpoint Sensors, **не удаляет** отдельный компонент Endpoint Sensors.	• Windows 7 SP1 Enterprise x86 x64. • Windows 8.1.1 Enterprise x86 x64. • Windows 10 RS3 Enterprise x86 x64. • Windows 10 RS4 Enterprise x86 x64. • Windows 10 RS5 Enterprise x86 x64. • Windows 10 RS6 Enterprise x86 x64. • Windows Server 2008 R2 Enterprise x64. • Windows Server 2012 Standard x64. • Windows Server 2012 R2 Standard x64. • Windows Server 2016 Standard
• KES 10 SP2 (Endpoint Sensors в составе KES версии 2.0) • KES 10 SP2 MR1 (Endpoint Sensors в составе KES версии 2.0) • KES 10 SP2 MR2 (Endpoint Sensors в составе KES версии 2.0)	Совместная работа. Работа компонента Endpoint Sensors в составе KES **не поддерживается**.	Стандартная процедура установки.	KES, устанавливающийся поверх отдельного компонента Endpoint Sensors, **не удаляет** отдельный компонент Endpoint Sensors.	

Версия программы "Лаборатории Касперского"	Режим совместимости	Установка отдельного компонента Endpoint Sensors после установки другой программы	Установка другой программы после установки отдельного компонента Endpoint Sensors	Поддерживаемые операционные системы
• KES 10 SP2 MR3 (Endpoint Sensors в составе KES версии 2.0)	Совместная работа. **Поддерживается** работа компонента Endpoint Sensors в составе KES.	Стандартная процедура установки.	KES, устанавливающийся поверх отдельного компонента Endpoint Sensors, **не удаляет** отдельный компонент Endpoint Sensors.	x64.
• KES 11.0.0 (Endpoint Sensors в составе KES версии 3.0)	Совместная работа. Работа компонента Endpoint Sensors в составе KES **не поддерживается**.	Для установки отдельного компонента Endpoint Sensors требуется отключить компонент Endpoint Sensors в составе программы KES. Подробнее о том, как отключить компонент Endpoint Sensors в составе программы KES см. в *Справке Kaspersky Endpoint Security* https://help.kaspersky.com/KESWin/11.1.1/ru-RU/132664.htm Если компонент не отключен, установка прерывается с ошибкой.	KES, устанавливающийся поверх отдельного компонента Endpoint Sensors, **не удаляет** отдельный компонент Endpoint Sensors независимо от того, включается ли компонент Endpoint Sensors в составе программы KES.	

Версия программы "Лаборатории Касперского"	Режим совместимости	Установка отдельного компонента Endpoint Sensors после установки другой программы	Установка другой программы после установки отдельного компонента Endpoint Sensors	Поддерживаемые операционные системы
• KES 11.0.1 (Endpoint Sensors в составе KES версии 3.0)	Совместная работа. **Поддерживается** работа компонента Endpoint Sensors в составе KES.	Для установки отдельного компонента Endpoint Sensors требуется отключить компонент Endpoint Sensors в составе программы KES. Подробнее о том, как отключить компонент Endpoint Sensors в составе программы KES см. в *Справке Kaspersky Endpoint Security* https://help.kaspersky.com/KESWin/11.1.1/ru-RU/132664.htm . Если компонент не отключен, установка прерывается с ошибкой.	KES, устанавливающийся поверх отдельного компонента Endpoint Sensors, **не удаляет** отдельный компонент Endpoint Sensors независимо от того, включается ли компонент Endpoint Sensors в составе программы KES.	
KES 11.1 (Endpoint Sensors в составе KES версии 3.5)	Совместная работа не поддерживается. Доступно только использование компонента Endpoint Sensors в составе KES.	Установка отдельного компонента Endpoint Sensors поверх KES невозможна. Вы можете включить использование встроенного компонента Endpoint Sensors https://help.kaspersky.com/KESWin/11.1.1/ru-RU/132664.htm в составе программы KES.	KES **удаляет** отдельный компонент Endpoint Sensors. Значения параметров отдельного компонента Endpoint Sensors не сохраняются.	

Совместимость компонента Endpoint Sensors версии 3.6 с программой Kaspersky Security для Windows Server версии 10.1.2 (KSWS 10.1.2)

Установка компонента Endpoint Sensors версии 3.6.0.62 на одном сервере с программой KSWS версии 10.1.2 поддерживается для следующих операционных систем:

- Windows Server 2008 R2 Enterprise x64.
- Windows Server 2012 Standard x64.
- Windows Server 2012 R2 Standard x64.

- Windows Server 2016 Standard x64.

Совместимость компонента Endpoint Sensors версии 3.6 с программой Kaspersky Security для виртуальных сред 5.1 Легкий агент (KSV LA)

Установка компонента Endpoint Sensors с программой KSV LA на одной виртуальной машине поддерживается для следующих операционных систем:

- Windows Server 2008 R2 Enterprise x64.
- Windows Server 2012 Standard x64.
- Windows Server 2012 R2 Standard x64.
- Windows Server 2016 Standard x64.

Для работы компонента Endpoint Sensors с программой KSV LA в виртуальной инфраструктуре должен быть установлен один из следующих гипервизоров в зависимости от платформы виртуализации:

- Платформа Microsoft Hyper-V®: гипервизор Microsoft Windows Server 2016 Hyper-V (в полном режиме или в режиме Server Core) со всеми доступными обновлениями.
- Платформа Citrix Hypervisor: гипервизор Citrix XenServer 7.1 LTSR.
- Платформа VMware vSphere™:
  - Гипервизор VMware ESXi 6.7.
  - Гипервизор VMware ESXi 6.5.
- Платформа KVM (Kernel-based Virtual Machine): гипервизор KVM на базе одной из следующих операционных систем:
  - Ubuntu Server 18.04 LTS.
  - Ubuntu Server 16.04 LTS.
  - Red Hat Enterprise Linux® Server 7.5.
  - CentOS 7.5.

Клонирование виртуальных машин с установленным компонентом Endpoint Sensors и программой KSV LA не поддерживается. Необходимо сначала клонировать виртуальную машину, сгенерировать для нее новый идентификатор SMBIOS GUID, а затем установить компонент Endpoint Sensors.

Совместимость программы Kaspersky Endpoint Agent 3.8 с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.8 совместима со следующими программами «Лаборатории Касперского»:

- Kaspersky Endpoint Security 10 для Windows: 10 SP2 MR3, 10 SP2 MR4.
- Kaspersky Endpoint Security 11 для Windows: 11.0.1, 11.1, 11.1.1, 11.2, 11.3.
- Kaspersky Security для виртуальных сред 5 Легкий агент: 5.1, 5.1.1 и выше.
- Kaspersky Security 10 для Windows Server: 10.1.0, 10.1.1, 10.1.2.

Если на устройстве установлен и используется Endpoint Sensor версии 3.6.X в составе Kaspersky Endpoint Security, рекомендуется отключить Endpoint Sensor перед установкой Kaspersky Endpoint Agent во избежание возможных конфликтов между программами.

Интеграция программы Kaspersky Endpoint Agent 3.8 с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.8 поддерживает интеграцию со следующими программами и решениями «Лаборатории Касперского»:

- Kaspersky Security Center версий 11 и 12.
- Kaspersky Sandbox 1.0.
- Kaspersky Anti Targeted Attack Platform 3.7.

Совместимость компонента Endpoint Agent с антивирусными программами других производителей

На компьютерах, на которые вы хотите установить компонент Endpoint Agent, может быть установлена одна из следующих антивирусных программ других производителей:

- Symantec™ Endpoint Protection.
- Sophos Endpoint Protection.
- ESET NOD32 Business Edition Smart Security.
- BitDefender GravityZone Advanced Business Security.
- McAfee® Endpoint Security 10.6.1.
- McAfee® Endpoint Security 10.7.

При одновременной установке нескольких антивирусных программ других производителей корректная работа компонента Endpoint Agent не гарантируется.

Если на компьютерах, на которых будет устанавливаться компонент Endpoint Agent, установлена программа RealTimes Desktop Service, рекомендуется ее удалить перед тем, как устанавливать Endpoint Agent.

kaspersky

О предоставлении данных

Для работы некоторых компонентов Kaspersky Endpoint Detection and Response необходима обработка данных на стороне "Лаборатории Касперского". Компоненты не отправляют данные без согласия администратора Kaspersky Endpoint Detection and Response.

Вы можете ознакомиться с перечнем данных и условиями их использования, а также дать согласие на обработку данных в следующих соглашениях между вашей организацией и "Лабораторией Касперского":

- В Лицензионном соглашении (например, при установке программы).

  Согласно условиям Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, перечисленную в Лицензионном соглашении в пункте Предоставление информации. Лицензионное соглашение входит в комплект поставки программы.

- В Положении о KSN (например, при установке программы или в меню администратора программы после установки).

  При участии в Kaspersky Security Network в "Лабораторию Касперского" автоматически передается информация, полученная в результате работы Kaspersky Endpoint Detection and Response. Перечень передаваемых данных указан в Положении о KSN. Пользователь Kaspersky Endpoint Detection and Response самостоятельно принимает решение об участии в KSN. Положение о KSN входит в комплект поставки программы.

  Перед тем, как данные KSN-статистики отправляются в "Лабораторию Касперского", они накапливаются в кеше на серверах с компонентами Kaspersky Endpoint Detection and Response.

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

При использовании Kaspersky Private Security Network в "Лабораторию Касперского" не передается информация о работе Kaspersky Endpoint Detection and Response, но данные KSN-статистики накапливаются в кеше на серверах с компонентами Kaspersky Endpoint Detection and Response в том же составе, что и при использовании Kaspersky Security Network. Эти накопленные данные KSN-статистики могут передаваться за пределы вашей организации в том случае, если сервер с программой Kaspersky Private Security Network находится за пределами вашей организации. Администратору Kaspersky Private Security Network необходимо обеспечить безопасность этих данных самостоятельно.

В этом разделе

kaspersky

Данные компонента Central Node

В этом разделе содержится следующая информация о данных пользователей, хранящихся на сервере с компонентом Central Node:

- состав хранимых данных;
- место хранения;
- срок хранения;
- доступ пользователей к данным.

В этом разделе

Данные в обнаружениях

Данные пользователя могут содержаться в обнаружениях. Информация об обнаружениях хранится на сервере с компонентом Central Node в директории /data/var/lib/kaspersky/storage/pgsql/10/data/ и ротируется по мере заполнения дискового пространства. Файлы, по результатам проверки которых возникло обнаружение, накапливаются на сервере с компонентом Central Node и ротируются по мере заполнения дискового пространства.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Endpoint Detection and Response не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлена программа, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Во всех обнаружениях хранится следующая информация:

- Время обнаружения.
- Дата и время изменения обнаружения.
- Категория обнаруженного объекта.
- Идентификатор пользователя, которому назначено обнаружение.
- Комментарии пользователя, добавленные в информацию об обнаружении.
- IP-адрес и имя компьютера, на котором выполнено обнаружение.
- Уникальный идентификатор компьютера, на котором выполнено обнаружение.

Если обнаружение выполнено технологией URL Reputation, на сервере может храниться следующая информация:

- URL-адрес, к которому обращался компьютер локальной сети организации.
- IP-адрес отправителя пакета данных.
- IP-адрес получателя пакета данных.
- Категория обнаруженного объекта (например, вредоносный или фишинговый URL-адрес), важность обнаружения для пользователя в соответствии с тем, какое влияние это событие может оказать на безопасность компьютера, по опыту "Лаборатории Касперского", имена обнаруженных APT-атак.
- Принадлежность группе VIP.
- Дата и время поступления сообщения в KEDR, с точностью до секунд.
- Список обнаруженных объектов.

Если обнаружение выполнено с помощью правил YARA, на сервере может храниться следующая информация:

- Версия правил YARA, с помощью которых было выполнено обнаружение.
- Категория обнаруженного объекта.
- Имена обнаруженных объектов.
- MD5-хеши обнаруженных объектов.

Если обнаружение выполнено с помощью компонента Sandbox, на сервере может храниться следующая информация:

- Время выполнения обнаружения.
- Версия баз программы, с помощью которых было выполнено обнаружение.
- Категория обнаруженного объекта.
- Имена обнаруженных объектов.
- MD5-хеши обнаруженных объектов.
- Дополнительная информация об обнаружении.

Если обнаружение выполнено в результате работы пользовательских правил IOC или TAA (IOA), на сервере может храниться следующая информация:

- Дата и время выполнения проверки.
- Идентификаторы компьютеров, на которых выполнено обнаружение.
- Имя IOC-файла.
- Содержимое IOC-файла.
- Информация об обнаруженных объектах.

Данные в событиях

Данные пользователя могут содержаться в событиях. Информация о произошедших событиях хранится на сервере с компонентом Central Node в директории /data/var/lib/kaspersky/storage/fastsearch/elasticsearch/data/ в течение 30 дней.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Endpoint Detection and Response не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлена программа, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Данные о событиях могут содержать следующую информацию:

- Имя компьютера, на котором произошло событие.
- Имя пользователя, под учетной записью которого произошло событие.
- Уникальный идентификатор компьютера с компонентом Endpoint Agent (ранее Endpoint Sensors).
- Тип события.
- Время события.
- Полные пути к файлам компьютеров с компонентом Endpoint Agent.
- Имена файлов компьютеров с компонентом Endpoint Agent.
- Полные имена папок компьютеров с компонентом Endpoint Agent.
- MD5-, SHA256-хеш файлов.
- Время создания файла.
- Время изменения файла.
- Параметры командной строки.
- Локальный IP-адрес адаптера.
- Локальный порт.
- Имя удаленного хоста.
- IP-адрес удаленного хоста.
- Порт на удаленном хосте.
- URL- и IP-адреса посещенных веб-сайтов, а также ссылки с этих веб-сайтов.
- Пути к ключам в реестре Windows.
- Информация о переменных реестра Windows: путь к переменной, имя переменной, значение переменной.
- Информация о файле процесса: путь к файлу, полное имя файла, размер файла, дата создания файла, дата изменения файла, MD5- и SHA256-хеш файла.
- Информация о файле родительского процесса: полное имя файла, путь к файлу, уникальный идентификатор файла, MD5- и SHA256-хеш файла, идентификатор родительского процесса Windows.
- Информация об интерпретированном файле: полное имя файла, путь к файлу, MD5- и SHA256-хеш файла.
- Информация о файле, запрещенном к запуску: полное имя файла, путь к файлу, MD5- и SHA256-хеш файла.
- Информация о DLL-модуле: полное имя, путь, размер, дата создания и дата изменения DLL-модуля, MD5- и SHA256-хеш DLL-модуля.

- Информация, связанная с событием создания файла: полное имя созданного файла, путь, размер, дата создания и изменения, MD5- и SHA256-хеш файла.
- Информация о файле драйвера: полное имя файла, путь к файлу, размер, дата создания и дата изменения, MD5- и SHA256-хеш файла.
- Новое и старое имена хоста в случае изменения имени хоста.
- Имя обнаруженного объекта.
- Информация о событии в журнале Windows: тип события, идентификатор типа события, идентификатор события, пользователь, под учетной записью которого событие записано в журнал, полный текст события из журнала событий Windows в формате XML.
- Информация, связанная с обнаружением KES: полное имя обнаруженного объекта, MD5- и SHA256-хеш файла, уникальный идентификатор процесса, Windows PID, параметры командной строки, тип обнаруженного объекта, имя угрозы, идентификатор записи в базе KES, версия базы KES, режим проверки, результат проверки, причина, по которой объект не может быть вылечен.

Данные в отчетах

Данные пользователя могут содержаться в отчетах. Информация об отчетах хранится на сервере с компонентом Central Node в директории /data/var/lib/kaspersky/storage/pgsql/10/data/ бессрочно.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Endpoint Detection and Response не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлена программа, к персональным данным других пользователей любыми системными средствами на его усмотрение.

В отчетах может содержаться следующая информация:

- Дата создания отчета.
- Период, за который сформирован отчет.
- Статус отчета.
- Текст отчета в виде HTML-кода.

Данные об объектах в Хранилище и на карантине

Объекты в Хранилище и на карантине могут содержать данные пользователя. Информация об объектах в Хранилище и о копиях объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, сохраненных на сервере с помощью задачи **Получить файл**, хранится на сервере с компонентом Central Node в директории /data/var/lib/kaspersky/storage/pgsql/10/data/ бессрочно.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Endpoint Detection and Response не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлена программа, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Данные об объектах в Хранилище и на карантине могут содержать следующую информацию:

- Имя объекта.
- Путь к объекту на компьютере с компонентом Endpoint Agent (ранее Endpoint Sensors).
- MD5-, SHA256-хеш файла.
- Идентификатор пользователя, поместившего объект на карантин на компьютере с компонентом Endpoint Agent (ранее Endpoint Sensors).
- Идентификатор пользователя, поместившего объект в Хранилище.
- Уникальный идентификатор компьютера, на котором хранится объект, помещенный на карантин.
- Категория обнаруженного объекта.
- Результаты проверки объекта с помощью отдельных модулей и технологий программы.

Данные о параметрах программы

Значения параметров программы хранятся на сервере с компонентом Central Node в директории /data/var/lib/kaspersky/storage/pgsql/10/data/ бессрочно.

Возможность ограничить права пользователей серверов и операционных систем, на которые установлен компонент Central Node, средствами Kaspersky Endpoint Detection and Response не предусмотрена. Администратору рекомендуется контролировать доступ пользователей серверов и операционных систем, на которые установлена программа, к персональным данным других пользователей любыми системными средствами на его усмотрение.

Данные о политиках и задачах хранятся на сервере Central Node в незашифрованном виде.

Данные о политиках

Данные о политиках могут содержать следующую информацию:

- MD5-, SHA256-хеш файла, который запрещен к запуску.
- Комментарий.
- Хосты, на которых запрещен запуск файла.
- Состояние запрета.

Данные о задачах

По результатам выполнения задачи формируется отчет, который хранится на сервере с компонентом Central Node.

Данные о задачах могут содержать следующую информацию:

- Идентификатор задачи.
- Время создания задачи.
- Имя и IP-адрес хоста, которому назначена задача.
- Максимальное время выполнения задачи.
- Приоритет выполнения задачи.

- Путь к файлу (для задач получения и удаления файла, помещения файла в Хранилище, завершения процесса).
- От чьего имени требуется выполнить программу.
- Тип задачи (выполнение команды или запуск файла).
- Путь к файлу, аргументы или командная строка.
- Рабочая директория.
- Путь к ключу реестра.
- Отчет о выполнении задачи.
- Комментарии пользователя к задаче.
- Идентификатор учетной записи пользователя, создавшего задачу.

Данные об ученых записях пользователей

Данные об учетных записях пользователей программы могут содержать следующую информацию:

- Идентификатор пользователя.
- Имя учетной записи и пароль пользователя.
- Роль пользователя в программе.
- Информация об активности пользователя.
- Права на доступ к серверам с ролью PCN.

Данные о компонентах Endpoint Agent (ранее Endpoint Sensors)

Данные о компонентах Endpoint Agent могут содержать следующую информацию:

- Уникальный идентификатор компьютера с компонентом Endpoint Agent.
- Имя компьютера с компонентом Endpoint Agent.
- Время получения первого пакета.
- Время получения последнего пакета.
- Информация о состоянии самозащиты.
- Версия компонента Endpoint Agent.
- Время и результат последней IOC-проверки на компьютере с компонентом Endpoint Agent.

Данные о параметрах пользовательских правил IOC и TAA (IOA)

Данные о параметрах пользовательских правил IOC и TAA (IOA) могут содержать следующую информацию:

- Имя IOC-файла.
- Запросы на проверку по пользовательским правилам IOC и TAA (IOA).
- Время последнего выполнения проверки.
- Состояние IOC-файла.
- Дата загрузки IOC-файла.
- Уровень важности создаваемых обнаружений.

Данные о правилах сетевой изоляции

Данные о правилах сетевой изоляции могут содержать следующую информацию:

- Имя правила.
- Уникальный идентификатор изолированного хоста.
- Статус правила.
- Имя учетной записи пользователя, создавшего или изменившего правило.
- Список исключений из правила.

Данные о шаблонах отчетов

Данные о шаблонах отчетов могут содержать следующую информацию:

- Идентификатор пользователя, создавшего или изменившего шаблон.
- Дата создания шаблона.
- Дата последнего изменения шаблона.
- HTML-код шаблона.

Данные об общих параметрах программы

Данные об общих параметрах программы могут содержать следующую информацию:

- Параметры схем расположения графиков в разделе **Мониторинг**.
- Параметры IOC-проверки.
- Показатели активности компонентов Endpoint Agent.
- Адреса группы VIP.

Служебные данные, необходимые для работы программы

Информация о служебных данных, необходимых для работы программы, приведена в таблице ниже. Служебные данные также могут содержать данные пользователей, описанных в этом разделе выше.

Таблица 6. Служебные данные, необходимые для работы программы

Тип данных	Место хранения	Доступ к данным	Срок хранения
Журнал событий операционной системы.	• /var/log	Доступ для пользователей с правами root.	Бессрочно.
Кеш данных программы (redis).	• /var/log	Доступ пользователей определяется администратором с помощью средств операционной системы. Доступ осуществляется только по шифрованному каналу IPSec.	Бессрочно.

Тип данных	Место хранения	Доступ к данным	Срок хранения
Файлы экспорта обнаружений. Файлы могут содержать следующую информацию: • Имя компьютера, на котором выполнено обнаружение. • Время обнаружения. • Категория обнаруженного объекта. • IP-адрес отправителя пакета данных. • IP-адрес получателя пакета данных. • URL-адрес отправителя пакета данных. • URL-адрес получателя пакета данных. • UserAgent компьютера с компонентом Endpoint Agent. • URL-адрес посещенного веб-сайта. • MD5-хеш обнаруженного объекта. • SHA256-хеш обнаруженного объекта. • Полное имя обнаруженного объекта. • Параметры командной строки. • Адрес электронной почты отправителя сообщения, в котором обнаружен объект. • Адреса электронной почты получателей сообщения, в котором обнаружен объект. • Имя домена, в котором выполнено обнаружение.	• /var/log	Доступ пользователей определяется администратором с помощью средств операционной системы. Экспорт данных доступен только для авторизованных пользователей. Доступ осуществляется только по шифрованному каналу IPSec.	Бессрочно.

Тип данных	Место хранения	Доступ к данным	Срок хранения
Артефакты компонента Sandbox, файлы PCAP перехваченного трафика.	• /var/opt/kaspersky/apt-agents/sb_storage	Доступ пользователей определяется администратором с помощью средств операционной системы.	Файлы ротируются при заполнении отведенного места хранения.
Очередь объектов на проверку.	• /var/opt/kaspersky/apt-collector/spool	Доступ пользователей определяется администратором с помощью средств операционной системы.	До выполнения проверки.
Объекты на карантине, а также объекты, полученные от компонента Endpoint Agent.	• /var/opt/kaspersky/apt/edr_quarantine • /var/opt/kaspersky/apt/edr_storage	Доступ пользователей определяется администратором с помощью средств операционной системы.	Файлы ротируются при заполнении отведенного места хранения.
YARA-правила.	• /var/opt/kaspersky/apt-agents/yara_rules	Доступ пользователей определяется администратором с помощью средств операционной системы.	Бессрочно.
Сертификаты серверов, используемые для интеграции компонентов программы.	• /etc/ssl/certs	Доступ пользователей определяется администратором с помощью средств операционной системы. Информация о действиях с сертификатами сохраняется в журнале событий программы.	Бессрочно.
Ключи шифрования, передаваемые между компонентами программы.	• /etc/opt/kaspersky/apt-base/ipsec.d	Доступ пользователей определяется администратором с помощью средств операционной системы. Информация об изменениях ключей шифрования сохраняется в журнале событий программы.	Бессрочно.

Данные компонента Sandbox

На время обработки тело переданного компонентом Central Node файла сохраняется в открытом виде на сервере с компонентом Sandbox. Во время обработки доступ к переданному файлу может получить администратор сервера в режиме Technical Support Mode. Проверенный файл удаляется специальным скриптом по расписанию. По умолчанию один раз в 60 минут.

Информация о данных, хранящихся на сервере с компонентом Sandbox, приведена в таблице ниже.

Таблица 7. Данные, хранящиеся на сервере с компонентом Sandbox

Состав данных	Место хранения	Срок хранения	Доступ к данным
Проверяемые файлы	/var/opt/kaspersky/sandbox/library/	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов.	Доступ пользователей определяется администратором с помощью средств операционной системы.
Результат проверки файлов	• /var/opt/kaspersky/sandbox/library/ • /tmp/	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов.	Доступ пользователей определяется администратором с помощью средств операционной системы.
Параметры задач	• /var/opt/kaspersky/sandbox/library/ • база данных компонента Sandbox	После получения компонентом Central Node результатов проверки или до автоматического удаления, но не более 24 часов в директории /var/opt/kaspersky/sandbox/library/. В базе данных компонента Sandbox до 90 дней.	Доступ пользователей к директории /var/opt/kaspersky/sandbox/library/ определяется администратором с помощью средств операционной системы. Для аутентификации пользователей в базе данных требуется пароль. Доступ к файлам базы данных имеют только пользователи, от имени которых запущены процессы базы данных, и пользователь с правами root. Доступ осуществляется только по шифрованному каналу IPSec.
Файлы трассировки	/var/log/kaspersky/sandbox/	До 21 дня.	Доступ пользователей определяется администратором с помощью средств операционной системы. Действия с файлами трассировки доступны только для авторизованных пользователей. Информация о действиях с файлами трассировки сохраняется в журнале событий программы.

kaspersky

Данные, пересылаемые между компонентами программы

Central Node и Endpoint Agent (ранее Endpoint Sensors)

Компонент Endpoint Agent отправляет на компонент Central Node отчеты о выполнении задач, информацию о событиях и обнаружениях, произошедших на компьютерах с компонентом Endpoint Agent, а также информацию о терминальных сессиях.

Если связь с компонентом Central Node отсутствует, все данные, предназначенные для отправки, накапливаются до тех пор, пока они не будут отправлены на компонент Central Node или компонент Endpoint Agent не будет удален с компьютера, но не более 21 дня.

Если событие произошло на компьютере пользователя, компонент Endpoint Agent отправляет следующие данные в базу событий:

1. Событие создания файла.
    - Сведения о процессе, создавшем файл: имя файла процесса, MD5-, SHA256-хеш файла процесса.
    - Имя файла.
    - Путь к файлу.
    - Полное имя файла.
    - MD5-, SHA256-хеш файла.
    - Дата создания и изменения файла.
    - Размер файла.
    - Поля заголовка события: ProviderName, EventId, Version, Level, Task, Opcode, Keywords, TimeCreatedSystemTime, EventRecordId, CorellationActivityId, ExecutionProcessID, ThreadID, Channel, Computer.
    - Поля тела события: AccessList, AccessMask, AccountExpires, AllowedToDelegateTo, Application, AuditPolicyChanges, AuthenticationPackageName, CategoryId, CommandLine, DisplayName, Dummy, ElevatedToken, EventCode, EventProcessingFailure, FailureReason, FilterRTID, HandleId, HomeDirectory, HomePath, ImpersonationLevel, IpAddress, IpPort, KeyLength, LayerName, LayerRTID, LmPackageName, LogonGuid, LogonHours, LogonProcessName, LogonType, MandatoryLabel, MemberName, MemberSid, NewProcessId, NewProcessName, NewUacValue, NewValue, NewValueType, ObjectName, ObjectServer, ObjectType, ObjectValueName, OldUacValue, OldValue, OldValueType, OperationType, PackageName, ParentProcessName, PasswordLastSet, PrimaryGroupId, PriviledgeList, ProcessId, ProcessName, ProfileChanged, ProfilePath, Protocol, PublisherId, ResourceAttributes, RestrictedAdminMode, SamAccountName, ScriptPath, ServiceAccount, ServiceFileName, ServiceName, ServiceStartType, ServiceType, SettingType, SettingValue, ShareLocalPath, ShareName, SidHistory, SourceAddress, SourcePort, Status, SubcategoryGuid, SubcategoryId, SubjectDomainName, SubjectLogonId, SubjectUserName, SubjectUserSid, SubStatus, TargetDomainName, TargetLinkedLogonId, TargetLogonId, TargetOutboundDomainName, TargetOutboundUserName, TargetUserName, TargetUserSid, TaskContent, TaskName, TokenElevationType, TransmittedServices, UserAccountControl, UserParameters, UserPrincipalName, UserWorkstations, VirtualAccount, Workstation, WorkstationName.
2. Событие мониторинга реестра.

- Сведения о процессе, изменившем реестр: ID процесса, имя файла процесса, MD5-, SHA256-хеш файла процесса.
- Путь к ключу в реестре.
- Имя переменной реестра.
- Данные переменной реестра.

3. Событие загрузки драйвера.
   - Имя файла.
   - Путь к файлу.
   - Полное имя файла.
   - MD5-, SHA256-хеш файла.
   - Размер файла.
   - Дата создания и изменения файла.
4. Событие открытия порта на прослушивание.
   - Сведения о процессе, открывшем порт на прослушивание: имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Номер порта.
   - IP-адрес адаптера.
5. Событие в журнале Windows.
   - Время события, хост, на котором произошло событие, имя учетной записи пользователя.
   - ID события.
   - Имя журнала/канала.
   - ID события в журнале.
   - Имя провайдера.
   - Подтип события аутентификации.
   - Имя домена.
   - Удаленный IP-адрес.
6. Событие запуска процесса.
   - Сведения о файле, запустившем процесс: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла.
   - UniquePID.
   - Параметры командной строки.
   - Сведения о родительском процессе: UniquePID, Windows ID процесса, MD5-, SHA256-хеш файла процесса.
   - Время окончания работы процесса.
7. Событие загрузки модуля.
   - Сведения о файле, загрузившем модуль: UniquePID, имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла.
   - Имя файла DLL.

- Путь к файлу DLL.
- Полное имя файла DLL.
- MD5-, SHA256-хеш файла DLL.
- Размер файла DLL.
- Дата создания и изменения файла DLL.

8. Событие блокирования запуска процесса.
   - Сведения о файле, который пытались выполнить: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла.
   - Параметры командной строки.
9. Событие блокирования запуска файла.
   - Сведения о файле, который пытались открыть: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, тип контрольной суммы, по которой произведена блокировка, размер файла (0 – MD5, !=0 – SHA256, для поиска не используется).
   - Сведения об исполняемом файле: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла.
   - Сведения о родительском процессе: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, PID, UniquePID.
10. Событие смены имени хоста.
    - Время события.
    - Старое имя хоста.
    - Новое имя хоста.
11. Событие изменения содержимого файла hosts.
    - Содержимое файла hosts.
12. Событие программы Kaspersky Endpoint Security для Windows, сохраняемое в базах программы.
    - Информация об обнаружении Kaspersky Endpoint Security для Windows.
13. Событие программы Kaspersky Endpoint Security для Windows, отображаемое пользователю.
    - Результат проверки.
    - Название обнаруженного объекта.
    - Идентификатор записи в базах программы.
    - Время выпуска баз программы, с помощью которых было выполнено обнаружение.
    - Режим обработки объекта.
    - Категория обнаруженного объекта (например, название вируса).
    - MD5-хеш обнаруженного объекта.
    - SHA256-хеш обнаруженного объекта.
    - Уникальный идентификатор процесса.
    - PID процесса, отображаемый в диспетчере задач Windows.
    - Командная срока запуска процесса.
    - Причина ошибки при обработке объекта.

14. Событие изменения организационного подразделения (OU) Active Directory.
    - Информация об организационных подразделениях (OU) Active Directory.

Central Node и Sandbox

Компонент Central Node отправляет на компонент Sandbox файлы и URL-адреса, выделенные из сетевого или почтового трафика. Перед передачей файлы никак не изменяются. Компонент Sandbox отправляет компоненту Central Node результаты проверки.

Central Node и Sensor

Программа может пересылать между компонентами Central Node и Sensor следующие данные:

- Информацию о лицензии.
- Данные компонента Endpoint Sensors, если настроена интеграция с прокси-сервером (см. раздел "Включение интеграции с прокси-сервером по протоколу ICAP" на стр. 189).
- Базы программы, если настроено получение обновления баз от компонента Central Node.

Серверы с ролями PCN и SCN

Если программа работает в режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76), то между PCN и подключенными SCN передаются следующие данные:

- Об обнаружениях.
- О событиях.
- О задачах.
- О политиках.
- О проверке по пользовательским правилам IOC, TAA (IOA), YARA.
- О файлах в Хранилище.
- Об учетных записях пользователей.
- О лицензии.
- Список компьютеров с установленным компонентом Endpoint Agent.
- Объекты, помещенные в Хранилище.
- Объекты, помещенные на карантин на компьютерах с компонентом Endpoint Agent.
- Файлы, прикрепленные к обнаружениям.
- IOC-файлы.

Данные компонента Endpoint Agent

Если вы используете компонент Endpoint Agent, для обеспечения основной функциональности, аудита и повышения скорости решения возникших проблем специалистами Службы технической поддержки "Лаборатории Касперского" программа Kaspersky Endpoint Agent хранит и обрабатывает данные локально.

На компьютерах с компонентом Endpoint Agent хранятся данные, подготовленные для отправки на серверы Kaspersky Endpoint Detection and Response и в Kaspersky Security Center в автоматическом режиме.

Файлы, подготовленные Endpoint Agent к отправке на проверку на серверы программы, хранятся на компьютерах с компонентом Endpoint Agent в открытом незашифрованном виде в той директории, которая по умолчанию используется для хранения файлов перед отправкой.

На сервер с компонентом Central Node могут передаваться файлы, связанные с обнаруженными событиями.

Среди этих данных могут быть персональные данные пользователя или конфиденциальные данные вашей организации.

Отключение отправки данных с компьютеров с компонентом Endpoint Agent на сервер с компонентом Central Node не предусмотрено.

Не используйте компонент Endpoint Agent на тех компьютерах, передача данных с которых запрещена политикой вашей организации.

Данные, полученные от компонента Endpoint Agent, хранятся в базе данных на сервере с компонентом Central Node и ротируются по мере заполнения дискового пространства.

Файлы, подготовленные к отправке компонентом Endpoint Agent на сервер с компонентом Central Node, хранятся на компьютерах с компонентом Endpoint Agent в открытом незашифрованном виде в той директории, которая по умолчанию используется для хранения файлов перед отправкой на каждом компьютере с компонентом Endpoint Agent.

Файлы с компьютеров с компонентом Endpoint Agent отправляются только на сервер с компонентом Central Node по защищенному SSL-соединению.

Файлы, зашифрованные на компьютерах с компонентом Endpoint Agent с помощью программ Windows Encrypting File System или Kaspersky File Level Encryption (в программе Kaspersky Endpoint Security для Windows), передаются на сервер с компонентом Central Node в расшифрованном виде.

Kaspersky Endpoint Detection and Response поддерживает возможность изменения параметров локального компьютера с компонентом Endpoint Agent, влияющих на производительность компьютера при взаимодействии с компонентом Central Node.
Изменение параметров следует производить исключительно по рекомендации Службы технической поддержки "Лаборатории Касперского".
Самостоятельное изменение параметров может ухудшить производительность локального компьютера.

Администратору Kaspersky Endpoint Detection and Response необходимо обеспечить безопасность компьютеров с компонентом Endpoint Agent и серверов Kaspersky Endpoint Detection and Response с перечисленными выше данными самостоятельно. Администратор Kaspersky Endpoint Detection and Response несет ответственность за доступ к данной информации.

В этом разделе содержится следующая информация о данных пользователей, хранящихся на компьютерах с компонентом Endpoint Agent:

- состав хранимых данных;
- место хранения;
- срок хранения;
- доступ пользователей к данным.

kaspersky

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов, удаляются с устройства при удалении программы.

В этом разделе

Данные, получаемые от компонента Central Node

Компонент Endpoint Agent сохраняет на жестком диске компьютера значения параметров, получаемые от компонента Central Node. Данные сохраняются в открытом незашифрованном виде в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Компонент Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Данные удаляются при удалении компонента Endpoint Agent.

Данные, получаемые от компонента Central Node, могут содержать следующую информацию:

- О сетевых соединениях.
- Об операционной системе, установленной на сервере с компонентом Central Node.
- Об учетных записях пользователей операционной системы.
- О пользовательских сессиях в операционной системе.
- О журнале событий Windows.
- О ресурсе типа RT_VERSION.
- О содержимом PE-файла.
- О службах операционной системы.

- Сертификат сервера с компонентом Central Node.
- URL- и IP-адреса посещенных веб-сайтов.
- Заголовки протокола HTTP.
- Имя компьютера.
- MD5-хеши файлов.
- Уникальный идентификатор компьютера с компонентом Endpoint Agent.
- Имена и значения ключей реестра Windows.
- Пути к ключам реестра Windows.
- Имена переменных реестра Windows.
- Имя записи локального DNS-кеша.
- Адрес из записи локального DNS-кеша в формате IPv4.
- IP-адрес или имя запрашиваемого хоста из локального DNS-кеша.
- Хост элемента локального DNS-кеша.
- Доменное имя элемента локального DNS-кеша.
- Адрес элемента ARP-кеша в формате IPv4.
- Физический адрес элемента APR-кеша.
- Серийный номер логического диска.
- Домашняя директория локального пользователя.
- Имя учетной записи пользователя, запустившего процесс.
- Путь к скрипту, запускаемому при входе пользователя в систему.
- Имя пользователя, под учетной записью которого произошло событие.
- Имя компьютера, на котором произошло событие.
- Полные пути к файлам компьютеров с компонентом Endpoint Agent.
- Имена файлов компьютеров с компонентом Endpoint Agent.
- Маски файлов компьютеров с компонентом Endpoint Agent.
- Полные имена папок компьютеров с компонентом Endpoint Agent.
- Комментарии поставщика файла.
- Маска файла-образа процесса.
- Путь к файлу-образу процесса, открывшего порт.
- Имя процесса, открывшего порт.
- Локальный IP-адрес порта.
- Доверенный публичный ключ цифровой подписи исполняемых модулей.
- Имя процесса.
- Имя сегмента процесса.
- Параметры командной строки.

kaspersky

Данные в полях событий Windows Event Log программы Kaspersky Endpoint Agent

Данные о событиях Журнала событий Windows хранятся в файле %SystemRoot%\System32\Winevt\Logs\Kaspersky-Security-Soyuz%4Product.evtx в открытом незашифрованном виде. Данные хранятся до удаления Kaspersky Endpoint Agent.

Эти данные могут автоматически передаваться в Kaspersky Security Center, но не передаются в Kaspersky Sandbox.

По умолчанию доступ на чтение к файлам имеют только пользователи с правами System и Administrator. Kaspersky Endpoint Agent не управляет правами доступа к этой папке и ее файлам. Доступ определяет системный администратор.

Данные о событиях могут содержать следующую информацию:

- О пользовательских сессиях в операционной системе.
- Об учетных записях пользователей операционной системы (userID).
- Об ошибках выполнения задач проверки объектов.
- О задачах на проверку объектов.
- Об обнаружениях Kaspersky Sandbox.
- О событиях Kaspersky Sandbox.
- Об IOC-файлах Kaspersky Endpoint Agent, сформированных при автоматическом реагировании.
- О результатах проверки объектов.
- О сертификатах серверов Kaspersky Sandbox.
- Об очереди объектов на проверку.
- Об изменении параметров Kaspersky Endpoint Agent.
- Об изменении политик Kaspersky Security Center.
- Об изменении статуса задачи на проверку объектов.
- О политиках Kaspersky Security Center.
- Об объектах на карантине.
- О действиях по автоматическому реагированию на обнаруженные угрозы.
- Об ошибках взаимодействия с серверами программы.

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов, удаляются с устройства при удалении программы.

Данные в запросах Kaspersky Endpoint Agent к Kaspersky Endpoint Detection and Response

При интеграции с компонентом Central Node следующие данные хранятся локально на устройстве с Kaspersky Endpoint Agent.

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов, удаляются с устройства при удалении программы.

Данные из запросов от Kaspersky Endpoint Agent к компоненту Central Node:

1. В запросах на синхронизацию:
   - Уникальный идентификатор Kaspersky Endpoint Agent.
   - Базовая часть веб-адреса сервера.
   - Имя устройства.
   - Локальное время на устройстве.
   - Статус самозащиты Kaspersky Endpoint Agent.
   - Имя и версия операционной системы, установленной на устройстве.
   - Версия Kaspersky Endpoint Agent.
   - Версии параметров программы и параметров задач.
   - Состояние задач в Kaspersky Endpoint Agent: идентификаторы выполняющихся задач, статусы выполнения, коды ошибок выполнения.
   - Состояние параметров Kaspersky Endpoint Agent: тип применяющихся параметров, версия параметров, статус применения параметров, коды ошибок применения.
2. В запросах на получение файлов с сервера:
   - Уникальные идентификаторы файлов.
   - Уникальный идентификатор Kaspersky Endpoint Agent.
   - Уникальные идентификаторы задач.
   - Базовая часть веб-адреса сервера с компонентом Central Node.
3. В отчетах о результатах выполнения задач:
   - Информация об объектах, обнаруженных при поиске IOC.
   - Флаги дополнительных действий, выполняемых Kaspersky Endpoint Agent по завершении задач (например, "deleteFileAfterReboot" : false).
   - Ошибки выполнения задач и коды возврата.
   - Статусы, с которыми завершались задачи.
   - Время завершения выполнения задач.
   - Версии параметров, с которыми выполнялись задачи.
   - Информация об объектах, переданных на сервер, помещенных на карантин, восстановленных из карантина: пути к объектам, MD5 и SHA256-хеши объектов, идентификаторы объектов на карантине.
   - Информация о процессах, запущенных или остановленных на устройстве с Kaspersky Endpoint Agent по запросу сервера: PID и UniquePID, error code.
   - Файлы, запрошенные сервером.
   - Пакеты телеметрии.

Данные из запросов от компонента Central Node к Kaspersky Endpoint Agent:

1. Параметры задач:
   - Типы задач.
   - Параметры расписания запуска задач.
   - Имена и пароли учетных записей, под которыми необходимо запускать задачи.
   - Версии параметров.
   - Идентификаторы объектов на карантине.
   - Пути к объектам.
   - MD5 и SHA256-хеши объектов.
   - Командная строка запуска процесса с аргументами.
   - Флаги дополнительных действий, выполняемых Kaspersky Endpoint Agent по завершении задачи.
   - Идентификаторы IOC-файлов, которые нужно получить с сервера.
   - IOC-файлы.
2. Параметры сетевой изоляции:
   - Типы параметров.
   - Версии параметров.
   - Списки исключений из сетевой изоляции и параметры исключений: направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам.
   - Флаги дополнительных действий, выполняемых Kaspersky Endpoint Agent.
   - Время автоматического отключения изоляции.
3. Параметры запрета запуска и открытия документов:
   - Типы параметров.
   - Версии параметров.
   - Списки правил запрета запуска и параметры правил: пути к объектам, типы объектов, MD5 и SHA256-хеши объектов.
   - Флаги дополнительных действий, выполняемых Kaspersky Endpoint Agent.
4. Параметры фильтрации событий:
   - Имена модулей.
   - Полные пути к объектам.
   - MD5 и SHA256-хеши объектов.
   - Идентификаторы записей в журнале событий Windows.
   - Параметры цифровых сертификатов.
   - Направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам.
   - Имена пользователей.
   - Типы входа пользователей.
   - Типы событий телеметрии, для которых применяются фильтры.

kaspersky

Служебные данные Kaspersky Endpoint Agent

К служебным данным Kaspersky Endpoint Agent относятся:

- данные, попадающие в конфигурационные файлы в результате настройки параметров администратором;
- данные, обрабатываемые при автоматическом реагировании на угрозы;
- данные, обрабатываемые при интеграции с Kaspersky Sandbox;
- данные, обрабатываемые при интеграции с компонентом Central Node.

Служебные данные хранятся в файле %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>. Данные в подпапке Settings зашифрованы с помощью Шифрующей файловой системы (EFS). Данные хранятся до удаления Kaspersky Endpoint Agent.

Эти данные могут автоматически передаваться в Kaspersky Security Center, но не передаются в Kaspersky Sandbox.

По умолчанию доступ к файлам имеют только пользователи с правами System (полный доступ) и Administrator (чтение и исполнение). Папка %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия> и подпапка Restored также доступны пользователям с правами User (только чтение).

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов, удаляются с устройства при удалении программы.

Kaspersky Endpoint Agent хранит следующие данные, обрабатываемые при автоматическом реагировании и интеграции с Kaspersky Sandbox:

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent:
   - Пароль доступа к Kaspersky Endpoint Agent.
   - Файлы на карантине.
   - Параметры Kaspersky Endpoint Agent.
   - Учетные данные пользователей операционной системы для запуска задач с правами определенного пользователя.
   - Учетные данные для авторизации на Сервере администрирования Kaspersky Security Center.
   - Учетные данные для авторизации на прокси-сервере.
   - Адреса пользовательских источников обновлений.
   - Открытый ключ сертификата для интеграции с Kaspersky Sandbox.
2. Кеш Kaspersky Endpoint Agent:
   - Время записи результата проверки в кеш.
   - MD5-хеш задачи проверки.
   - Идентификатор задачи проверки.
   - Результат проверки объекта.
3. Очередь запросов на проверку объекта:
   - Идентификатор объекта в очереди.

- Время помещения объекта в очередь.
- Статус обработки объекта в очереди.
- Идентификатор пользовательской сессии в операционной системе, в которой создана задача на проверку объекта.
- Системный идентификатор (SID) пользователя операционной системы, с правами учетной записью которого создана задача на проверку объекта.
- MD5-хеш задачи на проверку объекта.

4. Информация о задачах, для которых Kaspersky Endpoint Agent ожидает результат проверки от Kaspersky Sandbox:
   - Время получения задачи на проверку объекта.
   - Статус обработки объекта.
   - Идентификатор пользовательской сессии в операционной системе, в которой создана задача на проверку объекта.
   - Идентификатор задачи на проверку объекта.
   - MD5-хеш задачи на проверку объекта.
   - Системный идентификатор (SID) пользователя операционной системы, под учетной записью которого создана задача.
   - XML-схема автоматически созданного IOC.
   - MD5 и SHA256-хеши проверяемого объекта.
   - Ошибки обработки.
   - Имена объектов, на проверку которых создана задача.
   - Результат проверки объекта.

Kaspersky Endpoint Agent хранит локально следующие данные при интеграции с компонентом Central Node:

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent:
   - Файлы на карантине.
   - Параметры Kaspersky Endpoint Agent:
     - Пароль доступа к Kaspersky Endpoint Agent.
     - Учетные данные пользователей операционной системы для запуска задач с правами определенного пользователя.
     - Учетные данные для авторизации на Сервере администрирования Kaspersky Security Center.
     - Учетные данные для авторизации на прокси-сервере.
     - Адреса пользовательских источников обновлений.
     - Открытый ключ сертификата для интеграции с KATA Central Node.
     - Открытый ключ сертификата для интеграции с Kaspersky Sandbox.
     - Данные о лицензии.
2. Данные, необходимые для интеграции с компонентом Central Node:
   - Обновляемые схемы фильтрации телеметрии.
   - Очередь пакетов событий телеметрии.

- Кеш идентификаторов IOC-файлов, полученных от компонента Central Node.
- Объекты для передачи на сервер в рамках задачи Получить файл.

Данные в файлах трассировки и дампов Kaspersky Endpoint Agent

Kaspersky Endpoint Agent может выполнять запись отладочной информации в соответствии с заданными параметрами в файлы трассировки для оказания поддержки во время работы Kaspersky Endpoint Agent.

Файлы дампов Kaspersky Endpoint Agent формируются операционной системой при сбоях программы и перезаписываются при каждом сбое.

В файлы трассировки и дампов могут попасть любые персональные данные пользователя или конфиденциальные данные вашей организации.

Не используйте Kaspersky Endpoint Agent на хостах, передача данных с которых запрещена политикой вашей организации.

По умолчанию Kaspersky Endpoint Agent не записывает отладочную информацию.

Автоматическая отправка файлов трассировки и дампов за пределы хоста, на котором они были сформированы, не производится. Содержимое файлов трассировки можно просмотреть с помощью стандартных средств просмотра текстовых файлов. Файлы трассировки и дампов хранятся бессрочно и не удаляются при деинсталляции Kaspersky Endpoint Agent.

Отладочная информация может понадобиться при обращении в Службу технической поддержки.

Специальных механизмов ограничения доступа к файлам трассировки и дампов не предусмотрено. Администратор может самостоятельно настроить запись этой информации в защищенную папку.

Путь к папке для записи файлов трассировки и дампов по умолчанию не задан. Администратору нужно указать папку для записи файлов трассировки и дампов самостоятельно.

Данные в файлах трассировки и дампов могут содержать следующую информацию:

- Действия, выполненные Kaspersky Endpoint Agent на хосте.
- Информация об объектах, обрабатываемых Kaspersky Endpoint Agent.
- Ошибки, возникшие в процессе работы Kaspersky Endpoint Agent.
- Время события.
- Номер потока выполнения.
- Компонент программы, в результате работы которого произошло обнаружение.
- Важности события.
- Об исполняемых модулях.
- Об открытых портах.
- О сетевых соединениях.
- Об операционной системе, установленной на компьютере с компонентом Endpoint Agent.
- Об учетных записях пользователей операционной системы.
- О пользовательских сессиях в операционной системе.

- О журнале событий Windows.
- Об обнаружениях Kaspersky Endpoint Security для Windows.
- Об организационных подразделениях (OU) Active Directory®.
- Уникальный идентификатор компьютера с компонентом Endpoint Agent.
- Полное доменное имя компьютера.
- Серийный номер логического диска.
- Заголовки протокола HTTP.
- Полные пути к файлам компьютеров с компонентом Endpoint Agent.
- Имена файлов компьютеров с компонентом Endpoint Agent.
- Полные имена папок компьютеров с компонентом Endpoint Agent.
- Домашняя папка локального пользователя.
- Имя учетной записи пользователя, запустившего процесс.
- Путь к скрипту, запускаемому при входе пользователя в систему.
- Имя пользователя, под учетной записью которого произошло событие.
- URL- и IP-адреса посещенных веб-сайтов, а также ссылки с этих веб-сайтов.
- При использовании прокси-сервера: IP-адрес прокси-сервера, имя компьютера, порт, имя пользователя прокси-сервера.
- Внешние IP-адреса, с которыми было установлено соединение с локального компьютера.
- Команды запуска процесса.
- Параметры командной строки.
- Идентификатор Агента администрирования Kaspersky Security Center.
- Пути к ключам в реестре Windows.
- Имена переменных реестра Windows.
- Значения переменных реестра Windows.
- Разделы реестра Windows.
- Имена обнаруженных объектов.
- Имя записи локального DNS-кеша.
- IP-адрес из записи локального DNS-кеша в формате IPv4.
- IP-адрес или имя запрашиваемого хоста из локального DNS-кеша.
- Хост элемента локального DNS-кеша.
- Доменное имя элемента локального DNS-кеша.
- IP-адрес элемента ARP-кеша в формате IPv4.
- Физический адрес элемента APR-кеша.
- Имя учетной записи пользователя, запустившего сервис операционной системы.
- Параметры, с которыми запущен сервис операционной системы.
- Исходное имя файла (OriginalFileName) для ресурса RT_VERSION.

kaspersky

Данные, отправляемые в "Лабораторию Касперского" при принятии условий Положений о KSN и KMP

При согласии с условиями Положения о KSN (Kaspersky Security Network) и Положения о KMP (Kaspersky Managed Protection) программа автоматически отправляет информацию об этом в "Лабораторию Касперского".

Данные о принятии условий Положений могут храниться локально в папке %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Data\.

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов, удаляются с устройства при удалении программы.

Следующие данные отправляются в "Лабораторию Касперского" при принятии или отзыве согласия с условиями Положения о KSN и Положения о KMP:

- Идентификатор соглашения (KSN, KMP, EULA).
- Версия соглашения.
- Флаг принятия соглашения (1 – соглашение принято, 0 – соглашение отозвано).
- Дата принятия или отзыва соглашения.

"Лаборатория Касперского" может использовать эти данные для формирования статистической информации.

Данные в обнаружениях и событиях

Данные о событиях хранятся в бинарном виде в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata в открытом незашифрованном виде.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Компонент Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Данные о событиях могут содержать следующую информацию:

- Об исполняемых модулях.
- О сетевых соединениях.
- Об операционной системе, установленной на компьютере с компонентом Endpoint Agent.
- О пользовательских сессиях в операционной системе.
- Об учетных записях пользователей операционной системы.
- О журнале событий Windows.
- Об обнаружениях Kaspersky Endpoint Security для Windows.
- Об организационных подразделениях (OU) Active Directory.
- Заголовки протокола HTTP.
- Полное доменное имя компьютера.

- MD5-, SHA256-хеш файлов и их фрагментов.
- Уникальный идентификатор компьютера с компонентом Endpoint Agent.
- Уникальные идентификаторы сертификатов.
- Издатель сертификата.
- Субъект сертификата.
- Название алгоритма, при помощи которого выполнен отпечаток сертификата.
- Адрес и порт локального сетевого интерфейса.
- Адрес и порт удаленного сетевого интерфейса.
- Поставщик программы.
- Название программы.
- Имя переменной реестра Windows.
- Путь к ключу реестра Windows.
- Данные переменной реестра Windows.
- Имя обнаруженного объекта.
- Идентификатор Агента администрирования Kaspersky Security Center.
- Содержимое файла hosts.
- Командная строка запуска процесса.

Данные в отчетах о выполнении задач

Перед отправкой на компонент Central Node отчеты, а также сопутствующие файлы временно сохраняются на жестком диске компьютера с компонентом Endpoint Agent. Отчеты о выполнении задач сохраняются в архивированном незашифрованном виде в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\data_queue.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Компонент Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Отчеты о выполнении задач содержат следующую информацию:

- О результатах выполнения задач.
- Об исполняемых модулях.
- О процессах операционной системы.
- Об учетных записях пользователей.
- О пользовательских сессиях.
- Полное доменное имя компьютера.
- Уникальный идентификатор компьютера с компонентом Endpoint Agent.
- Файлы компьютера с компонентом Endpoint Agent.
- Имена альтернативных потоков NTFS.

- Полные пути к файлам компьютера с компонентом Endpoint Agent.
- Полные имена папок компьютера с компонентом Endpoint Agent.
- Содержимое стандартного потока вывода процесса.
- Содержимое стандартного потока ошибок процесса.

Данные в журнале установки

Администратор может включить запись журнала установки компонента Endpoint Agent (стандартными средствами msiexec) при установке с помощью командной строки. Администратор указывает путь к файлу, в котором будет сохраняться журнал установки.

В журнал записываются шаги процесса установки, а также командная строка вызова msiexec, которая содержит адрес сервера с компонентом Central Node и путь к файлу журнала установки.

Данные о файлах, запрещенных к запуску

Данные о файлах, запрещенных к запуску, хранятся в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\\protected\kata в открытом незашифрованном виде.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Компонент Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

Данные о файлах, запрещенных к запуску, могут содержать следующую информацию:

- Полный путь к запрещенному файлу.
- MD5-хеш файла.
- SHA256-хеш файла.
- Команда запуска процесса.

Данные, связанные с выполнением задач

При выполнении задачи помещения файла на карантин архив, содержащий этот файл, временно сохраняется в незашифрованном виде в одной из следующих папок:

- для компонента Endpoint Agent, входящего в состав программы Kaspersky Endpoint Security, в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp;
- для компонента Endpoint Agent, установленного из пакета Kaspersky Endpoint Detection and Response (Kaspersky Anti Targeted Attack Platform), в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\\protected\data\kata\temp.

При выполнении задачи запуска программы на хосте компонент Endpoint Agent локально хранит содержимое стандартных потоков вывода и ошибок запущенного процесса в открытом незашифрованном виде до тех пор, пока отчет о выполнении задачи не будет отправлен на компонент Central Node. Файлы хранятся в одной из следующих папок:

- для компонента Endpoint Agent, входящего в состав программы Kaspersky Endpoint Security, в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\\protected\kata\temp;

- для компонента Endpoint Agent, установленного из пакета Kaspersky Endpoint Detection and Response (Kaspersky Anti Targeted Attack Platform), в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\\protected\data\kata\temp.

По умолчанию при включенной самозащите доступ к файлам на чтение имеют только пользователи с правами System и Administrator. При выключенной самозащите пользователи с правами System и Administrator могут также удалять файлы, изменять их содержимое и изменять права доступа к ним. Компонент Endpoint Agent не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор.

kaspersky

Лицензирование программы

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

В этом разделе

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки программы.
- Прочитав документ /EULA/License.<язык>.

  Этот документ включен в комплект поставки программы.
- В веб-интерфейсе программы в разделе **Параметры**, подразделе **Лицензия** по кнопке **Лицензионное соглашение**.

- В веб-интерфейсе компонента Sandbox в меню  по ссылке **Лицензионное соглашение**.

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

О лицензии

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

Лицензия включает в себя право на получение следующих видов услуг:

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

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

В программе предусмотрены следующие типы лицензий:

- NFR (not for resale / не для перепродажи) – бесплатная лицензия на определенный период, предназначенная для ознакомления с программой и тестовых развертываний программы.
- Коммерческая – платная лицензия, предоставляемая при приобретении программы.

По истечении срока действия лицензии программа продолжает работу, но с ограниченной функциональностью. Чтобы использовать программу в режиме полной функциональности, вам нужно приобрести коммерческую лицензию или продлить срок действия коммерческой лицензии.

В текущей версии программы функциональность программы также зависит от типа установленного ключа.

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 программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

kaspersky

О ключе

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

► *Чтобы добавить ключ в программу,*

загрузите файл ключа.

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

О файле ключа

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

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

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

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

Для восстановления файла ключа обратитесь к продавцу лицензии.

Просмотр информации о лицензии и добавленных ключах

В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy вы можете просматривать информацию о лицензии и добавленных ключах в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса программы.

► *Чтобы просмотреть информацию о лицензии и добавленных ключах,*

в веб-интерфейсе сервера с компонентом Central Node выберите раздел **Параметры**, подраздел **Лицензия**.

В веб-интерфейсе отображается следующая информация о лицензии и добавленных ключах:

- серийный номер лицензии;
- дата активации программы;
- дата окончания срока действия лицензии;
- количество дней до окончания срока действия лицензии.

За 30 дней до окончания срока действия лицензии в разделе **Мониторинг** появляется уведомление о

необходимости продлить лицензию. Это уведомление отображается на всех серверах с компонентом Central Node (в режиме распределенного решения и multitenancy – на PCN и всех подключенных SCN) для всех пользователей независимо от их роли.

Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node

В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy вы можете просматривать текст Лицензионного соглашения в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса программы.

► *Чтобы просмотреть текст Лицензионного соглашения, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:*

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Лицензионное соглашение** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите текст Лицензионного соглашения.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр текста Политики конфиденциальности в веб-интерфейсе Central Node

В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy вы можете просматривать текст Политики конфиденциальности в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса программы.

► *Чтобы просмотреть текст Политики конфиденциальности, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:*

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Политика конфиденциальности** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите текст Политики конфиденциальности.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр информации о стороннем коде, используемом в программе

В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy вы можете просматривать информацию о стороннем коде, используемом в программе, в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального

администратора, администратора или пользователей веб-интерфейса программы.

► *Чтобы просмотреть информацию о стороннем коде, выполните следующие действия в веб-интерфейсе сервера с компонентом Central Node:*

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Сторонний код** в правом верхнем углу рабочей области.
3. В открывшемся окне просмотрите информацию о стороннем коде.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр текста Лицензионного соглашения в веб-интерфейсе Sandbox

► *Чтобы просмотреть текст Лицензионного соглашения в веб-интерфейсе сервера с компонентом Sandbox (см. раздел "Работа с компонентом Sandbox через веб-интерфейс" на стр. 156), выполните следующие действия:*

1. Войдите в веб-интерфейс Sandbox под учетными данными, которые вы задали при установке компонента Sandbox.
2. Нажмите на кнопку  в левой нижней части окна веб-интерфейса.
3. Откроется окно с информацией о компоненте Sandbox.
4. По ссылке **Лицензионное соглашение** раскройте окно с текстом Лицензионного соглашения программы.
5. Просмотрите текст Лицензионного соглашения.
6. По окончании просмотра нажмите на кнопку ×.

Просмотр текста Лицензионного соглашения на компьютере с Endpoint Agent

На каждом компьютере, на котором установлен отдельный компонент Endoint Agent, файл с Лицензионным соглашением находится в папке EULA в той директории, в которой установлен компонент Endpoint Agent.

Добавление ключа

В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) добавление ключа доступно только на сервере PCN.

► *Чтобы добавить ключ, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Лицензия**.
2. Выберите тип ключа: **KEDR**.
3. В разделе с выбранным типом ключа нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл ключа, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Ключ будет добавлен в программу.

Замена ключа

В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) замена ключа доступна только на сервере PCN.

► *Чтобы заменить активный ключ программы другим ключом, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Лицензия**.
2. Выберите тип ключа: **KEDR**.
3. В разделе с выбранным типом ключа нажмите на кнопку **Заменить**.

   Откроется окно выбора файлов.
4. Выберите файл ключа, которым вы хотите заменить активный ключ, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Загруженный ключ заменит активный ключ программы.

Удаление ключа

В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) удаление ключа доступно только на сервере PCN.

► *Чтобы удалить ключ, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Лицензия**.
2. Выберите тип ключа: **KEDR**.
3. В разделе с выбранным типом ключа нажмите на кнопку **Удалить**.

Откроется окно подтверждения удаления ключа.

4. Нажмите на кнопку **Да**.

   Окно подтверждения удаления ключа закроется.

Ключ будет удален.

Режимы работы программы в соответствии с лицензией

В программе предусмотрены различные режимы работы программы в зависимости от добавленных ключей.

Без лицензии

В этом режиме программа работает с момента установки программы и запуска веб-интерфейса до тех пор, пока вы не добавите ключ.

В режиме Без лицензии действуют следующие ограничения:

- Не обновляются базы программы.
- Отсутствует подключение к базе знаний Kaspersky Security Network.
- Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **Правила пользователей**, **Хранилище**, **Endpoint Agents**.

Коммерческая лицензия

В этом режиме программа подключается к базе знаний Kaspersky Security Network и обновляет базы.

По истечении срока годности ключа для коммерческой лицензии программа прекращает обновление баз и не подключается к базе знаний Kaspersky Security Network.

Для возобновления работы программы необходимо заменить ключ или добавить новый ключ для коммерческой лицензии.

kaspersky

Архитектура программы

В состав программы входят следующие основные компоненты:

- *Central Node*. Выполняет проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс программы.
- *Sandbox*. Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации.
- *Endpoint Agent.* Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.
- Sensor. Может использоваться в качестве прокси-сервера при обмене данными между компонентами Endpoint Agent и компонентом Central Node, чтобы снизить нагрузку на компонент Central Node.

В этом разделе

Компонент Central Node

На каждом сервере с компонентом Central Node работают следующие модули, ядра и технологии Kaspersky Endpoint Detection and Response:

- *Anti-Malware Engine* (далее также *AM* и *AM Engine*). Выполняет проверку файлов и объектов на вирусы и другие программы, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.
- *Mobile Attack Analyzer* (далее также *MAA*). Выполняет проверку исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения. В результате проверки Kaspersky Endpoint Detection and Response получает информацию об обнаруженных угрозах или их отсутствии.
- *YARA*. Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями программы.
- *Targeted Attack Analyzer* (далее также *TAA*, *TA Analyzer*). Выполняет статистический анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации. Выполняет поиск признаков сетевой активности, на которую пользователю программы рекомендуется обратить внимание, а также признаков целевых атак на IT-инфраструктуру организации.

- *KSN*. Выполняет проверку репутации файлов и URL-адресов в базе знаний Kaspersky Security Network и предоставляет сведения о категориях веб-сайтов (например, вредоносный веб-сайт, фишинговый веб-сайт).

Компонент Sandbox

На серверах с компонентом Sandbox запускаются виртуальные образы следующих операционных систем:

- Windows XP SP3, 32-разрядная.
- Windows 7, 64-разрядная.
- Windows 10, 64-разрядная.

Компонент Sandbox запускает объекты в этих операционных системах и анализирует поведение объектов для выявления вредоносной активности, признаков целевых атак на IT-инфраструктуру организации.

По умолчанию максимальный размер проверяемого файла составляет 100 Мб. Вы можете настроить параметры проверки в меню администратора консоли управления программой.
Максимальный уровень вложенности проверяемых архивов составляет 32.
Максимальное количество объектов, которое может находиться в очереди на проверку компонентом Sandbox за одни сутки, составляет 10 тысяч объектов. По достижении этого ограничения программа удаляет 10% объектов, поступивших на проверку раньше остальных, и заменяет их новыми объектами, поступившими на проверку. Удаленные объекты сохраняются в программе со статусом NOT_SCANNED (непроверенные).

Компонент Endpoint Agent

Компонент Endpoint Agent устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации и работающих под управлением операционной системы Microsoft Windows (далее также "компьютеры локальной сети организации" или "компьютеры"). На этих компьютерах компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляет данные наблюдения на сервер с компонентом Central Node.

Компьютеры, предназначенные для установки компонента Endpoint Agent, должны удовлетворять аппаратным и программным требованиям.

В качестве компонента Endpoint Agent также может использоваться компонент программы "Лаборатории Касперского" Kaspersky Endpoint Security. Endpoint Agent в составе программы Kaspersky Endpoint Security могут наблюдать за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправлять данные наблюдения на сервер с компонентом Central Node.

Если вы установите программу Kaspersky Endpoint Security на компьютер с компонентом Endpoint Sensor, компонент Endpoint Sensor будет удален независимо от того, включен ли компонент Endpoint Sensor в состав программы Kaspersky Endpoint Security или нет.

Кроме того, Kaspersky Endpoint Detection and Response позволяет интегрироваться с программой Kaspersky Security Center и получать статистику работы компонента Endpoint Agent.

Принцип работы программы

После интеграции в IT-инфраструктуру организации программа публикует информацию об обнаруженных признаках целевых атак и вторжений в IT-инфраструктуру организации в веб-интерфейс.

Вы можете настраивать параметры каждого компонента Central Node отдельно или управлять несколькими компонентами централизованно в режиме распределенного решения.

Принцип работы программы показан на рис. ниже.

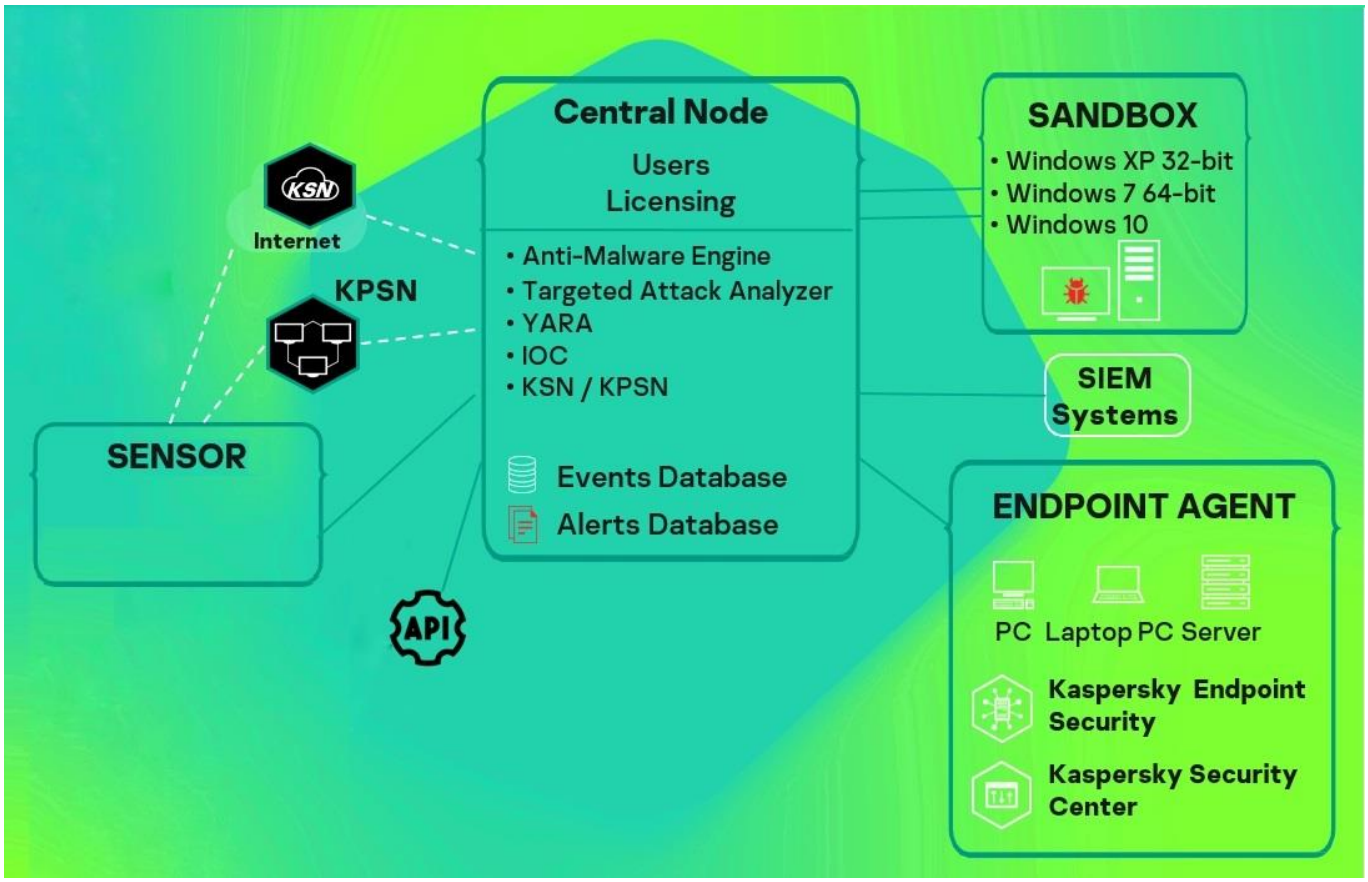

Рисунок 1: Принцип работы программы в режиме автономного решения

Распределенное решение (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) представляет собой двухуровневую иерархию серверов Central Node. В этой структуре выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*.

kaspersky

Распределенное решение и режим multitenancy

Вы можете настраивать параметры каждого компонента Central Node отдельно или управлять несколькими компонентами централизованно в режиме распределенного решения.

Распределенное решение представляет собой двухуровневую иерархию серверов с установленными компонентами Central Node. В этой структуре выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*. Для взаимодействия серверов необходимо подключить SCN к PCN.

PCN и SCN осуществляют проверку файлов и объектов с помощью тех же технологий, что и компонент Central Node, управляемый отдельно.

В распределенном решении вы можете централизованно управлять следующими функциональными областями программы:

- Пользователи.
- Обнаружения.
- Поиск угроз.
- Задачи.
- Политики.
- Правила пользователей.
- Хранилище.
- Endpoint Agents, в том числе сетевая изоляция хостов.
- Отчеты.

Если вы поддерживаете несколько организаций, вы можете работать с программой в режиме multitenancy. Вы можете установить Kaspersky Endpoint Detection and Response на один или несколько серверов Central Node для каждой организации. У каждой организации есть свой сервер PCN и подключенные к нему серверы SCN. Каждая организация может работать с программой независимо от других организаций. Организация-провайдер может работать с данными нескольких организаций.

Количество одновременных сеансов работы с программой под одной учетной записью ограничено одним IP-адресом. При попытке входа в программу под этим же именем пользователя с другого IP-адреса, первый сеанс работы с программой завершается.

Если вы используете режим распределенного решения и multitenancy, ограничение действует для каждого сервера PCN и SCN независимо друг от друга.

Вы можете использовать распределенное решение и режим multitenancy в следующих случаях:

- для защиты более 10 000 хостов организации;
- для централизованного управления программой в разных подразделениях организации;
- для централизованного управления программой на серверах нескольких организаций.

kaspersky

При переключении программы в режим распределенного решения и multitenancy управление лицензионными ключами становится доступно только на PCN. На SCN все ранее добавленные ключи удаляются. Каждый подключенный SCN получает ключ от PCN.

Вы можете развернуть программу в режиме распределенного решения и multitenancy по следующим сценариям:

- Установить компонент Central Node на новых серверах и назначить этим серверам роли PCN и SCN.
- Назначить роли PCN и SCN серверам с ранее установленным компонентом Central Node.

  В этом случае вам требуется обновить компонент Central Node до версии 3.7.

  Перед переключением серверов с установленными компонентами Central Node в режим распределенного решения ознакомьтесь с изменениями, которые произойдут в системе после смены режима работы. Назначение серверу роли PCN является необратимым.

В этом разделе

Сценарий перехода в режим распределенного решения и multitenancy

Переход программы в режим распределенного решения и режим multitenancy содержит следующие этапы:

a. **Установка компонентов Central Node (см. раздел "Установка и настройка компонента Central Node" на стр. 102)**

b. **Назначение одному из серверов роли PCN (см. раздел "Назначение серверу роли PCN" на**

стр. 81)

c. **Назначение остальным серверам роли SCN и отправка запросов на подключение к PCN (см. раздел "Назначение серверу роли SCN" на стр. 82)**

d. **Обработка запроса на подключение SCN к PCN (см. раздел "Обработка запросов на подключение SCN к PCN" на стр. 82)**

Изменения в параметрах программы при переходе в режим распределенного решения и multitenancy

Изменения в параметрах программы при переключении в режим распределенного решения и режим multitenancy приведены в таблице ниже.

Таблица 8. Изменения в параметрах программы при переключении в режим распределенного решения и multitenancy

Функциональная область	PCN	SCN
Пользователи	Пользователи и назначенные им роли сохраняются. Дополнительно пользователям PCN выдаются права на работу с PCN и всеми подключенными SCN.	Удаляются все пользователи, кроме пользователя, созданного в момент развертывания Central Node. После этого SCN запрашивает у PCN список пользователей и на основе этого списка создает локальных пользователей с такими же параметрами: • имя; • пароль; • роль; • статус. Пользователи, не имеющие прав на доступ к SCN, не отображаются в списке пользователей.
Обнаружения	В базу PCN добавляется информация об обнаружениях со всех подключенных SCN.	В информации об уже имеющихся обнаружениях перестает отображаться имя пользователя. Данные о пользователях удаляются из истории операций с обнаружением.

Функциональная область	PCN	SCN
Мониторинг	На закладке **Обнаружения** появляется возможность выбрать SCN, информация о которых должна быть отражена на графике. На закладке **Работоспособность системы** появляется статус соединения PCN с подключенными SCN.	На закладке **Работоспособность системы** появляется статус соединения с PCN.
Задачи	Задачи, созданные на сервере Central Node до назначения ему роли PCN, а также задачи, создаваемые на PCN после перехода в режим распределенного решения, распространяются на все подключенные SCN. В списке задач также отображаются задачи, созданные на SCN. Изменение параметров этих задач на PCN недоступно.	Отображаются задачи, созданные на PCN, а также задачи, созданные на этом SCN. Изменение параметров задач, созданных на PCN, недоступно.
Отчеты	Шаблоны и отчеты, созданные до переключения в режим распределенного решения, сохраняются. В таблице отчетов появляется графа **Серверы** с информацией о SCN, к которому относится обнаружение. После переключения в режим распределенного решения отображаются только отчеты, созданные на PCN.	Шаблоны и отчеты, созданные до переключения в режим распределенного решения, сохраняются. Информация о пользователе, создавшем отчет, сохраняется, если на PCN есть пользователь с таким же идентификатором (guid). В остальных случаях информация о пользователе удаляется. После переключения в режим распределенного решения отображаются только отчеты, созданные на SCN.

Функциональная область	PCN	SCN
Политики	Политики, созданные на сервере Central Node до назначения ему роли PCN, а также политики, создаваемые на PCN после перехода в режим распределенного решения, распространяются на все подключенные SCN. В списке политик также отображаются политики, созданные на SCN. Изменение параметров этих политик на PCN недоступно.	Отображаются политики, созданные на PCN, а также политики, созданные на этом SCN. Изменение параметров политик, созданных на PCN, недоступно.
Хранилище	Все файлы и метаданные, которые хранились на PCN до перехода в режим распределенного решения, сохраняются. В графе **Central Node** для них отображается имя PCN. На PCN также сохраняется содержимое Хранилища всех подключенных SCN.	Все файлы и метаданные, которые хранились на SCN до перехода в режим распределенного решения, сохраняются.
Исключения TAA	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Отправка уведомлений	Изменений нет.	Изменений нет.
Интеграция с Kaspersky Security Center	Интеграция с Kaspersky Security Center становится недоступна.	Интеграция с Kaspersky Security Center становится недоступна.
Поиск угроз	При поиске угроз по базе событий PCN отправляет запрос на все подключенные SCN. В результате обработки поискового запроса отображается список событий PCN и SCN выбранной организации.	Изменений нет.
Правила пользователей - TAA	IOC-файлы, добавленные на сервере Central Node до назначения ему роли PCN, распространяются на PCN. TAA (IOA)-правила, добавленные на сервере Central Node до назначения ему роли PCN, распространяются на PCN.	Отображаются IOC-файлы и TAA (IOA)-правила, добавляемые на PCN, а также IOC-файлы и TAA (IOA)-правила, добавляемые на этом SCN до и после перехода в режим распределенного решения.

Функциональная область	PCN	SCN
Резервное копирование программы	Резервное копирование программы доступно только на PCN, к которому не подключены SCN. Чтобы сделать резервное копирование программы на PCN, необходимо отключить все SCN от этого PCN.	Резервное копирование программы на SCN недоступно. Чтобы сделать резервное копирование программы на SCN, необходимо отключить этот сервер от PCN, переведя его в режим отдельного сервера.

Назначение серверу роли PCN

Назначение серверу роли PCN необратимо. После изменения роли сервера на PCN вы не сможете изменить роль этого сервера на SCN или отдельный сервер. Если вы захотите изменить роль этого сервера снова, вам потребуется переустановить программу.

► *Чтобы назначить серверу роль PCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера, которому вы хотите назначить роль PCN.
2. Выберите раздел **Режим работы**.
3. Нажмите на кнопку **Распределенное решение**.
4. В раскрывающемся списке **Роль сервера** выберите **Primary Central Node**.
5. В поле **Название организации** введите название организации, к которой относится этот сервер Central Node.
6. Нажмите на кнопку **Назначить роль PCN**.

   Откроется окно подтверждения действия.

   После подтверждения действия вам потребуется снова войти в веб-интерфейс программы.
7. Нажмите на кнопку **Да**.

Серверу будет назначена роль PCN и присвоено название организации.

После того, как вы снова войдете в веб-интерфейс программы под учетной записью администратора, в окне веб-интерфейса программы в разделе **Режим работы** отобразится следующая информация:

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера, необходимый для проверки подлинности при установке соединения с SCN.

- **Организации** – информация об организациях, к которым относится этот сервер, и о подключенных серверах SCN:
  - **IP** – Primary Central Node для этого сервера и IP-адреса серверов SCN (после их подключения).
  - **Сервер** – имя этого сервера и имена серверов SCN (после их подключения).

    Это имя не связано с именем хоста, на котором установлена программа. Вы можете его изменить.
  - **Отпечаток сертификата** – пустое значение для этого сервера и отпечатки сертификатов серверов SCN (после их подключения).
  - **Состояние** – состояние подключения серверов SCN (после их подключения), а также количество серверов организации.
- Таблица **Серверы, ожидающие авторизации** с информацией о подключенных SCN (см. раздел "Просмотр информации об организациях, серверах PCN и SCN" на стр. 83).

Назначение серверу роли SCN

► *Чтобы назначить серверу роль SCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера, которому вы хотите назначить роль SCN.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. Нажмите на кнопку **Распределенное решение**.
4. В раскрывающемся списке **Роль сервера** выберите **Secondary Central Node**.
5. В поле **IP-адрес сервера PCN** укажите IP-адрес сервера с ролью PCN, к которому вы хотите подключить SCN.
6. Нажмите на кнопку **Получить отпечаток сертификата**.

   В рабочей области отобразится отпечаток сертификата сервера с ролью PCN.
7. Свяжитесь с администратором PCN и сравните полученный отпечаток сертификата с отпечатком, указанным на PCN в разделе **Режим работы** в поле **Отпечаток сертификата**.
8. Если отпечатки сертификата на SCN и PCN совпадают, нажмите на кнопку **Отправить запрос на подключение**.

   Откроется окно подтверждения действия.
9. Нажмите на кнопку **Да**.

Серверу будет назначена роль SCN после того, как администратор PCN примет запрос на подключение. Сервер SCN будет относиться к той организации, которую укажет администратор PCN.

Обработка запросов на подключение SCN к PCN

► *Чтобы обработать запрос на подключение SCN к PCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

Вам нужно войти в веб-интерфейс того сервера PCN, на котором вы хотите обработать запросы на подключение от других серверов.

2. В окне веб-интерфейса программы выберите раздел **Режим работы**.

   В рабочей области отобразится таблица **Серверы, ожидающие авторизации**.

3. Свяжитесь с администратором SCN, отправившим запрос на подключение, и проверьте отпечаток сертификата в таблице **Серверы, ожидающие авторизации**. Он должен совпадать с отпечатком, отображаемым на SCN в разделе **Режим работы** в поле **Отпечаток сертификата из запроса**.

4. Если отпечатки сертификата на PCN и SCN совпадают, выполните одно из следующих действий:

   - Если вы хотите отклонить запрос на подключение от SCN, нажмите на кнопку **Отклонить**.
   - Если вы хотите принять запрос на подключение от SCN, выполните следующие действия:

     1. Нажмите на кнопу **Принять**.

        Откроется окно **Принять запрос на подключение**.

     2. В списке **Организация** выберите организацию, которой вы хотите назначить этот сервер SCN. Список формируется из организаций, добавленных ранее (см. раздел "Добавление организации на сервере PCN" на стр. 84).

     3. Нажмите на кнопку **Принять**.

Не рекомендуется принимать запросы на подключение при несовпадении отпечатков сертификата. Убедитесь в правильности введенных данных.

Если вы отклонили запрос на подключение, SCN продолжит работу в режиме отдельного сервера Central Node.

Просмотр информации об организациях, серверах PCN и SCN

В веб-интерфейсе сервера PCN вы можете просмотреть информацию об этом сервере, а также о всех серверах SCN, которые к нему подключены.

► *Чтобы просмотреть информацию об организациях, серверах PCN и SCN в режиме multitenancy, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN.

2. В окне веб-интерфейса программы выберите раздел **Режим работы**.

В рабочей области отобразится следующая информация об организациях и серверах:

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера PCN.
- **Организации** – информация об организациях, к которым относится этот сервер, а также все

серверы SCN, подключенные к PCN.

- **IP** – Primary Central Node для сервера PCN и IP-адреса серверов SCN, подключенных к PCN.
- **Сервер** – имя этого сервера и имена серверов SCN, подключенных к PCN.

  Это имя не связано с именем хоста, на котором установлена программа. Вы можете его изменить.
- **Отпечаток сертификата** – пустое значение для сервера PCN и отпечатки сертификатов серверов SCN, которые ожидают подключения к PCN.
- **Состояние** – состояние подключения, а также количество серверов организации.

- Таблица **Серверы, ожидающие авторизации** со следующей информацией:
  - **IP** – IP-адрес или доменное имя сервера SCN.
  - **Сервер** – имя сервера SCN, которое отображается в веб-интерфейсе программы.

    Это имя не связано с именем хоста, на котором установлена программа. Вы можете его изменить.
  - **Отпечаток сертификата** – отпечаток сертификата сервера SCN, передаваемый на PCN вместе с запросом на подключение.
  - **Состояние** – статус подключения SCN к PCN.

Добавление организации на сервере PCN

► *Чтобы добавить организацию в веб-интерфейсе сервера PCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Вам нужно войти в веб-интерфейс того сервера PCN, для которого вы хотите добавить организацию.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. В правой части рабочей области **Организации** нажмите на кнопку **Добавить**.
4. В поле **Имя** введите название организации, которую вы хотите добавить.
5. Нажмите на кнопку **Добавить**.

Организация будет добавлена и отобразится в списке.

Удаление организации на сервере PCN

► *Чтобы удалить организацию в веб-интерфейсе сервера PCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите удалить организацию.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.

3. В рабочей области **Организации** выберите организацию, которую вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

   Действие необратимо. Все глобальные объекты, а также отчеты и шаблоны отчетов, связанные с этой организацией, будут потеряны.

5. Нажмите на кнопку **Да**.

Организация будет удалена.

Изменение названия организации на сервере PCN

► *Чтобы изменить название организации в веб-интерфейсе сервера PCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите изменить название организации.

2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. В списке **Организации** нажмите на значок справа от названия организации, которое вы хотите изменить.

   Откроется окно изменения названия организации.

4. В поле **Имя** измените название организации.
5. Нажмите на кнопку **Сохранить**.

Название организации будет изменено.

Отключение SCN от PCN

Отключение SCN от PCN может быть односторонним.

Если вы отключите SCN через веб-интерфейс SCN, то изменения в параметрах будут применены только на SCN. На PCN по-прежнему будет отображаться информация об этом сервере.

Если вы отключите SCN через веб-интерфейс PCN, то информация об этом сервере будет удалена на PCN. Однако сервер с ролью SCN будет пытаться подключиться к PCN для синхронизации параметров.

Для двустороннего отключения необходимо выполнить обе инструкции, приведенные ниже. В этом случае SCN продолжит работать как отдельный сервер Central Node, на PCN будет отображаться информация об отключенном SCN.

Администратор Kaspersky Endpoint Detection and Response несет ответственность за сохранность конфиденциальных данных на серверах PCN, SCN и Central Node. Если вы планируете передать сервер SCN от одной организации другой, необходимо удалить все данные, оставшиеся на сервере после использования Kaspersky Endpoint Detection and Response и переустановить Kaspersky Endpoint Detection and Response перед передачей сервера другой организации.

► *Чтобы отключить SCN от PCN через веб-интерфейс PCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Войдите в веб-интерфейс того сервера PCN, от которого вы хотите отключить SCN.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. В списке серверов выберите SCN, который вы хотите отключить.
4. Нажмите на кнопку **Отключить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

SCN будет пытаться подключиться к PCN для синхронизации параметров.

► *Чтобы отключить SCN от PCN через веб-интерфейс SCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Войдите в веб-интерфейс того сервера SCN, который вы хотите отключить от PCN.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. Нажмите на кнопку **Отключить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

SCN будет отключен от PCN и продолжит работать как отдельный сервер Central Node.

Изменения в параметрах программы при отключении SCN от PCN

Изменения в параметрах программы после отключения SCN от PCN представлены в таблице ниже.

Таблица 9. Изменения параметров программы после отключения SCN от PCN

Функциональная область	PCN	SCN
Пользователи	Отключенный SCN не исключается из списка серверов, на которые распространяются права пользователей. Информация об изменении учетной записи пользователя, имеющего права на отключенный SCN, не передается на SCN.	Учетные записи пользователей, полученные с PCN, не удаляются. Появляется возможность создания новых учетных записей пользователей, а также отключения и смены пароля существующих учетных записей.
Обнаружения	Информация об обнаружениях на отключенном SCN удаляется.	История операций и вся информация об обнаружениях сохраняется.
Задачи	Задачи, созданные на отключенном SCN, удаляются.	Задачи, созданные на PCN, удаляются. Информация о пользователях, создавших задачи на SCN, сохраняется.
Отчеты	Все созданные ранее отчеты об отключенном SCN, а также возможность фильтровать список отчетов по этому серверу, сохраняются.	Шаблоны и отчеты не изменяются.
Политики	Политики, созданные на отключенном SCN, удаляются.	Политики, созданные на PCN, удаляются. Информация о пользователях, создавших политики на SCN, сохраняется.
Хранилище	Из Хранилища удаляются все объекты, относящиеся к отключенному SCN.	Все объекты в Хранилище сохраняются. В информации об объектах, полученных в рамках задач, созданных на PCN, перестает работать ссылка на задачу.
Исключения ТАА	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Отправка уведомлений	Изменений нет.	Изменений нет.
Интеграция с почтовыми сенсорами	Изменений нет.	Изменений нет.
Интеграция с Kaspersky Security Center	Настройка интеграции с Kaspersky Security Center остается недоступной.	Настройка интеграции с Kaspersky Security Center становится доступна.

Функциональная область	PCN	SCN
Поиск угроз	В результате обработки поискового запроса события, связанные с отключенным SCN, не отображаются.	Изменений нет.
Правила пользователей - TAA и IOC	IOC- и TAA (IOA)-правила отключенного SCN удаляются.	IOC- и TAA (IOA)-правила, созданные на PCN, удаляются.
Резервное копирование программы	Резервное копирование программы остается недоступным.	Резервное копирование программы становится доступным.

Вывод сервера SCN из эксплуатации

Если вы не планируете в дальнейшем использовать сервер SCN, вы можете вывести сервер SCN из эксплуатации программой, удалив его на PCN.

Администратор Kaspersky Endpoint Detection and Response несет ответственность за сохранность конфиденциальных данных на серверах PCN, SCN и Central Node. Если вы планируете передать сервер SCN от одной организации другой, необходимо удалить все данные, оставшиеся на сервере после использования Kaspersky Endpoint Detection and Response и переустановить Kaspersky Endpoint Detection and Response перед передачей сервера другой организации.

Вывод сервера SCN из эксплуатации программой состоит из следующих этапов:

a. **Удаление всех данных на SCN**

b. **Отключение SCN от PCN через веб-интерфейс PCN (см. раздел "Отключение SCN от PCN" на стр. 85)**

c. **Отключение SCN от PCN через веб-интерфейс SCN (см. раздел "Отключение SCN от PCN" на стр. 85)**

d. **Удаление SCN через веб-интерфейс PCN**

► *Чтобы удалить SCN через веб-интерфейс PCN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.

   Войдите в веб-интерфейс того сервера PCN, на котором вы хотите удалить SCN.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. В списке серверов выберите SCN, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.
5. В окне подтверждения нажмите на кнопку **Да**.

SCN будет удален. На PCN не будут отображаться сведения об удаленном SCN.

kaspersky

Руководство по масштабированию

Для достижения и сохранения оптимальной производительности при различных условиях работы программы требуется учитывать количество устройств в сети, топологию сети и необходимую вам функциональность программы.

Выбор оптимальной конфигурации программы состоит из следующих этапов:

1. Выбор типовой схемы развертывания
2. Расчет аппаратных требований с помощью калькулятора масштабирования

Типовые схемы развертывания и установки компонентов программы

Схема развертывания и установки компонентов программы определяется планируемой нагрузкой на серверы программы.

Компонент Endpoint Agent устанавливается на любых компьютерах, которые входят в IT-инфраструктуру организации и работают под управлением операционной системы Windows. На компьютерах с компонентом Endpoint Agent необходимо разрешить исходящее соединение с сервером с компонентом Central Node напрямую, без использования прокси-сервера.

Вы можете установить один или несколько компонентов Central Node. При установке нескольких компонентов Central Node вы можете использовать их независимо друг от друга или объединить для централизованного управления в режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76).

Выбор схемы развертывания зависит от используемой функциональности программы. Все приведенные в данном руководстве схемы применимы также для развертывания программы на виртуальной платформе.

Схема развертывания функциональности KEDR с компонентом Sandbox

Компонент Central Node всегда устанавливается вместе с компонентом Sensor. Если вам требуется использовать компонент Central Node отдельно, не выполняйте настройку компонента Sensor.

Схема работы программы при развертывании функциональности KEDR с компонентом Sandbox представлена на рис. ниже.

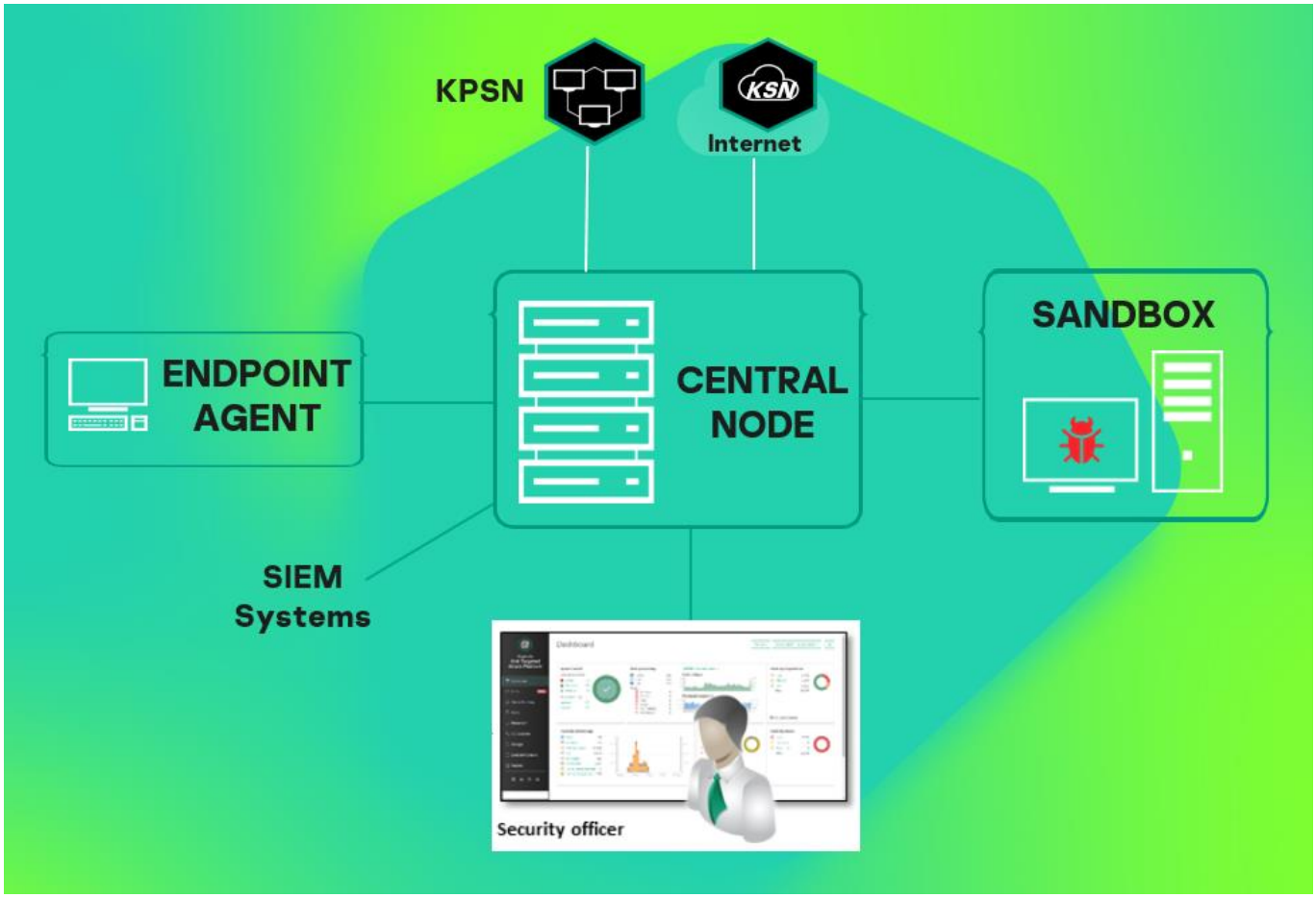

Рисунок 2: Схема работы программы при развертывании функциональности KEDR с компонентом Sandbox

kaspersky

Установка и первоначальная настройка решения

В этом разделе содержатся инструкции по установке и первоначальной настройке Kaspersky Endpoint Detection and Response.

В этом разделе

Подготовка к установке компонентов программы

В этом разделе представлена информация о том, как подготовить IT-инфраструктуру вашей организации к установке компонентов программы.

В этом разделе

Рекомендуется разрешить соединение с серверами Kaspersky Endpoint Detection and Response и с веб-интерфейсом Kaspersky Endpoint Detection and Response только для доверенных узлов и рабочих станций по их IP-адресу. Для недоверенных рабочих станций с компонентом Endpoint Agent достаточно разрешить соединение с сервером Central Node на порт 443. Вы можете настроить доступ по IP-адресам доверенных серверов средствами внешнего администрирования (например, настроить маршрутизатор или сетевой экран).

Подготовка IT-инфраструктуры к установке компонентов программы

► *Перед установкой программы подготовьте IT-инфраструктуру вашей организации к*

установке компонентов программы:

1. Убедитесь, что серверы, а также компьютер, предназначенный для работы с веб-интерфейсом программы, и компьютеры, на которых устанавливается компонент Endpoint Agent, удовлетворяют аппаратным и программным требованиям (см. стр. 24).
2. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Sandbox:
   a. Для обоих сетевых интерфейсов запретите доступ сервера с компонентом Sandbox в локальную сеть организации для обеспечения безопасности сети от анализируемых объектов.
   b. Для первого сетевого интерфейса разрешите доступ сервера с компонентом Sandbox в интернет для обновления баз и анализа поведения объектов.
   c. Для второго сетевого интерфейса разрешите входящее соединение сервера с компонентом Sandbox на следующие порты:
      - TCP 22 для подключения к серверу по протоколу SSH.
      - TCP 443 для получения объектов на проверку от компонента Central Node.
      - TCP 8443 для использования веб-интерфейса программы.
3. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Central Node:
   a. Разрешите входящее соединение сервера с компонентом Central Node на следующие порты:
      - TCP 22 для подключения к серверу по SSH.
      - TCP 8081 для получения данных от сервера с компонентом Sensor.
      - TCP 10000 для добавления метаданных в базу данных Targeted Attack Analyzer (если компонент Sensor устанавливается на отдельный сервер).
      - TCP 443 для получения данных от компьютеров с компонентом Endpoint Agent.
      - TCP 6379 для синхронизации с базой данных Redis на сервере с компонентом Sensor.
      - TCP 8443 для просмотра результатов проверки в веб-интерфейсе программы.
      - TCP 4443 при перенаправлении трафика от компонентов Endpoint Agent через сервер с компонентом Sensor на сервер с компонентом Central Node.
   b. Разрешите исходящее соединение сервера с компонентом Central Node на следующие порты:
      - UDP 161 для получения данных о состоянии компонента Sensor (если компонент Sensor устанавливается на отдельный сервер).
      - TCP 80 и 443 для связи с серверами службы KSN и серверами обновлений "Лаборатории Касперского".
      - TCP 443 для передачи объектов на проверку компоненту Sandbox.
      - TCP 601 для отправки сообщений в SIEM-систему.
4. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Sensor:
   a. Для сетевого интерфейса, используемого для интеграции с прокси-сервером и почтовым сервером, разрешите входящее соединение сервера с компонентом Sensor на следующие порты:

- TCP 22 для подключения к серверу по SSH.
- TCP 1344 для получения трафика от прокси-сервера.
- TCP 25 для получения SMTP-трафика от почтового сервера.
- TCP 443 при перенаправлении трафика от компонентов Endpoint Agent на сервер с компонентом Central Node.
- UDP 161 для передачи данных о состоянии компонентов и их баз на сервер с компонентом Central Node.

b. Разрешите исходящее соединение сервера с компонентом Sensor на следующие порты:

- TCP 8081 для передачи объектов на сервер с компонентом Central Node.
- TCP 80 и 443 для связи с серверами службы KSN и серверами обновлений "Лаборатории Касперского".
- TCP 6379 для синхронизации с базой данных Redis на сервере с компонентом Central Node.
- TCP 995 (или TCP 110 для незащищенных соединений) для интеграции с почтовым сервером.
- TCP 4443 при перенаправлении трафика от компонентов Endpoint Agent на сервер с компонентом Central Node.

5. Разрешите входящее соединение компьютеров с компонентом Endpoint Agent и сервера с компонентом Central Node напрямую, без использования прокси-сервера.
6. Разрешите на сетевом оборудовании шифрованный канал связи между серверами с компонентами Central Node и Sensor.

   Соединение между серверами с компонентами Central Node и Sensor происходит внутри шифрованного канала связи на базе IPSec с использованием протокола ESP.
7. Если вы используете режим распределенного решения и multitenancy, произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонентов Central Node:

   a. Разрешите входящее соединение сервера с ролью PCN на порты 8444 и 5432.

   b. Разрешите входящее соединение сервера с ролью SCN на порт 5432.

   c. Разрешите на сетевом оборудовании установку шифрованного канала связи между серверами с компонентами Central Node и Sensor.

      Соединение между серверами с ролью PCN и SCN происходит внутри шифрованного канала связи на базе IPSec с использованием протокола ESP.

При необходимости вы можете назначить другие порты для работы компонентов программы в меню администратора сервера с компонентом Central Node. При изменении портов в меню администратора вам нужно разрешить соединения на эти порты внутри IT-инфраструктуры вашей организации.

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3

Если в качестве почтового сервера вы используете почтовый сервер Microsoft Exchange и отправитель настроил запрос уведомления о прочтении сообщения электронной почты, то необходимо отключить

отправку уведомлений о прочтении. В противном случае уведомления о прочтении будут отправляться с того адреса электронной почты, который вы настроили в качестве адреса электронной почты для приема сообщений Kaspersky Endpoint Detection and Response. Также необходимо отключить автоматическую обработку приглашений на встречи для предотвращения заполнения почтового ящика для приема сообщений Kaspersky Endpoint Detection and Response.

► *Чтобы отключить отправку уведомлений о прочтении с адреса электронной почты для приема сообщений Kaspersky Endpoint Detection and Response, выполните следующие действия:*

1. На сервере Microsoft Exchange проверьте, включена ли отправка уведомлений. Для этого выполните команду:

   ```
   Get-MailboxMessageConfiguration -Identity <адрес электронной почты для приема сообщений Kaspersky Endpoint Detection and Response> | fl
   ```

2. Если отправка уведомлений включена, выполните команду:

   ```
   Set-MailboxMessageConfiguration -Identity <адрес электронной почты для приема сообщений Kaspersky Endpoint Detection and Response> -ReadReceiptResponse NeverSend
   ```

Отправка уведомлений о прочтении с адреса электронной почты для приема сообщений будет отключена.

► *Чтобы отключить автоматическую обработку приглашений на встречи, выполните следующие действия:*

1. На сервере Microsoft Exchange проверьте, включена ли отправка уведомлений. Для этого выполните команду:

   ```
   Get-CalendarProcessing -Identity <адрес электронной почты для приема сообщений Kaspersky Endpoint Detection and Response> | fl
   ```

2. Если автоматическая обработка приглашений на встречи включена, выполните команду:

   ```
   Set-CalendarProcessing -Identity <адрес электронной почты для приема сообщений Kaspersky Endpoint Detection and Response> -AutomateProcessing:None
   ```

Автоматическая обработка приглашений на встречи будет отключена.

Подготовка виртуальной машины к установке компонента Sandbox

► *Чтобы подготовить виртуальную машину к установке компонента Sandbox, выполните следующие действия:*

1. Запустите гипервизор. Например, Vmware ESXi.
2. Откройте консоль для управления виртуальными машинами.
3. В контекстном меню виртуальной машины, на которой вы хотите установить компонент Sandbox, выберите пункт **Edit Settings**.

   Откроется окно свойств виртуальной машины.

4. На закладке **Virtual Hardware** раскройте блок параметров **CPU** и установите флажок **Expose**

hardware-assisted virtualization to guest OS.

5. На закладке **VM Options** в раскрывающемся списке **Latency Sensitivity** выберите **High**.
6. Нажмите на кнопку **OK**.

Виртуальная машина будет готова к установке компонента Sandbox.

Порядок установки и настройки компонентов программы

Выполняйте действия по установке и настройке программы в следующем порядке:

1. Установите компонент Sandbox:

   a. Установите базовую систему с образа диска sandbox-3.7.0-187-inst.x86_64_en-ru.iso.

   b. Перезагрузите установленную систему.

   c. Войдите в систему под учетной записью `root` с паролем `123456`.

   d. Примонтируйте образ диска sandbox-3.7.0-187-addon.x86_64_en-ru.iso.

   e. Выполните скрипт install-addon, расположенный в корневой папке примонтированного образа.

2. Настройте компонент Sandbox. Мастер настройки запустится автоматически при выполнении скрипта. После установки компонента Sandbox дальнейшая его настройка возможна через веб-интерфейс.

   e. **3. Установите образы дисков операционных систем Microsoft Windows и программ для работы компонента Sandbox (см. раздел "Установка и настройка образов операционных систем и программ для работы компонента Sandbox" на стр. 166).**

4. Установите компоненты Central Node и Sensor:

   a. Установите базовую систему с образа диска kata-cn-3.7.0-713-inst.x86_64_en-ru.iso.

   b. Перезагрузите установленную систему.

   c. Войдите в систему под учетной записью `root` с паролем `123456`.

   d. Примонтируйте образ диска kata-cn-3.7.0-713-addon.x86_64_en-ru.iso.

   e. Выполните скрипт install-addon, расположенный в корневой папке примонтированного образа.

5. Настройте компоненты Central Node и Sensor. Мастер настройки запустится автоматически после перезагрузки системы.

   При наличии нескольких компонентов Central Node вы можете использовать программу в режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76).

   При наличии нескольких компонентов Sensor вы можете установить и настроить компонент Sensor на необходимом количестве серверов.

   При необходимости использования компонента Central Node отдельно от компонента Sensor пропускайте шаги по настройке компонента Sensor при установке компонентов Central Node и Sensor (см. раздел "Установка и настройка компонентов Central Node и Sensor на одном сервере" на стр. 102).

   f. 6. Установите компонент Endpoint Agent на компьютерах, входящих в IT-инфраструктуру

организации, запустив инсталляционный пакет `endpointagent.msi`.

kaspersky

Установка компонента Sandbox

Этот раздел представляет собой пошаговую инструкцию по установке компонента Sandbox.

► *Чтобы приступить к установке компонента Sandbox, выполните следующие действия:*

1. Запустите образ диска с компонентом Sandbox.

   Запустится мастер установки.
2. Нажмите на кнопку **Ok**.

В этом разделе

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно просмотреть Лицензионное соглашение и принять его условия. Если условия Лицензионного соглашения не приняты, установка не выполняется.

Также вам нужно просмотреть Политику конфиденциальности и принять ее условия.

► *Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности, выполните следующие действия:*

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите **English** и нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения.
2. Ознакомьтесь с Лицензионным соглашением.
3. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept**.

   Откроется окно с текстом Политики конфиденциальности.

4. Ознакомьтесь с Политикой конфиденциальности.
5. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **I accept**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор диска для установки компонента Sandbox

На этом шаге выберите физический диск для установки компонента Sandbox.

► *Чтобы выбрать диск для установки компонента Sandbox, выполните следующие действия:*

1. В окне **Select device** в списке дисков выберите диск для установки компонента Sandbox и нажмите на клавишу **ENTER**.

   Если диск не пустой, отобразится окно подтверждения форматирования этого диска и установки программы на него.
2. Нажмите на кнопку **Install**.

   Архив с установочными файлами распакуется на диск. Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 3. Назначение имени хоста

На этом шаге назначьте имя хоста сервера для использования DNS-серверами.

► *Чтобы назначить имя хоста сервера, выполните следующие действия:*

1. В поле **Hostname** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, host.domain.com или host.domain.subdomain.com).
2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор управляющего сетевого интерфейса в списке

Для работы компонента Sandbox необходимо подключить минимум две сетевые карты и настроить следующие сетевые интерфейсы:

- Управляющий сетевой интерфейс. Этот интерфейс предназначен для доступа к серверу с компонентом Sandbox по протоколу SSH, а также через этот интерфейс сервер с компонентом Sandbox будет принимать объекты с сервера с компонентом Central Node.
- Сетевой интерфейс для доступа обрабатываемых объектов в интернет. Через этот интерфейс объекты, которые обрабатывает компонент Sandbox, смогут предпринимать попытки действий в интернете, а компонент Sandbox сможет анализировать их поведение. Если вы запретите доступ в интернет, компонент Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

> Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

На этом шаге выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.

► *Чтобы выбрать управляющий сетевой интерфейс, выполните следующие действия:*

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
2. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Назначение адреса и маски сети управляющего интерфейса

► *Чтобы назначить IP-адрес и маску сети управляющего сетевого интерфейса, выполните следующие действия:*

1. В поле **Address** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
2. В поле **Netmask** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
3. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Добавление адресов DNS-серверов

► *Чтобы добавить адреса DNS-серверов, выполните следующие действия:*

1. В окне **DNS servers** выберите **New** и нажмите на клавишу **ENTER**.

   Откроется окно ввода адреса DNS-сервера.
2. В поле **DNS server** введите IP-адрес основного DNS-сервера в формате IPv4.
3. Нажмите на кнопку **Ok**.

   Окно ввода адреса DNS-сервера закроется.
4. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, повторите действия в окне **DNS servers**.
5. Когда вы добавите все DNS-серверы, в окне **DNS servers** выберите **Continue** и нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Настройка статического сетевого маршрута

► *Чтобы настроить статический сетевой маршрут, выполните следующие действия:*

1. В окне **IPv4 Routes** выберите **New** и нажмите на клавишу **ENTER**.

   Откроется окно **IPv4 Static Route**.
2. В поле **Address/Mask** введите IP-адрес и маску подсети, для которой вы хотите настроить сетевой маршрут.
3. Если вы хотите использовать сетевой маршрут по умолчанию, введите 0.0.0.0/0.
4. В поле **Gateway** введите IP-адрес шлюза.
5. Нажмите на кнопку **Ok**.
6. Если вы хотите добавить другие сетевые маршруты, повторите действия в окне **IPv4 Static Route**.
7. Когда вы закончите добавлять сетевые маршруты, нажмите на кнопку **Continue**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка минимальной длины пароля администратора Sandbox

► *Чтобы задать минимальную длину пароля администратора компонента Sandbox, выполните следующие действия:*

1. В поле **Minimal length** введите количество символов. Рекомендуется использовать пароли длиной 12 и более символов.
2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Создание учетной записи администратора Sandbox

На этом шаге создайте учетную запись администратора для работы в веб-интерфейсе Sandbox, в меню администратора и в консоли управления сервером с компонентом Sandbox.

► *Чтобы создать учетную запись администратора Sandbox, выполните следующие действия:*

1. В поле **Username** введите имя учетной записи администратора. По умолчанию используется учетная запись admin.
2. В поле **Password** введите пароль учетной записи администратора.

   Пароль должен удовлетворять следующим требованиям:

   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);

- символ нижнего регистра (a-z);
- цифру;
- специальный символ;

- не должен совпадать с именем пользователя.

3. В поле **Confirm password** введите пароль повторно.
4. Нажмите на кнопку **Ok**.

   Откроется окно с IP-адресом сервера Sandbox. По этому адресу вы можете открыть веб-интерфейс Sandbox в браузере. Для входа используйте созданную учетную запись администратора Sandbox.

   Сервер Sandbox перезагрузится.

Перейдите к настройке компонента Sandbox через веб-интерфейс (см. раздел "Работа с компонентом Sandbox через веб-интерфейс" на стр. 156).

kaspersky

Установка и настройка компонентов Central Node и Sensor на одном сервере

Этот раздел представляет собой пошаговую инструкцию по установке и предварительной настройке компонентов Central Node и Sensor на одном сервере.

► *Чтобы приступить к установке компонентов Central Node и Sensor и выбрать роль сервера, выполните следующие действия:*

1. Запустите образ диска с компонентами Central Node и Sensor.

   Запустится мастер установки.

2. Выберите установку с диска программы **Kaspersky Anti Targeted Attack Platform**.

   Откроется окно начала установки программы.

3. Нажмите на кнопку **Ok**.

   Откроется окно выбора роли сервера.

4. Выберите **Act as Central Node**.

   > Роль Central Node включает в себя установку и настройку компонентов Central Node и Sensor на одном сервере.

   При необходимости использования компонента Central Node отдельно от компонента Sensor пропускайте шаги по настройке компонента Sensor при установке компонентов Central Node и Sensor (см. раздел "Установка и настройка компонентов Central Node и Sensor на одном сервере" на стр. 102).

5. Откроется окно подтверждения выбора роли сервера.

   Нажмите на кнопку **Confirm role**.

Запустится мастер установки компонентов Central Node и Sensor на одном сервере.

kaspersky

В этом разделе

Шаг 1. Настройка минимальной длины пароля администратора

► *Чтобы задать минимальную длину пароля администратора, выполните следующие действия:*

1. В поле **Minimal length** введите количество символов. Рекомендуется использовать пароли длиной 12 и более символов.
2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Создание учетной записи для работы в меню администратора и в консоли управления сервером

► *Чтобы создать учетную запись администратора для работы в меню администратора и в консоли управления сервером, выполните следующие действия:*

1. В поле **Username** введите имя пользователя учетной записи администратора.
2. В поле **Password** введите пароль учетной записи администратора.

Пароль должен удовлетворять следующим требованиям:

- должен содержать минимум 8 символов;
- должен содержать символы минимум трех типов:
  - символ верхнего регистра (A-Z);
  - символ нижнего регистра (a-z);
  - цифру;
  - специальный символ;
- не должен совпадать с именем пользователя.

3. В поле **Confirm password** введите пароль повторно.
4. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Назначение имени хоста

На этом шаге назначьте имя хоста сервера для использования DNS-серверами.

► *Чтобы назначить имя хоста сервера, выполните следующие действия:*

1. В поле **Hostname** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, host.domain.com или host.domain.subdomain.com).
2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Первоначальное включение сетевого интерфейса

Необходимо включить сетевые интерфейсы для последующей настройки их параметров.

После первого включения сетевого интерфейса вы сможете отключать и включать каждый сетевой интерфейс в окне настройки сетевого интерфейса.

► *Чтобы впервые включить сетевой интерфейс, выполните следующие действия:*

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите включить.
2. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения включения сетевого интерфейса.
3. Нажмите на кнопку **Yes**.

   Сетевой интерфейс будет включен.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Назначение адреса и маски сети управляющего интерфейса

► *Чтобы назначить IP-адрес и маску сети управляющего сетевого интерфейса, выполните следующие действия:*

1. Выберите параметр **IP addr** и нажмите на клавишу **ENTER**.

   Откроется окно ввода IP- адреса и маски сети.
2. В поле **Address** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
3. В поле **Netmask** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
4. Нажмите на кнопку **Ok**.

   Окно ввода IP- адреса и маски сети закроется.
5. Выберите **Go back** и нажмите на клавишу **ENTER**.

   Окно настройки сетевого интерфейса закроется.
6. Выберите **Continue** и нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Настройка сетевого маршрута для использования по умолчанию

На этом шаге настройте сетевой маршрут, который программа будет использовать по умолчанию.

► *Чтобы настроить статический сетевой маршрут, выполните следующие действия:*

1. В списке **Default route** выберите **Interface** и нажмите на клавишу **ENTER**.

   Откроется список сетевых интерфейсов.
2. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут и нажмите на клавишу **ENTER**.

   Мастер установки вернется к окну настройки сетевого маршрута.
3. Выберите параметр **Gateway** и нажмите на клавишу **ENTER**.

   Откроется окно ввода статического адреса шлюза.
4. В поле **Gateway** введите статический адрес шлюза.
5. Нажмите на кнопку **Ok**.

   Мастер установки вернется к окну настройки сетевого маршрута.

   Напротив названия параметра **Gateway** отобразится статический адрес шлюза, который вы назначили.
6. Выберите **Continue** и нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

kaspersky

Шаг 7. Настройка параметров DNS

На этом шаге настройте параметры DNS для работы серверов с компонентами программы.

► *Чтобы назначить статические DNS-адреса, выполните следующие действия:*

1. В окне **Select action - Resolver** выберите любой параметр (например, **Search list**) и нажмите на клавишу **ENTER**.

   Отобразится окно ввода статических DNS-адресов.
2. В поле **Search list** введите DNS-суффикс, который вы хотите использовать в программе. Например, example.com.
3. В поле **Primary** введите IP-адрес основного DNS-сервера в формате IPv4.
4. В поле **Secondary** введите IP-адрес дополнительного DNS-сервера в формате IPv4.
5. Нажмите на кнопку **Ok**.

   Отобразится окно настройки параметров DNS с установленными статическими параметрами DNS.
6. Проверьте правильность установленных параметров DNS.
7. Выберите **Continue** и нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка параметров соединения с прокси-сервером

На этом шаге включите или отключите использование прокси-сервера для обновления баз и подключения к службе KSN, настройте параметры соединения с прокси-сервером, а также включите или отключите использование прокси-сервера при подключении к локальным адресам сети вашей организации.

В этом разделе

Включение и отключение использования прокси-сервера

► *Чтобы включить или отключить использование прокси-сервера, выполните следующие действия:*

1. Выберите параметр **Enabled**.
2. Нажмите на клавишу **ENTER**.

   Если использование прокси-сервера было отключено, оно включится. Напротив названия параметра **Enabled** отобразится значение **yes**.

   Если использование прокси-сервера было включено, оно отключится. Напротив названия параметра **Enabled** отобразится значение **no**.

Перейдите к настройке параметров соединения с прокси-сервером в текущем окне.

Настройка параметров соединения с прокси-сервером

► *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. В окне **Select Action - Proxy** выберите любой параметр (например, **Host)** и нажмите на клавишу **ENTER**.

   Отобразится окно настройки параметров соединения с прокси-сервером.

2. В поле **Proxy URL** введите URL-адрес прокси-сервера, порт подключения, а также имя пользователя и пароль, если вы хотите использовать аутентификацию на прокси-сервере.

   Вводите данные в формате `http://<имя пользователя прокси-сервера>:<пароль пользователя прокси-сервера>@<IP-адрес или URL-адрес прокси-сервера>:<порт подключения к прокси-серверу>`

   Например, http://admin:password@10.1.1.1:3128

3. Нажмите на кнопку **Ok**.

   Окно настройки параметров соединения с прокси-сервером закроется.

   В окне **Select Action - Proxy** отобразятся значения параметров соединения с прокси-сервером.

Перейдите к включению или отключению использования прокси-сервера при подключении к локальным адресам сети вашей организации в текущем окне.

Если сервер обновлений баз находится внутри IT-инфраструктуры вашей организации или вы используете KPSN, отключите использование прокси-сервера при подключении к локальным адресам сети вашей организации.

Включение и отключение использования прокси-сервера при подключении к локальным адресам

► *Чтобы включить или отключить использование прокси-сервера при подключении к локальным адресам сети вашей организации, выполните следующие действия:*

1. Выберите параметр **Local addresses**.
2. Нажмите на клавишу **ENTER**.

   Если использование прокси-сервера при подключении к локальным адресам было отключено, оно включится. Напротив названия параметра **Local addresses** отобразится значение **use proxy**.

   Если использование прокси-сервера при подключении к локальным адресам было включено, оно отключится. Напротив названия параметра **Local addresses** отобразится значение **bypass**.

3. Выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Установка часового пояса

► *Чтобы установить часовой пояс, выполните следующие действия:*

1. В окне **Select Timezone - Select Country** выберите страну из списка (например, **Russia**) и нажмите на клавишу **ENTER**.

   Отобразится список часовых поясов, доступных для выбранной страны.

2. Выберите часовой пояс и нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения выбора часового пояса.

3. Если часовой пояс выбран верно, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Настройка синхронизации времени с NTP-сервером

На этом шаге вы можете настроить синхронизацию времени сервера с NTP-сервером.

► *Чтобы отказаться от синхронизации времени с NTP-сервером, выполните следующие действия:*

1. В окне **Use NTP to set clock** нажмите на кнопку **No**.

   Откроется окно **Set the system clock manually**.

2. Нажмите на одну из следующих кнопок:

   - **No**, если вы не хотите вручную настроить время.

   Мастер установки программы сразу перейдет к следующему шагу.

   - **Yes**, если вы хотите вручную настроить время.

   Откроется окно **Set the system clock**, в котором вы можете настроить время.

3. По окончании настройки времени выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

► *Чтобы включить синхронизацию времени с NTP-сервером, выполните следующие действия:*

1. В окне **Use NTP to set clock** нажмите на кнопку **Yes**.

   Откроется окно **Configure NTP servers**.

2. В окне **Configure NTP servers** выберите **New**.

   Откроется окно **Add NTP server**.

3. В поле **NTP server** введите IP-адрес или URL-адрес NTP-сервера, с которым вы хотите настроить синхронизацию времени.
4. Нажмите на кнопку **Ok**.

   Окно **Add NTP server** закроется.

Адрес NTP-сервера добавится в список NTP-серверов в окне **Configure NTP servers**.

5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 11. Настройка интеграции с компонентом Sandbox

► *Чтобы подключиться к серверу, на котором вы установили компонент Sandbox, выполните следующие действия:*

1. В окне **Sandbox access** сверьте IP-адрес и отпечаток сертификата с IP-адресом и отпечатком сертификата на сервере с компонентом Sandbox.
2. Выберите **New**.
3. Нажмите на клавишу **ENTER**.
4. Откроется окно **Sandbox node**.
5. В поле **Sandbox name** введите имя сервера с компонентом Sandbox для отображения на серверах с компонентом Central Node.
6. В поле **Sandbox node** введите IP-адрес или URL-адрес сервера с компонентом Sandbox.
7. Нажмите на кнопку **Ok**.

   Откроется окно **Sandbox access**.
8. Проверьте параметры подключения к серверу Sandbox.
9. Если вы хотите включить или отключить использование сервера с компонентом Sandbox, нажмите на строку с именем и адресом этого сервера.

   По умолчанию использование сервера с компонентом Sandbox, подключение к которому вы настроили, включено.
10. Выберите **Continue**.
11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Вы можете принять, отклонить или отозвать ранее принятый запрос на подключение от серверов Central Node в веб-интерфейсе Sandbox.

► *Чтобы принять, отклонить или отозвать запрос на подключение от серверов Central Node, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Авторизация KATA**.

   В разделе **Запросы на подключение от Central Node** отобразится список запросов на подключение от компонентов Central Node.

   В каждом запросе на подключение содержится следующая информация:

   - **IP** – IP-адрес сервера Central Node.
   - **Отпечаток сертификата** – отпечаток TLS-сертификата Cental Node, с помощью которого устанавливается шифрованное соединение между серверами.

- **Состояние** – состояние запроса на подключение.

  Может иметь значения **Ожидание** или **Принят**.

2. Убедитесь, что отпечаток сертификата Cental Node соответствует отпечатку сертификата на стороне Cental Node.

   Вы можете проверить отпечаток сертификата Central Node в меню администратора сервера Central Node в разделе **Manage server certificate**.

3. Нажмите на одну из следующих кнопок в строке с запросом на подключение от компонента Central Node:

   - **Принять**, если вы хотите принять запрос на подключение.
   - **Отклонить**, если вы хотите отклонить запрос на подключение.
   - **Отозвать**, если вы хотите отозвать ранее принятый запрос на подключение.

4. Нажмите на кнопку **Применить** в нижней части окна.

Шаг 12. Выделение диска для базы данных компонента Targeted Attack Analyzer

Для оптимальной работы компонента Targeted Attack Analyzer рекомендуется выделить на сервере физический диск объемом не менее 1 ТБ для базы данных компонента.

На этом шаге вы можете выделить физический диск для базы данных компонента Targeted Attack Analyzer или отказаться от выделения физического диска.

► *Чтобы отказаться от выделения диска, выполните следующие действия:*

1. В окне **Select device** выберите **Continue without separate disk drive**.
2. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

► *Чтобы выделить диск, выполните следующие действия:*

1. В окне **Select device** выберите диск, который вы хотите выделить для базы данных компонента Targeted Attack Analyzer.
2. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения действия.

3. Нажмите на кнопку **Yes**.

Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

kaspersky

Шаг 13. Создание учетной записи администратора веб-интерфейса Kaspersky Endpoint Detection and Response

► *Чтобы создать учетную запись дминистратора веб-интерфейса программы, выполните следующие действия:*

1. В поле **Username** введите имя пользователя учетной записи.

   По умолчанию используется имя пользователя Administrator.
2. В поле **Password** введите пароль учетной записи администратора.

   Пароль должен удовлетворять следующим требованиям:

   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ;
   - не должен совпадать с именем пользователя.
3. В поле **Confirm password** введите пароль повторно.
4. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 14. Настройка интеграции с прокси-сервером по протоколу ICAP

На этом шаге вы можете настроить интеграцию программы с прокси-сервером, использующимся в вашей организации, по протоколу ICAP.

Если вы используете отдельный прокси-сервер, по умолчанию Kaspersky Endpoint Detection and Response не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов. Администратору программы необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Endpoint Detection and Response с помощью туннелирования трафика или средствами iptables.

► *Чтобы отказаться от интеграции программы с прокси-сервером,*

в окне **Enable ICAP processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

► *Чтобы включить интеграцию программы с прокси-сервером, выполните следующие действия:*

1. В окне **Enable ICAP processing** нажмите на кнопку **Yes**.

   Откроется окно с URI-адресом сервера, на который вы устанавливаете компонент Central Node.

   Используйте этот URI-адрес для настройки интеграции по протоколу ICAP на прокси-сервере, использующемся в вашей организации.

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 15. Настройка интеграции с почтовым сервером по протоколу POP3

На этом шаге вы можете настроить интеграцию с почтовым сервером по протоколу POP3 после предварительной подготовки IT-инфраструктуры вашей организации.

► *Чтобы отказаться от интеграции с почтовым сервером по протоколу POP3,*

в окне **Enable POP3 processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

► *Чтобы настроить интеграцию с почтовым сервером по протоколу POP3, выполните следующие действия:*

1. В окне **Enable POP3 processing** нажмите на кнопку **Yes**.

   Откроется окно настройки интеграции с почтовым сервером по протоколу POP3.

2. Выберите параметр **Server**.
3. Нажмите на клавишу **ENTER**.

   Откроется окно **POP3 server**.

4. В поле **Server** введите IP-адрес почтового сервера, с которым вы хотите настроить интеграцию.
5. Нажмите на кнопку **Ok**.

   Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.

6. Выберите параметр **Encrypted**.
7. Нажмите на клавишу **ENTER**.

   - Если шифрованное соединение с почтовым сервером было отключено, оно включится. Напротив названия параметра **Encrypted** отобразится значение **yes**.
   - Если шифрованное соединение с почтовым сервером было включено, оно отключится. Напротив названия параметра **Encrypted** отобразится значение **no**.

8. Выберите параметр **Username**.
9. Нажмите на клавишу **ENTER**.

   Откроется окно **POP3 access**.

10. В поле **Username** введите имя учетной записи для доступа к почтовому серверу по протоколу POP3.
11. В поле **Password** введите пароль доступа к почтовому серверу.
12. Нажмите на кнопку **Ok**.

    Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.
13. Выберите параметр **Check interval**.
14. Нажмите на клавишу **ENTER**.

    Откроется окно **Check interval**.
15. В поле **Check interval** введите частоту соединения с почтовым сервером в секундах.
16. Нажмите на кнопку **Ok**.

    Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.
17. В разделе **Accepts certificates** настройте параметры TLS-шифрования соединения программы с внешними почтовыми серверами по протоколу POP3.
    - Если вы хотите, чтобы программа принимала любые TLS-сертификаты при соединении с внешними почтовыми серверами, выполните следующие действия:
      a. Выберите вариант **any certificate**.
      b. Нажмите на клавишу **ENTER**, чтобы напротив варианта **any certificate** отобразилось значение **yes**.
    - Если вы хотите, чтобы программа принимала недоверенные самоподписанные TLS-сертификаты при соединении с внешними почтовыми серверами, выполните следующие действия:
      1. Выберите вариант **untrusted self-signed**.
      2. Нажмите на клавишу **ENTER**, чтобы напротив варианта **untrusted self-signed** отобразилось значение **yes**.
    - Если вы хотите, чтобы программа принимала только доверенные TLS-сертификаты при соединении с внешними почтовыми серверами, выполните следующие действия:
      a. Выберите вариант **any certificate**.
      b. Нажмите на клавишу **ENTER**, чтобы напротив варианта **any certificate** отобразилось значение **no**.
      c. Выберите вариант **untrusted self-signed**.
      d. Нажмите на клавишу **ENTER**, чтобы напротив варианта **untrusted self-signed** отобразилось значение **no**.

    При установке соединения с внешним почтовым сервером рекомендуется настроить прием только доверенных TLS-сертификатов. Прием недоверенных TLS-сертификатов не гарантирует защиту соединения от MITM-атак. Прием доверенных TLS-сертификатов также не полностью гарантирует защиту соединения от MITM-атак, но является самым безопасным из поддерживаемых способов интеграции с почтовым сервером по протоколу POP3.
18. При необходимости в разделе **Cipher list** измените параметры OpenSSL, используемые при установке соединения с почтовым сервером по протоколу POP3. Выполните действия:

a. Выберите **edit**.

b. Нажмите на клавишу **ENTER**.

Откроется окно **Cipher list**.

c. В поле **Cipher list** измените набор шифров.

19. Нажмите на кнопку **Ok**.

Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.

20. Выберите **Continue**.
21. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 16. Просмотр Лицензионного соглашения и Политики конфиденциальности

Для продолжения установки вам нужно просмотреть Лицензионное соглашение и принять его условия. Если условия Лицензионного соглашения не приняты, установка не выполняется.

Также вам нужно просмотреть Политику конфиденциальности и принять ее условия.

► *Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности, выполните следующие действия:*

1. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите **English**.

2. Нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения.

3. Ознакомьтесь с Лицензионным соглашением.
4. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept the terms**.

   Откроется окно с текстом Политики конфиденциальности.

5. Ознакомьтесь с Политикой конфиденциальности.
6. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **I accept the terms**.

Мастер установки перейдет к следующему шагу.

kaspersky

Установка и удаление отдельного компонента Endpoint Sensors

Этот раздел представляет собой инструкцию по установке и удалению компонента Endpoint Sensors, устанавливающегося на отдельные компьютеры.

Если вы хотите использовать компонент Endpoint Agent в составе Kaspersky Endpoint Security, выполните интеграцию Kaspersky Endpoint Detection and Response (Kaspersky Anti Targeted Attack Platform) с программой Kaspersky Endpoint Agent (см. раздел "Настройка интеграции Kaspersky Endpoint Detection and Response (Kaspersky Anti Targeted Attack Platform) с программой Kaspersky Endpoint Agent" на стр. 126).

Если вы установите программу Kaspersky Endpoint Security на компьютер с компонентом Endpoint Sensors, компонент Endpoint Sensors будет удален независимо от того, включен ли компонент Endpoint Sensors в состав программы Kaspersky Endpoint Security или нет.

В этом разделе

Особенности установки отдельного компонента Endpoint Sensors при совместной работе программы с KES

Совместимость KES и компонента Endpoint Sensors версии 3.5

► *Если вы используете KES версии 10 SP2 MR3 или 11.0 и хотите использовать отдельный компонент Endpoint Sensors версии 3.5, выполните следующие действия:*

1. Отключите компонент Endpoint Sensors в составе программы KES.

   Подробнее о том, как отключить компонент Endpoint Sensors в составе программы KES см. в *Справке Kaspersky Endpoint Security*.

2. Установите отдельный компонент Endpoint Sensors версии 3.5 на все компьютеры сети вашей организации, на которых вы хотите использовать компонент Endpoint Sensors.

Совместимость KES и отдельного компонента Endpoint Sensors версии 3.6

Сценарий установки отдельного компонента Endpoint Sensors версии 3.6 и программы KES на одном компьютере зависит от версии KES. Информация о совместимости программы и компонента и сценарии установки приведены в таблице ниже.

Программа KES версии 11.1 совместима только с компонентом Endpoint Sensors, входящим в состав программы KES. Установка программы KES версии 11.1 и отдельного компонента Endpoint Sensors на одном компьютере невозможна.
Программа KES версии 11.2 и выше совместима только с компонентом Endpoint Agent, входящим в состав программы KES. Установка программы KES версии 11.2 и выше и отдельного компонента Endpoint Sensors на одном компьютере невозможна.

Таблица 10. Сценарии установки KES и отдельного компонента Endpoint Sensors

Версия KES	Установка отдельного компонента Endpoint Sensors после установки KES	Установка KES после установки отдельного компонента Endpoint Sensors
• KES10 SP1 MR3 • KES10 SP1 MR4 • KES 10 SP2 • KES 10 SP2 MR1 • KES 10 SP2 MR2 • KES 10 SP2 MR3	Стандартная процедура установки.	Стандартная процедура установки.
• KES 11.0.0 • KES 11.0.1	Требуется отключить компонент Endpoint Sensors в составе программы KES. Подробнее о том, как отключить компонент Endpoint Sensors в составе программы KES см. в *Справке Kaspersky Endpoint Security*. Если компонент не отключен, установка прерывается с ошибкой.	Стандартная процедура установки.
KES 11.1 и выше	Установка прерывается с ошибкой.	KES удаляет отдельный компонент Endpoint Sensors.

Установка отдельного компонента Endpoint Sensors

Перед установкой отдельного компонента Endpoint Sensor администратору требуется убедиться, что в папке установки нет файлов других программ. Рекомендуется предоставить доступ на запись в папку установки только пользователям с ролями System и Administrator.
Для установки компонента Endpoint Sensor ваша учетная запись должна обладать правами локального администратора.

► *Чтобы установить компонент Endpoint Sensor на компьютеры локальной сети организации, с которых Kaspersky Endpoint Detection and Response получает и обрабатывает данные, выполните следующие действия:*

1. Загрузите установочный файл компонента Endpoint Sensor на компьютер любым доступным способом.
2. Запустите на компьютере приложение для работы в командной строке.
3. В командной строке введите следующую команду:

   ```
   msiexec /i "<путь к установочному файлу компонента Endpoint Sensor с указанием имени файла и расширения msi>" /qn /l*v <путь к журналу установки>\install.log SERVER=<адрес сервера с компонентом Central Node> acceptEULA=1
   ```

   Если вы используете компонент Sensor в качестве прокси-сервера, вместо IP-адреса или FQDN-имени Central Node укажите IP-адрес или FQDN-имя сервера с компонентом Sensor.

4. Нажмите на клавишу **ENTER**.

Установка отдельного компонента Endpoint Sensor завершится.

Вы также можете установить компонент Endpoint Sensor с помощью утилиты Orca.exe компании Microsoft или удаленно как объект групповой политики Microsoft Windows. Подробнее об этих способах установки см. в документации компании Microsoft.

kaspersky

Удаление отдельного компонента Endpoint Sensors

Для удаления компонента Endpoint Sensors с компьютера локальной сети организации ваша учетная запись должна обладать правами локального администратора.

Вы можете удалить компонент Endpoint Sensors средствами операционной системы Microsoft Windows, установленной на компьютере локальной сети организации. Процедура удаления зависит от версии операционной системы. Подробнее об удалении программ средствами операционной системы Microsoft Windows смотрите в документации компании Microsoft.

При удалении компонента Endpoint Sensors удаляются следующие данные:

- Все данные, накопленные в процессе работы компонента Endpoint Sensors на компьютере.
- Конфигурационный файл из папки C:\Program Data\Kaspersky Lab\Endpoint Sensor 3.6.
- Ветка реестра HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Endpoint Sensor 3.6\protected (для 32-разрядной операционной системы), HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\Endpoint Sensor 3.6 (для 64-разрядной операционной системы) и все хранящиеся в ней ключи.

После удаления компонента Endpoint Sensors необходимо перезагрузить компьютер, на котором он был установлен.

kaspersky

Настройка доверенного соединения Kaspersky Endpoint Detection and Response с отдельным компонентом Endpoint Sensors

Чтобы компонент Endpoint Sensors мог отправлять файлы на сервер с компонентом Central Node, вам нужно усилить безопасность и настроить доверенное соединение между компонентом Endpoint Sensors и сервером Central Node или Sensor (если вы настроили перенаправление трафика на Sensor (см. раздел "Настройка перенаправления трафика от Endpoint Agent на сервер Sensor" на стр. 137)).

Вы можете настроить доверенное соединение при соблюдении следующих условий конфигурации локальной сети вашей организации:

- В локальной сети вашей организации развернуты доменные службы Active Directory.
- Компьютеры, на которых установлен компонент Endpoint Sensors, подключены к Active Directory.

Выпол**няйте действия по настройке доверенного соединения в следующем порядке:**

a. Генерация (см. раздел "Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Endpoint Detection and Response" на стр. 120) или загрузка самостоятельно подготовленного TLS-сертификата (см. раздел "Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Endpoint Detection and Response" на стр. 120) сервера Central Node в веб-интерфейсе Central Node (если TLS-сертификат сервера Central Node не создан ранее) или Генерация (если вы настроили перенаправление трафика на сервер Sensor (см. раздел "Настройка перенаправления трафика от Endpoint Agent на сервер Sensor" на стр. 137)).

b. Скачивание TLS-сертификата сервера Central Node (см. раздел "Скачивание TLS-сертификата сервера Central Node на компьютер" на стр. 122) или сервера Sensor (см. раздел "Скачивание TLS-сертификата сервера Sensor на компьютер" на стр. 124) на компьютер.

c. Подготовка и загрузка TLS-сертификата в Active Directory (см. раздел "Подготовка и загрузка TLS-сертификата сервера Central Node в Active Directory" на стр. 124).

В этом разделе

kaspersky

Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Endpoint Detection and Response

Если вы уже используете TLS-сертификат сервера Central Node и сгенерируете новый сертификат, сертификат, который используется в программе, будет удален и заменен на сгенерированный сертификат.
Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node (см. раздел "Настройка интеграции с внешними системами" на стр. 207).
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox (см. раздел "Настройка интеграции с компонентом Sandbox" на стр. 204).
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent (см. раздел "Настройка перенаправления трафика от Endpoint Agent на сервер Sensor" на стр. 137).
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory) (см. раздел "Подготовка и загрузка TLS-сертификата сервера Central Node в Active Directory" на стр. 124).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

► *Чтобы сгенерировать TLS-сертификат сервера Central Node, выполните следующие действия:*

1. Войдите в веб-интерфейс программы (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
3. В разделе **TLS-сертификат** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Kaspersky Endpoint Detection and Response сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Endpoint Detection and Response

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Endpoint Detection and Response (Kaspersky Anti Targeted Attack Platform).

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации OpenSSL.

Если вы уже используете TLS-сертификат сервера Central Node и загрузите новый сертификат, сертификат, который используется в программе, будет удален и заменен на загруженный сертификат. Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node (см. раздел "Настройка интеграции с внешними системами" на стр. 207).
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox (см. раздел "Настройка интеграции с компонентом Sandbox" на стр. 204).
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent (см. раздел "Настройка перенаправления трафика от Endpoint Agent на сервер Sensor" на стр. 137).
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory) (см. раздел "Подготовка и загрузка TLS-сертификата сервера Central Node в Active Directory" на стр. 124).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс программы, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
3. В разделе **TLS-сертификат** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Endpoint Detection and Response.

Скачивание TLS-сертификата сервера Central Node на компьютер

► *Чтобы скачать TLS-сертификат сервера на компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **TLS-сертификат** нажмите на кнопку **Скачать**.

Файл сертификата сервера будет сохранен в папке загрузки браузера.

Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor

► *Чтобы сгенерировать TLS-сертификат сервера с компонентом Sensor, выполните следующие действия в меню администратора сервера с компонентом Sensor (см. раздел "Начало работы в меню администратора программы" на стр. 142):*

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Manage server certificate**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Certificate management**.
5. В нижней части окна выберите пункт **New**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно с информацией о новом сертификате.
7. Нажмите на кнопку **Continue**.

   Откроется окно подтверждения действия.
8. Нажмите на кнопку **Generate**.

   Начнется создание сертификата.
9. По окончании создания сертификата нажмите на клавишу **ENTER**.

   Откроется окно с информацией об установленном сертификате.
10. Нажмите на кнопку **Continue**.

    Откроется окно подтверждения действия.
11. Нажмите на кнопку **Ok**.

Сертификат будет создан. Данные сертификатов, установленных ранее, будут перезаписаны.

Загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его на сервер с компонентом Sensor по протоколу SCP. Подробнее о способах загрузки файлов по протоколу SCP см. в документации к

операционной системе, установленной на том компьютере, с которого вы хотите загрузить TLS-сертификат.

Файл TLS-сертификата, предназначенный для загрузки на сервер, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Имя файла должно быть kata.pem.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат на сервер с компонентом Sensor по протоколу SCP, выполните следующие действия в интерфейсе работы по протоколу SCP вашего компьютера (на примере операционной системы Linux):*

1. Выполните команду `scp kata.pem admin@<IP-адрес сервера с компонентом Sensor>:`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Sensor, заданный при установке (см. раздел "Шаг 4. Создание учетной записи для работы в меню администратора и в консоли управления сервером" на стр. **Ошибка! Закладка не определена.**).

TLS-сертификат будет загружен на сервер с компонентом Sensor.

► *Чтобы применить загруженный TLS-сертификат на сервере с компонентом Sensor, выполните следующие действия в меню администратора сервера с компонентом Sensor (см. раздел "Начало работы в меню администратора программы" на стр. 142):*

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Manage server certificate**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Certificate management**.
5. В нижней части окна выберите пункт **kata.pem**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно **Uploaded certificate**.
7. Выберите пункт **Install certificate**.
8. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения действия.
9. Нажмите на кнопку **Yes**.

   Откроется окно с информацией о сертификате.
10. Нажмите на кнопку **Continue**.

    Откроется окно подтверждения действия.

11. Нажмите на кнопку **Install**.

    Начнется установка сертификата.

12. По окончании установки сертификата нажмите на клавишу **ENTER**.

    Откроется окно с информацией о примененном сертификате.

13. Нажмите на кнопку **Continue**.

    Откроется окно подтверждения действия.

14. Нажмите на кнопку **Ok**.

Сертификат будет применен. Данные сертификатов, установленных ранее, будут перезаписаны.

Скачивание TLS-сертификата сервера Sensor на компьютер

Вы можете скачать TLS-сертификат с сервера Sensor на любой компьютер, имеющий доступ к серверу с компонентом Sensor, по протоколу SCP. Подробнее о способах загрузки файлов по протоколу SCP см. в документации к операционной системе, установленной на том компьютере, на который вы хотите скачать TLS-сертификат.

► *Чтобы скачать TLS-сертификат с сервера с компонентом Sensor по протоколу SCP, выполните следующие действия в интерфейсе работы по протоколу SCP вашего компьютера (на примере операционной системы Linux):*

1. Выполните команду `scp admin@<IP-адрес сервера с компонентом Sensor>:ssl/kata.crt .`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Sensor, заданный при установке (см. раздел "Шаг 4. Создание учетной записи для работы в меню администратора и в консоли управления сервером" на стр. **Ошибка! Закладка не определена.**).

TLS-сертификат будет загружен с сервера с компонентом Sensor в текущую директорию.

Подготовка и загрузка TLS-сертификата сервера Central Node в Active Directory

► *Чтобы подготовить и загрузить TLS-сертификат в Active Directory, выполните следующие действия для каждого сервера с компонентом Central Node:*

1. Выберите контейнер Active Directory для размещения сертификата. Компонент Endpoint Sensors поддерживает поиск объекта serviceConnectionPoint в следующих расположениях (в порядке очередности поиска):

   - `ldap://CN=<Active Directory Site, в котором находится компьютер с компонентом Endpoint Sensors>,CN=Sites,<configurationPartition>`

     `ldap://CN=Services, <раздел конфигурации Active Directory>`

Публиковать сертификат в контейнере Sites рекомендуется, если для какого-либо из Active Directory Site развернут отдельный компонент Central Node.

2. В выбранном контейнере создайте объект типа serviceConnectionPoint.
3. Откройте TLS-сертификат сервера с компонентом Central Node в формате PEM в текстовом редакторе и выполните следующие действия:
   a. Удалите строки BEGIN CERTIFICATE и END CERTIFICATE.
   b. Удалите все переносы строк.
4. Заполните атрибуты serviceConnectionPoint следующим образом:
   - keywords содержит строку-идентификатор 013D90F9-517B-486D-A7E8-888439D1DD61.
   - serviceDNSName в точности совпадает с адресом сервера Central Node, указанным при установке компонента Endpoint Sensors.

     Если в качестве адреса при установке задан IP-адрес, атрибут должен содержать тот же IP-адрес. Если в качестве адреса при установке задано FQDN-имя сервера, атрибут должен содержать то же FQDN-имя сервера.
   - serviceBindingInformation содержит SSL-сертификат сервера с компонентом Central Node в формате PEM в одну строку.

Компонент Endpoint Sensors ищет объект serviceConnectionPoint последовательно сначала в контейнере Sites, затем в контейнере Services. Используется первый найденный объект, у которого атрибут keywords содержит уникальный идентификатор, а атрибут serviceDnsName в точности совпадает с адресом сервера Central Node, заданным при установке компонента Endpoint Sensors.

Если в одном и том же контейнере Active Directory располагаются два и более объекта serviceConnectionPoint, у которых атрибут keywords содержит уникальный идентификатор, а значения serviceDNSName совпадают, компонент Endpoint Sensors будет иметь ограниченную функциональность.

Если компонент Endpoint Sensors не может декодировать значение атрибута serviceBindingInformation в бинарный формат или если значение атрибута – пустая строка, компонент Endpoint Sensors будет иметь ограниченную функциональность.

kaspersky

Настройка интеграции Kaspersky Endpoint Detection and Response с программой Kaspersky Endpoint Agent

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Detection and Response с программой Kaspersky Endpoint Agent. Вам понадобится выполнить действия и на стороне Kaspersky Endpoint Detection and Response через веб-интерфейс (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) и меню администратора программы (см. раздел "Начало работы в меню администратора программы" на стр. 142), и на стороне Kaspersky Endpoint Agent через консоль администрирования KSC.

В этом разделе

kaspersky

Настройка доверенного соединения Kaspersky Endpoint Detection and Response с программой Kaspersky Endpoint Agent

Вам понадобится настроить доверенное соединение Kaspersky Endpoint Detection and Response с Kaspersky Endpoint Agent и на стороне Kaspersky Endpoint Detection and Response (Kaspersky Anti Targeted Attack Platform) через веб-интерфейс (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) и меню администратора программы (см. раздел "Начало работы в меню администратора программы" на стр. 142), и на стороне Kaspersky Endpoint Agent через консоль администрирования KSC.

Вы можете использовать один из следующих вариантов доверенного соединения:

1. С использованием TLS-сертификата Kaspersky программы. Без проверки TLS-сертификата Kaspersky Endpoint Agent на стороне Kaspersky Endpoint Detection and Response.
   a. Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Endpoint Detection and Response (на стр. 127).

      Kaspersky Endpoint Agent устанавливает доверенное соединение с программой с использованием TLS-сертификата сервера Central Node. Kaspersky Endpoint Detection and Response не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.
2. С использованием TLS-сертификатов Kaspersky Endpoint Detection and Response и Kaspersky Endpoint Agent. С проверкой TLS-сертификата Kaspersky Endpoint Agent на стороне Kaspersky Endpoint Detection and Response.
   a. Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Endpoint Detection and Response (на стр. 128)

      Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Endpoint Detection and Response с использованием TLS-сертификата сервера Central Node. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Endpoint Detection and Response проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

В этом разделе

Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent

Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Endpoint Detection and Response с использованием TLS-сертификата сервера Central Node. Kaspersky Endpoint Detection and Response не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

Если вы используете этот вариант настройки доверенного соединения, настройка состоит из следующих

этапов:

a. **Генерация (см. раздел "Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Endpoint Detection and Response" на стр. 120) или загрузка самостоятельно подготовленного TLS-сертификата (см. раздел "Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Endpoint Detection and Response" на стр. 120) сервера Central Node в веб-интерфейсе Central Node (если TLS-сертификат сервера Central Node не создан ранее).**
b. **Скачивание TLS-сертификата сервера Central Node на компьютер (на стр. 122).**
c. **Загрузка TLS-сертификата сервера Central Node в Kaspersky Endpoint Agent через консоль администрирования KSC (см. раздел "Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent" на стр. 131).**

Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent

Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Endpoint Detection and Response с использованием TLS-сертификата сервера Central Node. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Endpoint Detection and Response проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

Если вы используете этот вариант настройки доверенного соединения, настройка состоит из следующих этапов:

a. **Генерация (см. раздел "Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Endpoint Detection and Response" на стр. 120) или загрузка самостоятельно подготовленного TLS-сертификата (см. раздел "Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Endpoint Detection and Response" на стр. 120) сервера Central Node в веб-интерфейсе Central Node (если TLS-сертификат сервера Central Node не создан ранее).**
b. **Скачивание TLS-сертификата сервера Central Node на компьютер (на стр. 122).**
c. **Загрузка TLS-сертификата сервера Central Node в Kaspersky Endpoint Agent через консоль администрирования KSC (см. раздел "Загрузка TLS-сертификата сервера Central Node в Kaspersky Endpoint Agent" на стр. 131).**
d. **Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Endpoint Detection and Response (на стр. 132).**
e. **Генерация и скачивание крипто-контейнера с TLS-сертификатом Kaspersky Endpoint Agent (см. раздел "Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Endpoint Detection and Response и скачивание крипто-контейнера" на стр. 132) или загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Endpoint Detection and Response (на стр. 133).**

Если вы подготавливаете TLS-сертификат Kaspersky Endpoint Agent самостоятельно, вам нужно создать крипто-контейнер формата PFX с этим сертификатом. Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

f. **Загрузка крипто-контейнера с сертификатом Kaspersky Endpoint Agent в Kaspersky Endpoint Agent через консоль администрирования KSC (см. раздел "Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent" на стр. 136).**

Скачивание TLS-сертификата сервера Central Node на компьютер

► *Чтобы скачать TLS-сертификат сервера на компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **TLS-сертификат** нажмите на кнопку **Скачать**.

Файл сертификата сервера будет сохранен в папке загрузки браузера.

Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Endpoint Detection and Response

Если вы уже используете TLS-сертификат сервера Central Node и сгенерируете новый сертификат, сертификат, который используется в программе, будет удален и заменен на сгенерированный сертификат.
Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно настроить соединение Central Node, PCN и SCN с Sandbox (см. раздел "Настройка интеграции с компонентом Sandbox" на стр. 204).
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory) (см. раздел "Подготовка и загрузка TLS-сертификата сервера Central Node в Active Directory" на стр. 124).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

► *Чтобы сгенерировать TLS-сертификат сервера Central Node, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
3. В разделе **TLS-сертификат** нажмите на кнопку **Сгенерировать**.

Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Программа сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс программы

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Endpoint Detection and Response.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Если вы уже используете TLS-сертификат сервера Central Node и загрузите новый сертификат, сертификат, который используется в программе, будет удален и заменен на загруженный сертификат. Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно настроить соединение Central Node, PCN и SCN с Sandbox (см. раздел "Настройка интеграции с компонентом Sandbox" на стр. 204).
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory) (см. раздел "Подготовка и загрузка TLS-сертификата сервера Central Node в Active Directory" на стр. 124).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Endpoint Detection and Response, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
3. В разделе **TLS-сертификат** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Endpoint Detection and Response.

Загрузка TLS-сертификата сервера Central Node в Kaspersky Endpoint Agent

► *Чтобы загрузить TLS-сертификат сервера Central Node в Kaspersky Endpoint Agent, выполните следующие действия:*

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. В блоке политик Kaspersky Endpoint Agent выберите нужную политику и откройте ее свойства двойным щелчком мыши.

   Откроются свойства выбранной политики.
4. В разделе **Интеграция с KATA** выберите подраздел **KATA Central Node**.
5. Установите флажок **Включить интеграцию с KATA**.
6. В поле **Адрес** введите адрес сервера Central Node программы Kaspersky Endpoint Detection and Response, с которым вы хотите настроить интеграцию, и выберите порт подключения. По умолчанию используется порт 443.
7. Установите флажок **Использовать доверенное соединение**.
8. Нажмите на кнопку **Добавить новый TLS-сертификат**.

   Откроется окно **Добавление TLS-сертификата**.
9. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Endpoint Detection and Response и скачанного на компьютер (см. раздел "Скачивание TLS-сертификата сервера Central Node на компьютер" на стр. 122):

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Обзор**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Open**.
   - Скопируйте содержание файла сертификата в поле **Вставьте текстовые данные TLS-сертификата**.

   В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Endpoint Detection and Response. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.
10. Нажмите на кнопку **Добавить**.

    Информация о добавленном TLS-сертификате отобразится в разделе интеграции с Kaspersky Endpoint Detection and Response (Kaspersky Anti Targeted Attack Platform).
11. В правом верхнем углу блока параметров измените положение переключателя с **Политика не**

применяется на **Под политикой**.

12. Нажмите на кнопку **OK**.

TLS-сертификат сервера Central Node будет загружен в Endpoint Agent.

Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе программы

► *Чтобы включить использование доверенного соединения с Kaspersky Endpoint Agent, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.
3. Включите переключатель **Проверять TLS-сертификаты Endpoint Agent**.

Программа будет проверять данные TLS-сертификата при попытках подключения Kaspersky Endpoint Agent к Kaspersky Endpoint Detection and Response.

Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе программы и скачивание крипто-контейнера

► *Чтобы сгенерировать TLS-сертификат соединения Kaspersky Endpoint Detection and Response с Kaspersky Endpoint Agent, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.
3. Нажмите на кнопку **Сгенерировать**.

Kaspersky Endpoint Detection and Response сгенерирует новый TLS-сертификат. Страница автоматически обновится.

На ваш локальный компьютер в папку загрузки браузера будет загружен файл крипто-контейнера с сертификатом Kaspersky Endpoint Agent в формате PFX.

Вы можете использовать крипто-контейнер для настройки проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node при попытке подключения к Kaspersky Endpoint Detection and Response (см. раздел "Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent" на стр. 136).

По умолчанию крипто-контейнер не защищен паролем. Вы можете установить пароль крипто-контейнера.

Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

В крипто-контейнере содержится только файл сертификата и не содержится файл закрытого ключа. Kaspersky Endpoint Detection and Response не хранит закрытые ключи TLS-шифрования соединения.

Загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс программы

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Endpoint Detection and Response.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Если вы подготавливаете TLS-сертификат Kaspersky Endpoint Agent самостоятельно, вам нужно создать крипто-контейнер формата PFX с этим сертификатом и загрузить крипто-контейнер в Kaspersky Endpoint Agent (см. раздел "Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent" на стр. 136).

Вы можете использовать крипто-контейнер для настройки проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node при попытке подключения к Kaspersky Endpoint Detection and Response (см. раздел "Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent" на стр. 136).

Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

В крипто-контейнере должен содержится только файл сертификата и не должен содержится файл закрытого ключа.Kaspersky Endpoint Detection and Response не хранит закрытые ключи TLS-шифрования соединения.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Endpoint Detection and Response, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.

3. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Endpoint Detection and Response.

Просмотр таблицы TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Endpoint Detection and Response

► *Чтобы просмотреть список TLS-сертификатов соединения с Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Endpoint Detection and Response, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.
3. Откроется список TLS-сертификатов со следующими данными по каждому сертификату:
   - **TLS-сертификат** - отпечаток сертификата.
   - **Серийный номер** - серийный номер сертификата.
   - **Истекает** - дата истечения срока действия сертификата.

Фильтрация и поиск TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Endpoint Detection and Response

Вы можете отфильтровать TLS-сертификаты для отображения в таблице по одной или обеим графам **TLS-сертификат** и **Серийный номер** или выполнить поиск TLS-сертификатов по этим графам таблицы по указанным вами показателям.

► *Чтобы выполнить фильтрацию и поиск TLS-сертификатов в таблице, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.
3. Откроется список TLS-сертификатов со следующими данными по каждому сертификату:

- **TLS-сертификат** - отпечаток сертификата.
- **Серийный номер** - серийный номер сертификата.
- **Истекает** - дата истечения срока действия сертификата.

4. Если вы хотите отфильтровать или найти TLS-сертификаты по отпечатку сертификата:
   a. По ссылке **TLS-сертификат** откройте окно настройки фильтрации.
   b. В поле **TLS-сертификат** введите несколько символов отпечатка сертификата.
   c. Нажмите на кнопку **Применить**.
5. Если вы хотите отфильтровать или найти TLS-сертификаты по серийному номеру:
   a. По ссылке **Серийный номер** откройте окно настройки фильтрации.
   b. В поле **Серийный номер** введите несколько символов серийного номера.
   c. Нажмите на кнопку **Применить**.

В таблице отобразятся только TLS-сертификаты, соответствующие заданным вами условиям.

► *Чтобы сбросить фильтр по одному или нескольким условиям фильтрации,*

нажмите на кнопку ⊠ справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

> Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

Удаление TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Endpoint Detection and Response

► *Чтобы удалить один или несколько TLS-сертификатов соединения с Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Endpoint Detection and Response, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.
3. Откроется таблица TLS-сертификатов.
4. Установите флажки рядом с одним или несколькими TLS-сертификатами, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

6. Нажмите на кнопку **Да**.

Выбранные TLS-сертификаты будут удалены.

Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка крипто-контейнера в Kaspersky Endpoint Agent

► *Чтобы настроить проверку TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузить крипто-контейнер с сертификатом Kaspersky Endpoint Agent в Kaspersky Endpoint Agent, выполните следующие действия:*

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. В блоке политик Kaspersky Endpoint Agent выберите нужную политику и откройте ее свойства двойным щелчком мыши.

   Откроются свойства выбранной политики.
4. В разделе **Интеграция с KATA** выберите подраздел **KATA Central Node**.
5. Нажмите на кнопку **Настроить дополнительную защиту**.
6. В открывшемся окне установите флажок **Защита подключения с помощью клиентского сертификата**.
7. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла на вашем локальном компьютере.
8. Выберите файл крипто-контейнера сертификата Kaspersky Endpoint Agent, сгенерированного на сервере Kaspersky Endpoint Detection and Response и скачанного на жесткий диск вашего компьютера (см. раздел "Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Endpoint Detection and Response и скачивание крипто-контейнера" на стр. 132).
9. Нажмите на кнопку **OK**.

   Окно закроется.
10. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
11. Нажмите на кнопку **OK**.

Крипто-контейнер с сертификатом Kaspersky Endpoint Agent будет загружен в Kaspersky Endpoint Agent. Kaspersky Endpoint Detection and Response будет проверять TLS-сертификат Kaspersky Endpoint Agent при попытке подключения.

kaspersky

Настройка перенаправления трафика от Endpoint Agent на сервер Sensor

Вы можете использовать сервер Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Agent и компонентом Central Node, чтобы снизить нагрузку на компонент Central Node.

При настройке перенаправления трафика учитывайте следующие ограничения:

- Максимальный объем входящего трафика для компонента Sensor не должен превышать 1 Гбит/с.
- Максимальное количество компьютеров с компонентом Endpoint Agent составляет 1000 шт.
- Рекомендуемая ширина канала между серверами с компонентами Central Node и Sensor составляет 15% от трафика на SPAN-порте.
- Максимально допустимые потери пакетов, пересылаемых между серверами с компонентами Sensor и Central Node, составляют 10% при задержке отправки пакетов до 100 мс.

Вы можете использовать компонент Sensor в качестве прокси-сервера, только если компоненты Sensor и Central Node расположены на разных серверах.
Если вы используете компонент Sensor в качестве прокси-сервера, убедитесь, что при интеграцииKaspersky Endpoint Detection and Response с программой Kaspersky Endpoint Agent на стороне Kaspersky Endpoint Agent (см. раздел "Настройка интеграции и доверенного соединения с Kaspersky Endpoint Detection and Response на стороне Kaspersky Endpoint Agent" на стр. 139) вместо IP-адреса Central Node вы указали IP-адрес Sensor.

В этом разделе

Включение и отключение перенаправления трафика от Endpoint Agent на сервер Sensor

► *Чтобы включить или отключить использование Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Agent и компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Sensor (см. раздел "Начало работы в меню администратора программы" на стр. 142):*

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.

3. Выберите пункт **Configure Central Node**.
4. Нажмите на клавишу **ENTER**.
5. В открывшемся окне укажите IP-адрес сервера с компонентом Central Node.
6. Нажмите на кнопку **Ok**.

   Откроется окно с информацией о сертификате компонента Central Node.
7. Убедитесь, что отображаемый сертификат совпадает с сертификатом компонента Central Node, который вы скачали.
8. Нажмите на кнопку **Accept**.
9. Если соединение с компонентом Central Node уже установлено или запрос на авторизацию отправлен, в открывшемся окне подтверждения действия нажмите на кнопку **Yes**.
10. В открывшемся окне **Update source** выполните одно из следующих действий:
    - Если вы хотите использовать сервер с компонентом Central Node в качестве источника обновления баз программы, нажмите на кнопку **Yes**.
    - Если вы не хотите использовать сервер с компонентом Central Node в качестве источника обновления баз программы, нажмите на кнопку **No**.
11. Если вы хотите использовать Sensor в качестве прокси-сервера, в открывшемся окне **Enable Proxy to Central Node** нажмите на кнопку **Yes**.

    Использование Sensor в качестве прокси-сервера будет включено после подтверждения авторизации на сервере с компонентом Central Node.
12. Если вы уже используете Sensor в качестве прокси-сервера и хотите отключить его, в открывшемся окне **Proxy to Central Node** нажмите на кнопку **Yes**.

    Использование Sensor в качестве прокси-сервера будет отключено после подтверждения авторизации на сервере с компонентом Central Node.

Авторизация Sensor на сервере Central Node

► *Чтобы авторизовать Sensor на сервере с компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Central Node (см. раздел "Начало работы в меню администратора программы" на стр. 142):*

1. В главном окне меню администратора выберите пункт **Program settings**.
2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.
3. Выберите пункт **Configure Sensor connections**.

   Откроется окно со списком запросов на авторизацию от серверов Sensor.
4. В нижней части окна выберите IP-адрес сервера Sensor, запрос на авторизацию от которого вы хотите подтвердить или отклонить.

   Откроется окно подтверждения авторизации.
5. Если вы хотите авторизовать выбранный сервер с Sensor, выберите пункт **Accept Sensor**.

   Запрос на авторизацию будет подтвержден.

6. Если вы хотите отклонить авторизацию выбранного сервера Sensor, выберите пункт **Reject Sensor**.

   Запрос на авторизацию будет отклонен.

Настройка интеграции и доверенного соединения с Kaspersky Endpoint Detection and Response на стороне Kaspersky Endpoint Agent

► *Чтобы настроить интеграцию с Kaspersky Endpoint Detection and Response на стороне Kaspersky Endpoint Agent, выполните следующие действия:*

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.
3. В блоке политик Kaspersky Endpoint Agent выберите нужную политику и откройте ее свойства двойным щелчком мыши.

   Откроются свойства выбранной политики.
4. В разделе **Интеграция с KATA** выберите подраздел **KATA Central Node**.
5. Установите флажок **Включить интеграцию с KATA**.
6. В поле **Адрес** введите адрес сервера Central Node программы Kaspersky Endpoint Detection and Response, с которым вы хотите настроить интеграцию, и выберите порт подключения. По умолчанию используется порт 443.
7. Установите флажок **Использовать доверенное соединение**.
8. Нажмите на кнопку **Добавить новый TLS-сертификат**.

   Откроется окно **Добавление TLS-сертификата**.
9. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Endpoint Detection and Response и скачанного на компьютер (см. раздел "Скачивание TLS-сертификата сервера Central Node на компьютер" на стр. 122):

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Обзор**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Open**.
   - Скопируйте содержание файла сертификата в поле **Вставьте текстовые данные TLS-сертификата**.

   В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Endpoint Detection and Response. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.
   Если вы настроили перенаправление трафика на сервер с компонентом Sensor, вам нужно загрузить TLS-сертификат сервера Sensor, предварительно скачанный на компьютер (см. раздел "Скачивание TLS-сертификата сервера Sensor на компьютер" на стр. 124).
10. Нажмите на кнопку **Добавить**.

    Информация о добавленном TLS-сертификате отобразится в разделе интеграции с Kaspersky Endpoint Detection and Response.

11. Нажмите на кнопку **Настроить дополнительную защиту**.
12. В открывшемся окне установите флажок **Защита подключения с помощью клиентского сертификата**.
13. Нажмите на кнопку **Загрузить**.

    Откроется окно выбора файла на вашем локальном компьютере.
14. Выберите файл крипто-контейнера сертификата Kaspersky Endpoint Agent, сгенерированного на сервере Kaspersky Endpoint Detection and Response и скачанного на жесткий диск вашего компьютера (см. раздел "Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Endpoint Detection and Response и скачивание крипто-контейнера" на стр. 132).
15. Нажмите на кнопку **OK**.

    Окно закроется.
16. В поле **Время ожидания** укажите максимальное время ожидания ответа сервера Central Node программы Kaspersky Endpoint Detection and Response в минутах.
17. В поле **Отправлять запрос на синхронизацию на сервер KATA каждые...** укажите интервал в минутах.
18. Если вы хотите, чтобы Kaspersky Endpoint Agent проверял, есть ли данные о предыдущих проверках объектов в кеше прежде, чем отправлять объекты на проверку в Kaspersky Endpoint Detection and Response, установите флажок **Использовать кеш события** и укажите время хранения результатов проверки объекта в кеше в секундах.
19. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Под политикой**.
20. Нажмите на кнопку **OK**.

Интеграция с Kaspersky Endpoint Detection and Response на стороне Kaspersky Endpoint Agent будет настроена.

kaspersky

Начало работы с программой

Этот раздел содержит информацию о том, как начать работу с программой в веб-интерфейсе, в меню администратора и в режиме Technical Support Mode.

В этом разделе

Начало работы в веб-интерфейсе программы

Веб-интерфейс Kaspersky Endpoint Detection and Response расположен на сервере с компонентом Central Node.

Веб-интерфейс Kaspersky Endpoint Detection and Response защищен от *CSRF-атак* (см. раздел "*CSRF-атака*" на стр. 494) и работает только в том случае, если браузер пользователя веб-интерфейса программы предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Kaspersky Endpoint Detection and Response, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом Kaspersky Endpoint Detection and Response осуществляется через прокси-сервер вашей организации, убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

► *Чтобы начать работу в веб-интерфейсе, выполните следующие действия:*

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, введите IP-адрес сервера с компонентом Central Node.

   Откроется окно ввода учетных данных пользователя программы.

2. Введите имя пользователя и пароль доступа к веб-интерфейсу программы, которые вы задали на этапе установки и настройки компонента Central Node.

Откроется страница **Мониторинг** веб-интерфейса программы.

Вы можете начать работу в веб-интерфейсе Kaspersky Endpoint Detection and Response.

Количество одновременных сеансов работы с программой под одной учетной записью ограничено одним IP-адресом. При попытке входа в программу под этим же именем пользователя с другого IP-адреса, первый сеанс работы с программой завершается.

kaspersky

Начало работы в меню администратора программы

Вы можете работать с параметрами каждого из компонентов программы Central Node и Sandbox в меню администратора в консоли управления каждого сервера, на котором установлен компонент программы.

Убедитесь, что доступ к меню администратора и консоли управления серверами Kaspersky Endpoint Detection and Response есть только с тех компьютеров, которым вы разрешили этот доступ.
Убедитесь, что компьютеры, которым вы разрешаете доступ, находятся в защищенном периметре вашей сети.
Вы можете настроить доступ к меню администратора и консоли управления серверами Kaspersky Endpoint Detection and Response с определенных компьютеров, с помощью утилиты командной строки iptables. Подробнее о работе с iptables см. документацию к iptables.

► *Чтобы начать работу в меню администратора компонента Sandbox или Central Node в консоли управления сервером с компонентом Sandbox или Central Node, выполните следующие действия:*

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы (см. стр. 91).

   Отобразится меню администратора компонента программы.

Вы можете начать работу в меню администратора компонента программы.

Начало работы с программой в режиме Technical Support Mode

Не рекомендуется выполнять действия с Kaspersky Endpoint Detection and Response в режиме Technical Support Mode без консультации или указания сотрудников Службы технической поддержки.

Вы можете работать с компонентами программы Central Node и Sandbox в режиме Technical Support Mode.

Режим Technical Support Mode предоставляет администратору Kaspersky Endpoint Detection and Response неограниченные права (root) доступа к программе и всем данным (в том числе персональным), которые в ней хранятся.

Работа с Kaspersky Endpoint Detection and Response из консоли управления в режиме Technical Support Mode (см. стр. 142) с правами учетной записи суперпользователя позволяет выполнять следующие действия:

- Управлять параметрами работы программы с помощью конфигурационных файлов.

При этом могут быть изменены параметры шифрования данных при передаче между узлами программы, параметры хранения и обработки объектов проверки.

В этом случае данные передаются в открытом виде. Администратору Kaspersky Endpoint Detection and Response необходимо обеспечить безопасность серверов с этими данными самостоятельно. Администратор Kaspersky Endpoint Detection and Response несет ответственность за изменение конфигурационных файлов программы.

- Управлять параметрами журнала трассировки.

Файлы трассировки могут содержать конфиденциальные данные пользователя.

► *Чтобы начать работу с программой в режиме Technical Support Mode, выполните следующие действия:*

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы (см. стр. 91).

   Отобразится меню администратора компонента программы.
3. В меню администратора программы выберите режим **Technical Support Mode**.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Если вы действительно хотите выполнять действия с программой в режиме Technical Support Mode, выберите **Yes** и нажмите на клавишу **ENTER**.

kaspersky

Управление учетными записями администраторов и пользователей программы

В Kaspersky Endpoint Detection and Response предусмотрены учетные записи для серверов со следующими компонентами:

- Sensor. Учетная запись администратора для работы в меню администратора программы и в консоли управления сервером (в режиме Technical Support Mode).

  По умолчанию используется учетная запись admin.

- Sandbox. Учетная запись администратора для работы в меню администратора программы, в консоли управления сервером (в режиме Technical Support Mode) и в веб-интерфейсе Sandbox.

  По умолчанию используется учетная запись admin.

- Central Node. Следующие учетные записи:

  - Учетная запись администратора для работы в меню администратора программы и в консоли управления сервером (в режиме Technical Support Mode).

    По умолчанию используется учетная запись admin, созданная при установке программы.

  - Учетная запись локального администратора веб-интерфейса программы.

    По умолчанию используется учетная запись Administrator, созданная при установке программы. Вы можете создать другие учетные записи администратора веб-интерфейса программы (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146) после установки.

  - Учетная запись администратора веб-интерфейса программы.

  - Учетные записи пользователей веб-интерфейса программы с ролями **Сотрудник службы безопасности** и **Старший сотрудник службы безопасности**.

Данные каждой из этих учетных записей хранятся на том сервере с компонентом программы, к которому она относится.

В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy данные каждой из этих учетных записей хранятся на PCN и на том сервере с компонентом программы, к которому она относится.

Учетная запись администратора для работы в консоли управления сервером обладает неограниченными правами на управление сервером с компонентом программы, к которому она относится (правами суперпользователя). Под этой учетной записью вы можете выключить или перезагрузить сервер, а также изменить параметры программы в режиме Technical Support Mode в консоли управления сервером.

Учетная запись администратора для работы в консоли управления сервером (admin) имеет неограниченный доступ к данным на этом сервере. Пароль учетной записи администратора для работы в консоли управления сервером должен быть надежным. Администратору необходимо обеспечить безопасность серверов самостоятельно. Администратор несет ответственность за доступ к данным, хранящимся на серверах.

Под учетной записью с ролью **Администратор** вы можете добавлять, включать и отключать учетные записи пользователей программы, а также изменять пароли учетных записей администраторов и пользователей веб-интерфейса программы. В режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy управление учетными записями пользователей осуществляется на PCN.

Учетная запись локального администратора веб-интерфейса программы предназначена для сотрудников вашей организации, в чьи обязанности входит управление Kaspersky Endpoint Detection and Response. При входе в программу под этой учетной записью отображаются все разделы веб-интерфейса, доступные пользователю с ролью **Администратор**.

Под учетной записью администратора веб-интерфейса программы можно управлять программой, но, в отличие от локального администратора веб-интерфейса программы, этой учетной записи недоступно управление серверами PCN и SCN, а также организациями в разделе **Режим работы**.

Роли **Сотрудник службы безопасности** и **Старший сотрудник службы безопасности** предназначены для сотрудников вашей организации, в чьи обязанности входит работа с событиями и задачами Kaspersky Endpoint Detection and Response. При входе в программу под учетными записями с этими ролями отображаются все разделы веб-интерфейса, доступные сотрудникам службы безопасности. Пользователю с ролью **Старший сотрудник службы безопасности** доступны все операции. Ограничения пользователей с ролью **Сотрудник службы безопасности** представлены в таблице ниже.

*Таблица 11. Ограничения доступа пользователей программы с ролью **Сотрудник службы безопасности***

Функциональная область / Раздел веб-интерфейса	Ограничения
Мониторинг	Недоступны графики событий группы VIP. Нет возможности перейти по ссылке на графике в раздел **Обнаружения**.
Обнаружения	Недоступны следующие действия: • просмотр информации об обнаружении; • отметка о завершении обработки обнаружения группы VIP; • операции над несколькими обнаружениями; • экспорт списка всех обнаружений.
Поиск угроз	Недоступны события, которые относятся к хостам из обнаружений группы VIP.
Задачи	Нет доступа.
Политики	Нет доступа.
Правила пользователей	Доступ на чтение.
Хранилище	Нет доступа к объектам, помещенным в Хранилище в результате выполнения задач. Полный доступ к объектам, загруженным пользователем вручную.

Функциональная область / Раздел веб-интерфейса	Ограничения
Endpoint Agents	Доступ к просмотру таблиц компьютеров с компонентом Endpoint Agent, ограничения по просмотру данных о задачах, о политиках и о сетевой изоляции.
Сетевая изоляция хостов	Нет доступа.
Отчеты	Нет доступа.
Параметры: Расписание IOC-проверки	Доступ на чтение.
Параметры: Endpoint Agents	Доступ на чтение.
Параметры: Репутационная база KPSN	Нет доступа.
Параметры: Отправка уведомлений	Нет доступа к правилам для отправки уведомлений об обнаружениях. Полный доступ к правилам отправки уведомлений о проблемах в работе программы.
Параметры: Статус VIP	Доступ на чтение.
Правила пользователей: YARA	Доступ только на экспорт правил.
Параметры: Исключения TAA	Доступ на чтение и экспорт.
Параметры: Пароли к архивам	Нет доступа.
Параметры: Лицензия	Доступ на чтение.

Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, то для каждой учетной записи вы можете разрешить или запретить доступ к организациям и веб-интерфейсу сервера SCN.

Создание учетной записи пользователя веб-интерфейса программы

Вы можете создавать учетные записи пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**.

► *Чтобы создать учетную запись пользователя веб-интерфейса программы, выполните следующие действия:*

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый пользователь**.
4. Если вы хотите включить учетную запись, включите переключатель **Состояние**.

   По умолчанию учетная запись включена.

Если учетная запись включена, доступ к веб-интерфейсу программы разрешен. Если учетная запись отключена, доступ к веб-интерфейсу программы запрещен.

5. В раскрывающемся списке **Роль** выберите одну из следующих ролей:
   - **Старший сотрудник службы безопасности**.
   - **Сотрудник службы безопасности**.
6. В поле **Имя пользователя** введите имя пользователя, учетную запись которого вы хотите создать.

   Имя пользователя должно удовлетворять следующим требованиям:
   - должно быть уникальным в списке имен пользователей (регистр имеет значение);
   - должно содержать максимум 32 символа;
   - может содержать буквы A-Z, a-z, цифры 0-9, дефис (-) или символ подчеркивания (_);
   - должно начинаться с буквы (A-Z или a-z).
7. В поле **Новый пароль** введите пароль доступа пользователя к веб-интерфейсу.

   Пароль должен удовлетворять следующим требованиям:
   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.
8. В поле **Подтвердите пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.
9. В разделе **Доступ** настройте права доступа:
   a. Включите переключатель **Веб-интерфейс SCN**, если вы хотите предоставить пользователю доступ не только к веб-интерфейсу этого сервера PCN, но и к веб-интерфейсам всех доступных серверов SCN.
   b. Справа от названия параметра **Организации** установите флажки рядом с названиями одной или нескольких организаций, к веб-интерфейсам серверов которых вы хотите предоставить доступ.

      Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех компаний.
10. Нажмите на кнопку **Добавить**.

Учетная запись пользователя программы будет создана.

kaspersky

Изменение прав доступа учетной записи пользователя веб-интерфейса программы

Вы можете изменить права доступа пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** к данным серверов PCN и SCN, а также организаций, связанных с этими серверами.

► *Чтобы изменить права доступа учетной записи пользователя веб-интерфейса программы, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. Выберите учетную запись, права доступа которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
4. Если вы хотите включить или отключить учетную запись, измените положение переключателя **Состояние**.
5. Если нужно, в разделе **Доступ** измените положение переключателя **Веб-интерфейс SCN**:
   - Переведите переключатель в положение **Включено**, если вы хотите предоставить пользователю доступ не только к веб-интерфейсу этого сервера PCN, но и к веб-интерфейсам всех доступных серверов SCN.
   - Переведите переключатель в положение **Отключено**, если вы хотите предоставить пользователю доступ только к веб-интерфейсу этого сервера PCN.
6. Справа от названия параметра **Организации** установите или снимите флажки рядом с названиями организаций, к веб-интерфейсам серверов которых вы хотите изменить доступ.

   Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех организаций.
7. Нажмите на кнопку **Сохранить**.

Права доступа учетной записи будут изменены.

Включение и отключение учетной записи администратора или пользователя веб-интерфейса программы

► *Чтобы включить или отключить учетную запись администратора или пользователя веб-интерфейса программы, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. В списке учетных записей выберите учетную запись пользователя, которую вы хотите включить или отключить.
4. Выполните одно из следующих действий в графе **Состояние**:
   - Включите переключатель рядом с именем учетной записи, если вы хотите включить учетную

запись.

- Выключите переключатель рядом с именем учетной записи, если вы хотите отключить учетную запись.

Отобразится окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Состояние учетной записи будет изменено.

Изменение пароля учетной записи администратора или пользователя программы

► *Чтобы изменить пароль учетной записи администратора или пользователя программы, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. В списке учетных записей выберите учетную запись, пароль которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
4. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу программы.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.
5. В поле **Подтвердите пароль** повторно введите новый пароль.
6. Нажмите на кнопку **Сохранить**.

Пароль учетной записи администратора или пользователя программы будет изменен.

Изменение пароля своей учетной записи

► *Чтобы изменить пароль своей учетной записи, выполните следующие действия:*

1. Войдите в веб-интерфейс под своей учетной записью.
2. В нижней части окна веб-интерфейса программы по ссылке с именем вашей учетной записи

раскройте список действий.

3. Выберите действие **Изменить пароль**.

   Откроется окно **Изменить пароль**.

4. В поле **Старый пароль** введите текущий пароль доступа к веб-интерфейсу программы.
5. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу программы.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.

6. В поле **Подтвердите пароль** повторно введите новый пароль.
7. Нажмите на кнопку **Изменить пароль**.

Пароль доступа к веб-интерфейсу программы вашей учетной записи будет изменен.

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Detection and Response использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (далее также "KSN") – это инфраструктура облачных служб, предоставляющая пользователям доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Detection and Response на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, данные о которых еще не вошли в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы, а также помогает другим пользователям Kaspersky Security Network оперативно получать информацию об угрозах IT-инфраструктуре предприятий.

Когда вы участвуете в Kaspersky Security Network, Kaspersky Endpoint Detection and Response отправляет в Kaspersky Security Network запросы о репутации файлов, интернет-ресурсов и программного обеспечения и получает ответ, содержащий данные о репутации этих объектов.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается на этапе установки Kaspersky Endpoint Detection and Response, его можно изменить в любой момент.

Подробнее об участии в Kaspersky Security Network вы можете прочитать в Положении о Kaspersky Security Network.

Если вы не хотите участвовать в KSN, вы можете использовать Kaspersky Private Security Network (далее также "KPSN") – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

По вопросам приобретения программы Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

Настройка участия в KSN производится на сервере Central Node.
Если вы используете режим распределенного решения и multitenancy, настраивайте участие в KSN на сервере PCN. Настройка участия в KSN распространится на все серверы SCN, подключаемые к PCN.

kaspersky

В этом разделе

Просмотр Положения о KSN и настройка участия в KSN

► *Чтобы настроить участие в Kaspersky Security Network, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Участие в KSN/KPSN**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **KSN**.
4. Ознакомьтесь с Положением о Kaspersky Security Network и выберите один из следующих вариантов:
   - **Я согласен участвовать в KSN**, если вы согласны с условиями Положения о KSN и хотите участвовать в KSN.
   - **Я не согласен участвовать в KSN**, если вы не согласны с условиями Положения о KSN и не хотите участвовать в KSN.

   Если вы не согласны с условиями Положения, использование Kaspersky Security Network не будет включено.
5. Нажмите на кнопку **Применить**.

Участие в Kaspersky Security Network будет настроено.

Создание учетной записи администратора веб-интерфейса программы

Под учетной записью администратора веб-интерфейса программы можно управлять программой, но, в отличие от локального администратора веб-интерфейса программы, этой учетной записи недоступно управление серверами PCN и SCN, а также организациями в разделе **Режим работы**.

► *Чтобы создать учетную запись администратора веб-интерфейса программы, выполните следующие действия:*

1. Войдите в веб-интерфейс под учетной записью администратора программы.

2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый пользователь**.
4. Если вы хотите включить учетную запись, включите переключатель **Состояние**.

   По умолчанию учетная запись включена.

   > Если учетная запись включена, доступ к веб-интерфейсу программы разрешен. Если учетная запись отключена, доступ к веб-интерфейсу программы запрещен.
5. В раскрывающемся списке **Роль** выберите **Администратор**.
6. В поле **Имя пользователя** введите имя пользователя, учетную запись которого вы хотите создать.

   Имя пользователя должно удовлетворять следующим требованиям:

   - должно быть уникальным в списке имен пользователей (регистр имеет значение);
   - должно содержать максимум 32 символа;
   - может содержать буквы A-Z, a-z, цифры 0-9, дефис (-) или символ подчеркивания (_);
   - должно начинаться с буквы (A-Z или a-z).
7. В поле **Новый пароль** введите пароль доступа к веб-интерфейсу.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.
8. В поле **Подтвердите пароль** повторно введите пароль доступа к веб-интерфейсу.
9. Нажмите на кнопку **Добавить**.

Учетная запись администратора веб-интерфейса программы будет создана.

Если вы используете режим multitenancy, учетная запись администратора веб-интерфейса сервера PCN имеет доступ к данным всех организаций, связанных с этим сервером.

kaspersky

Включение использования KPSN

► *Чтобы включить использование KPSN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Участие в KSN/KPSN**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **KPSN**.
4. В блоке **Конфигурационные файлы KPSN** загрузите файлы kc_private.xms, kh_private.xms и ksncli_private.dat с помощью кнопки **Обзор**.
5. Нажмите на кнопку **Применить**.

Использование Kaspersky Private Security Network будет включено.

Настройка подключения к локальной репутационной базе KPSN

Программа может сохранять информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить подключение Kaspersky Endpoint Detection and Response к локальной репутационной базе KPSN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Репутационная база KPSN**.
3. В поле **Хост** укажите IP-адрес сервера KPSN, на котором хранится локальная репутационная база KPSN.
4. Нажмите на кнопку **Обзор** справа от поля **TLS-сертификат**.

   Откроется окно выбора файлов.
5. Выберите файл сертификата для аутентификации пользователей в KPSN и нажмите на кнопку **Открыть**.
6. Нажмите на кнопку **Обзор** справа от поля **TLS-ключ шифрования**.

   Откроется окно выбора файлов.
7. Выберите файл, содержащий закрытый ключ шифрования, и нажмите на кнопку **Открыть**.

Подключение к локальной репутационной базе KPSN будет настроено.

kaspersky

Настройка сохранения информации в локальную репутационную базу KPSN

Программа может сохранять MD5- и SHA256-хеши объектов, обнаруженных компонентом Sandbox, в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

► *Чтобы настроить сохранение информации об обнаружениях в локальную репутационную базу KPSN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью старшего сотрудника службы безопасности.
2. Выберите раздел **Параметры**, подраздел **Репутационная база KPSN**.
3. Выполните одно из следующих действий:
   - Включите переключатель **Присваивать объектам статус "Недоверенный"**, если вы хотите, чтобы программа присваивала обнаружениям статус *Недоверенный* и сохраняла информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN.
   - Выключите переключатель **Присваивать объектам статус "Недоверенный"**, если вы не хотите сохранять информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN.
4. Нажмите на кнопку **Сохранить**.

Настройка сохранения информации в локальную репутационную базу KPSN будет выполнена.

Отказ от участия в KSN и использования KPSN

► *Чтобы отказаться от участия в Kaspersky Security Network и использования KPSN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Участие в KSN/KPSN**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **Не подключен**.
4. Нажмите на кнопку **Применить**.

Вы не будете участвовать в KSN и использовать KPSN.

kaspersky

Работа с компонентом Sandbox через веб-интерфейс

Веб-интерфейс Sandbox расположен на сервере с компонентом Sandbox.

Веб-интерфейс Sandbox защищен от *CSRF-атак* (см. раздел "*CSRF-атака*" на стр. 494) и работает только в том случае, если браузер пользователя веб-интерфейса предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Sandbox, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом осуществляется через прокси-сервер вашей организации, проверьте параметры и убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

► *Чтобы начать работу в веб-интерфейсе Sandbox, выполните следующие действия:*

1. В браузере на любом компьютере, на котором разрешен доступ к серверу с компонентом Sandbox, введите IP-адрес сервера с компонентом Sandbox (см. стр. 99).

   Откроется окно ввода учетных данных администратора компонента Sandbox.

2. Введите имя пользователя и пароль администратора компонента Sandbox, который вы задали при установке компонента Sandbox.

Вы можете начать работу в веб-интерфейсе Sandbox.

Если вы используете несколько серверов с компонентом Sandbox, производите настройку параметров каждого компонента Sandbox из веб-интерфейса Sandbox этого сервера.

В этом разделе

kaspersky

Обновление баз компонента Sandbox

Базы компонента Sandbox представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код и признаки подозрительного поведения объектов.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений автоматически один раз в час или обновлять базы вручную.

В этом разделе

Запуск обновления баз вручную

► *Чтобы запустить обновление баз вручную, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.

   В блоке параметров **Последнее обновление** отобразятся время и статус последней попытки обновления баз Sandbox.

2. Нажмите на кнопку **Запустить**.

Выбор источника обновления баз

► *Чтобы выбрать источник обновления баз, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. В блоке параметров **Источник обновлений** выберите источник, из которого вы хотите получать пакет обновлений:

   - **Сервер обновлений "Лаборатории Касперского"**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.

   - **Сервер обновлений "Лаборатории Касперского" (безопасное подключение)**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется выполнять обновления баз по протоколу

HTTPS.

- **Другой сервер**.

  Программа будет подключаться к папке с базами программы по протоколу HTTP и загружать актуальные базы.

3. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите URL-адрес пакета обновлений на вашем FTP- или HTTP-сервере или укажите полный путь к директории с пакетом обновлений.
4. Нажмите на кнопку **Применить** в нижней части окна.

Включение и отключение использования прокси-сервера для обновления баз

► *Чтобы включить или отключить использование прокси-сервера для обновления баз компонента Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. В рабочей области выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы хотите использовать прокси-сервер при обновлении баз компонента Sandbox.
   - Выключите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы не хотите использовать прокси-сервер при обновлении баз компонента Sandbox.

Настройка параметров соединения с прокси-сервером для обновления баз

► *Чтобы настроить параметры соединения с прокси-сервером для обновления баз компонента Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. Включите переключатель рядом с названием блока параметров **Прокси-сервер**.
3. В поле **Адрес** введите адрес прокси-сервера.
4. В поле **Порт** укажите номер порта прокси-сервера.
5. В поле **Имя пользователя** введите имя пользователя прокси-сервера.
6. В поле **Пароль** введите пароль подключения к прокси-серверу.
7. Выполните одно из следующих действий:
   - Установите флажок **Не использовать прокси-сервер для локальных адресов**, если вы не хотите использовать прокси-сервер для внутренних адресов электронной почты вашей организации.
   - Снимите флажок **Не использовать прокси-сервер для локальных адресов**, если вы хотите использовать прокси-сервер независимо от принадлежности адресов электронной почты к вашей организации.
8. Нажмите на кнопку **Применить** в нижней части окна.

kaspersky

Настройка соединения компонентов Sandbox и Central Node

Предусмотрен следующий порядок настройки соединения компонента Sandbox с компонентом Central Node:

1. В меню администратора или в веб-интерфейсе каждого сервера с компонентом Central Node создается запрос на подключение к компоненту Sandbox.
2. В веб-интерфейсе Sandbox отображаются запросы на подключение.

   Вы можете принять или отклонить каждый запрос.

Создание запроса на подключение к Sandbox в меню администратора Central Node

Для создания соединения между компонентами Central Node и Sandbox, необходимо отправить запрос на подключение к компоненту Sandbox с каждого компонента Central Node.

► *Чтобы создать запрос на подключение к компоненту Sandbox, выполните следующие действия:*

1. Зайдите в консоль сервера Central Node, с которого вы хотите создать запрос на подключение к Sandbox, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя пользователя admin и пароль, заданный при установке и настройке компонента Central Node (см. раздел "Шаг 2. Создание учетной записи для работы в меню администратора и в консоли управления сервером" на стр. 103).

   Отобразится меню администратора программы.
3. В меню администратора программы выберите **Program Settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действия.
5. Выберите действие **Configure Sandbox connection**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно **Sandbox access**.
7. Выберите **New**.
8. Нажмите на клавишу **ENTER**.

   Откроется окно **Sandbox node**.
9. В поле **Sandbox name** введите доменное имя сервера Sandbox, запрос на подключение к которому вы создаете.
10. В поле **Sandbox node** введите IP-адрес сервера Sandbox, запрос на подключение к которому вы создаете.
11. Нажмите на кнопку **Ok**.

    Откроется окно выбора действия.
12. Выберите строку с IP-адресом сервера Sandbox.
13. Нажмите на клавишу **ENTER**.

14. Откроется окно **Sandbox key fingerprint**, содержащее отпечаток сертификата Sandbox и просьбу подтвердить подлинность отпечатка сертификата.
15. Убедитесь, что отпечаток сертификата соответствует отпечатку сертификата в веб-интерфейсе Sandbox, запрос на подключение к которому вы создаете.
16. После того, как вы убедились, что отпечатки сертификатов идентичны, нажмите на кнопку **Yes**.

    Откроется окно подтверждения отправки запроса на подключения к компоненту Sandbox.
17. Нажмите на кнопку **Yes**.

    Вы вернетесь к окну выбора действия с IP-адресом сервера Sandbox.

Если запрос на подключение к компоненту Sandbox отправлен успешно, напротив названия параметра Enabled отобразится значение **Yes**.

Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox

Вы можете принять, отклонить или отозвать ранее принятый запрос на подключение от серверов Central Node в веб-интерфейсе Sandbox.

► *Чтобы принять, отклонить или отозвать запрос на подключение от серверов Central Node, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Авторизация KATA**.

   В разделе **Запросы на подключение от Central Node** отобразится список запросов на подключение от компонентов Central Node.

   В каждом запросе на подключение содержится следующая информация:

   - **IP** – IP-адрес сервера Central Node.
   - **Отпечаток сертификата** – отпечаток TLS-сертификата Cental Node, с помощью которого устанавливается шифрованное соединение между серверами.
   - **Состояние** – состояние запроса на подключение.

     Может иметь значения **Ожидание** или **Принят**.
2. Убедитесь, что отпечаток сертификата Cental Node соответствует отпечатку сертификата на стороне Cental Node.

   Вы можете проверить отпечаток сертификата Central Node в меню администратора сервера Central Node в разделе **Manage server certificate**.
3. Нажмите на одну из следующих кнопок в строке с запросом на подключение от компонента Central Node:

   - **Принять**, если вы хотите принять запрос на подключение.
   - **Отклонить**, если вы хотите отклонить запрос на подключение.
   - **Отозвать**, если вы хотите отозвать ранее принятый запрос на подключение.
4. Нажмите на кнопку **Применить** в нижней части окна.

kaspersky

Настройка сетевых интерфейсов компонента Sandbox

В этом разделе содержится информация о настройке сетевых интерфейсов компонента Sandbox.

Настройка параметров DNS

► *Чтобы настроить параметры DNS, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В поле **Имя хоста** введите имя сервера, на который вы устанавливаете компонент Sandbox, в формате FQDN (например, sandbox).
3. Справа от названия параметра **DNS-серверы** нажмите на кнопку **Добавить**.

   Добавится пустое поле ввода IP-адреса DNS-сервера.
4. Введите IP-адрес основного DNS-сервера в формате IPv4.
5. Нажмите на кнопку ✓ справа от поля ввода.

   DNS-сервер будет добавлен.
6. Если вы хотите добавить дополнительный DNS-сервер, повторите действия 2-5.
7. Если вы хотите удалить добавленный DNS-сервер, нажмите на кнопку 🗑 справа от строки с IP-адресом DNS-сервера.

   Вы можете удалить только дополнительные DNS-серверы. Вы не можете удалить основной DNS-сервер. Если вы добавили 2 и более DNS-сервера, вы можете удалить любой из них, при этом оставшийся DNS-сервер будет использоваться в качестве основного.

Настройка параметров управляющего сетевого интерфейса

Управляющий сетевой интерфейс предназначен для доступа к серверу с компонентом Sandbox по протоколу SSH, также через этот интерфейс компонент Sandbox будет принимать объекты от компонента Central Node.

Вы можете настроить управляющий сетевой интерфейс во время установки компонента Sandbox (см. раздел "Шаг 4. Выбор управляющего сетевого интерфейса в списке" на стр. 98).

Вы также можете настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox.

► *Чтобы настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Управляющий интерфейс** в раскрывающемся списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу, если IP-адрес не назначен.

4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. Нажмите на кнопку **Применить** в нижней части окна.

Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет

Объекты, которые обрабатывает компонент Sandbox, могут предпринимать попытки действий в интернете через сетевой интерфейс для доступа обрабатываемых объектов в интернет. Компонент Sandbox может анализировать поведение этих объектов.

Если вы запретите доступ в интернет, компонент Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

Сетевой интерфейс для доступа обрабатываемых объектов в интернет должен быть изолирован от локальной сети вашей организации.

Если в соответствии с политикой безопасности вашей организации с компьютеров пользователей локальной сети запрещен доступ в интернет, и вы настроили сетевой интерфейс Sandbox для доступа обрабатываемых объектов в интернет, есть риск возникновения следующего сценария: Злоумышленник может прикрепить вредоносную программу к произвольному файлу и запустить Sandbox-проверку этого файла с компьютера пользователя локальной сети. Этот файл будет выведен за пределы локальной сети через сетевой интерфейс для доступа обрабатываемых объектов в интернет в процессе проверки файла компонентом Sandbox.

Отсутствие сетевого интерфейса Sandbox для доступа обрабатываемых объектов в интернет исключает риски подобной передачи информации, однако снижает качество обнаружений.

► *Чтобы настроить сетевой интерфейс для доступа обрабатываемых объектов в интернет, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Интерфейс для выхода в интернет** в списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать для доступа обрабатываемых объектов в интернет.

   Управляющий сетевой интерфейс, которые вы настроили ранее, недоступен для выбора в этом списке сетевых интерфейсов.
3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. В поле **Шлюз по умолчанию** введите адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
6. Нажмите на кнопку **Применить** в нижней части окна.

kaspersky

Добавление, изменение и удаление статических сетевых маршрутов

Вы можете настроить статические сетевые маршруты во время установки компонента Sandbox.

Вы также можете добавить, удалить или изменить статические сетевые маршруты в веб-интерфейсе Sandbox.

► *Чтобы добавить статический сетевой маршрут, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** нажмите на кнопку **Добавить**.

   В списке статических сетевых маршрутов добавится строка с пустыми полями.
3. В поле **IP** введите IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
4. В поле **Маска** введите маску подсети.
5. В поле **Шлюз** введите IP-адрес шлюза.
6. В списке **Интерфейс** выберите сетевой интерфейс, для которого вы хотите добавить статический сетевой маршрут.
7. Нажмите на кнопку ✓.
8. Нажмите на кнопку **Применить** в нижней части окна.

► *Чтобы удалить статический сетевой маршрут, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите удалить, нажмите на кнопку 🗑.
3. Нажмите на кнопку **Применить** в нижней части окна.

► *Чтобы изменить статический сетевой маршрут, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите изменить, нажмите на кнопку ✎.

   Строка статического сетевого маршрута станет доступна для редактирования. Вы можете изменить один или несколько параметров статического сетевого маршрута.
3. В поле **IP** измените IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
4. В поле **Маска** измените маску подсети.
5. В поле **Шлюз** измените IP-адрес шлюза.
6. В списке **Интерфейс** выберите сетевой интерфейс, для которого вы редактируете сетевой маршрут.
7. Нажмите на кнопку ✓.
8. Нажмите на кнопку **Применить** в нижней части окна.

kaspersky

Обновление системы Sandbox

"Лаборатория Касперского" может выпускать пакеты обновлений Kaspersky Endpoint Detection and Response и отдельных компонентов программы. Например, могут выпускаться срочные пакеты обновлений, устраняющие уязвимости и ошибки, плановые обновления, добавляющие новые или улучшающие существующие функции программы и ее компонентов.

После выпуска обновлений Sandbox вы можете установить их через веб-интерфейс Sandbox.

Перед установкой обновлений через веб-интерфейс Sandbox вам нужно загрузить пакет обновления в формате TGZ и инструкцию по установке данного обновления с сайта "Лаборатории Касперского" на ваш компьютер.

► *Чтобы обновить систему Sandbox через веб-интерфейс, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление системы**.

   Справа от названия параметра **Текущая версия программы** отобразится текущая версия компонента Sandbox.
2. Нажмите на кнопку **Обзор** справа от поля **Пакет обновления**.

   Откроется окно выбора файлов.
3. Выберите файл обновления, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Вы можете следить за ходом обновления системы Sandbox в окне **Журнал обновлений** раздела **Обновление системы** веб-интерфейса Sandbox.

Пакет обновления будет установлен автоматически. Процесс обновления может занять несколько минут. Сервер Sandbox перезагрузится. Компонент Sandbox будет недоступен во время обновления системы.

Установка даты и времени системы Sandbox

► *Чтобы установить дату и время сервера с компонентом Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Дата и время**.
2. В раскрывающемся списке **Страна** выберите нужную страну.
3. В раскрывающемся списке **Часовой пояс** выберите нужный часовой пояс.
4. Если вы хотите синхронизировать время с NTP-сервером, включите переключатель справа от названия параметра **Синхронизация с NTP-серверами**.
5. Если вы хотите установить дату и время вручную, не включайте переключатель справа от названия параметра **Синхронизация с NTP-серверами** и выполните следующие действия:

   a. В поле **Дата** введите текущую дату или нажмите на кнопку и выберите дату в календаре.

b. В поле **Время** введите текущее время.

6. Нажмите на кнопку **Применить** в нижней части окна.

Установка и настройка образов операционных систем и программ для работы компонента Sandbox

В комплекте поставки вы получаете три ISO-образа операционных систем Windows XP SP3, 64-разрядной Windows 7, 64-разрядной Windows 10 и программ, необходимых для работы компонента Sandbox. Вам не требуется активировать эти операционные системы и программ. В поставляемых образах уже добавлен лицензионный ключ Microsoft.

Компонент Sandbox будет запускать объекты в этих операционных системах и анализировать поведение объектов для выявления вредоносной активности, признаков целевых атак и вторжений в IT-инфраструктуру организации.

При возникновении проблем с активацией операционных систем или программ в веб-интерфейсе компонента Sandbox отобразится сообщение об ошибке. В этом случае рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Загрузка ISO-образов операционных систем и программ для работы компонента Sandbox

► *Чтобы загрузить ISO-образ операционной системы и программ, необходимых для работы компонента Sandbox, выполните следующие действия для каждого ISO-образа:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В группе параметров **Образы виртуальных машин** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
3. Выберите файл формата ISO, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

В списке **Образы виртуальных машин** отобразится загруженный образ операционной системы и программ, необходимых для работы компонента Sandbox.

Выполните действия по загрузке образов операционных систем и программ, необходимых для работы компонента Sandbox, для каждого ISO-образа.

Создание виртуальных машин с образами операционных систем и программ для работы компонента Sandbox

► *Чтобы создать виртуальную машину с образом операционной системы и программ,*

необходимых для работы компонента Sandbox, выполните следующие действия для каждой виртуальной машины:

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В списке **Образы виртуальных машин** в строке с названием образа операционной системы и программ для работы компонента Sandbox нажмите на кнопку **Создать VM**.

   Откроется окно **Лицензионное соглашение**, содержащее тексты следующих лицензионных соглашений:

   - MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1.
   - MICROSOFT WINDOWS XP PROFESSIONAL EDITION SERVICE PACK 3.
   - MICROSOFT OFFICE 2010 DESKTOP APPLICATION SOFTWARE.
   - MICROSOFT OFFICE 2007 DESKTOP APPLICATION SOFTWARE.
   - MICROSOFT OFFICE 2003 DESKTOP APPLICATION SOFTWARE.
   - ADOBE® Personal Computer Software License Agreement.
   - MICROSOFT VISUAL C++ 2005 RUNTIME LIBRARIES.
   - MICROSOFT VISUAL C++ 2008 RUNTIME LIBRARIES (X86, IA64 AND X64), SERVICE PACK 1.
   - MICROSOFT VISUAL C++ 2010 RUNTIME LIBRARIES.
   - MICROSOFT VISUAL C++ 2012 RUNTIME LIBRARIES.
   - MICROSOFT VISUAL C++ REDISTRIBUTABLE FOR VISUAL STUDIO 2013.
   - MICROSOFT VISUAL STUDIO 2017 TOOLS, ADD-ONs and C++ REDISTRIBUTABLE.
3. Ознакомьтесь с текстами лицензионных соглашений и нажмите на кнопку **Принять** в правом нижнем углу окна **Лицензионное соглашение**.

   Откроется окно **Unpack**. Архив с образом операционной системы и программ для работы компонента Sandbox будет распакован.
4. В списке **Не установленные виртуальные машины** окна **Виртуальные машины** появится виртуальная машина, готовая к активации операционных систем и программ, а также к установке.

Выполните действия по созданию виртуальных машин с образами операционных систем и программ для работы компонента Sandbox для каждой виртуальной машины.

Установка виртуальных машин с образами операционных систем и программ для работы компонента Sandbox

► *Чтобы установить все готовые к установке виртуальные машины с образами операционных систем и программ для работы компонента Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В левом нижнем углу списка **Не установленные виртуальные машины** нажмите на кнопку

Установить готовые VM.

Виртуальные машины с операционными системами, рядом с названиями которых в списке **Не установленные виртуальные машины** отображается статус **Готова к установке**, будут установлены и отобразятся в списке в верхней части окна **Виртуальные машины**.

Удаление всех виртуальных машин, ожидающих установки

► *Чтобы удалить все виртуальные машины, ожидающие установки, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В левом нижнем углу списка **Не установленные виртуальные машины** нажмите на кнопку **Удалить все ожидающие VM**.

   Виртуальные машины с операционными системами и программами для работы компонента Sandbox, ожидающие установки, будут удалены.

Установка максимального количества одновременно запускаемых виртуальных машин

Задайте ограничение для количества одновременно запускаемых виртуальных машин с операционными системами, в которых компонент Sandbox будет обрабатывать объекты.

Количество одновременно запускаемых виртуальных машин не может превышать 200.

Рассчитывайте количество одновременно запускаемых виртуальных машин с образами операционных систем следующим образом: количество ядер процессора нужно умножить на 1,5.

► *Чтобы установить максимальное количество одновременно запускаемых виртуальных машин, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В группе параметров **Гостевые виртуальные машины** в поле **Максимум VM одновременно** введите количество одновременно запускаемых виртуальных машин.

   Вы можете ввести число от 1 до 200.
3. Нажмите на кнопку **Сохранить**.

Загрузка журнала системы Sandbox на жесткий диск

Данные в журнале системы Sandbox хранятся в открытом незашифрованном виде. Данные хранятся за последние 7 дней.

► *Чтобы загрузить журнал системы Sandbox на жесткий диск, выполните следующие*

действия:

1. В окне веб-интерфейса Sandbox выберите раздел **Общая информация**.
2. В группе параметров **Журнал системы** нажмите на кнопку **Скачать**.
3. Журнал системы Sandbox загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы с программой.

Экспорт параметров Sandbox

► *Чтобы экспортировать параметры системы Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Общая информация**.
2. В группе параметров **Параметры** нажмите на кнопку **Экспортировать**.

   Откроется окно **Предупреждение**, содержащее предупреждение об особенностях экспорта параметров системы.

   Параметры системы Sandbox зависят от аппаратных и программных параметров сервера, на котором установлен компонент Sandbox. Экспортируемые параметры системы Sandbox предназначены для импорта на этот же или строго идентичный по конфигурации сервер. Попытки восстановить конфигурацию системы Sandbox значениями параметров, сохраненными на другой системе Sandbox, могут нарушить работу системы Sandbox.

3. Нажмите на кнопку **Сохранить**.

Файл формата tar.gz загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы программы. В файле содержатся все текущие параметры системы Sandbox.

Архивы с резервной копией параметров системы могут содержать такие конфиденциальные данные, как, например, пароли, закрытые ключи. Администратору Kaspersky Endpoint Detection and Response необходимо обеспечить безопасность этих данных самостоятельно.

Импорт параметров Sandbox

► *Чтобы импортировать параметры Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Общая информация**.
2. В группе параметров **Параметры** нажмите на кнопку **Импортировать**.

   Откроется окно **Предупреждение**, содержащее предупреждение об особенностях импорта параметров системы.

Параметры компонента Sandbox зависят от аппаратных и программных параметров сервера, на котором установлен Sandbox. Экспортируемые параметры Sandbox предназначены для импорта на этот же или строго идентичный по конфигурации сервер. Попытки восстановить конфигурацию одной системы Sandbox настройками параметров, сохраненными на другой системе Sandbox, могут нарушить работу системы.

3. Нажмите на кнопку **Восстановить**.

   Откроется окно выбора файлов.

4. Выберите файл формата tar.gz с параметрами Sandbox, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

   Если импорт параметров Sandbox прошел успешно, сервер Sandbox перезагрузится. Через несколько минут вам нужно обновить окно браузера и повторить вход.

Архивы с резервной копией конфигурации системы могут содержать такие конфиденциальные данные, как, например, пароли, закрытые ключи. Администратору Kaspersky Endpoint Detection and Response необходимо обеспечить безопасность хранения этих данных самостоятельно.

Перезагрузка сервера Sandbox

► *Чтобы перезагрузить сервер Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Общая информация**.
2. В группе параметров **Питание** нажмите на кнопку **Перезагрузить**.

   Откроется окно подтверждения перезагрузки сервера Sandbox.
3. Нажмите на кнопку **Да**.

Сервер Sandbox перезагрузится. Через несколько минут вы сможете войти в систему.

Выключение сервера Sandbox

► *Чтобы выключить сервер Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Общая информация**.
2. В группе параметров **Питание** нажмите на кнопку **Выключить**.

   Откроется окно подтверждения выключения сервера Sandbox.
3. Нажмите на кнопку **Да**.

Сервер Sandbox выключится.

Изменение пароля учетной записи администратора Sandbox

► *Чтобы изменить пароль учетной записи администратора Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Общая информация**.
2. В блоке параметров **Изменить пароль** отобразится имя учетной записи администратора Sandbox, которое вы задали при установке Sandbox и поля для изменения пароля.
3. В поле **Текущий пароль** введите текущий пароль учетной записи администратора Sandbox.
4. В поле **Новый пароль** введите новый пароль учетной записи администратора Sandbox.
5. В поле **Подтвердите пароль** введите новый пароль учетной записи администратора Sandbox повторно.
6. Нажмите на кнопку **Изменить пароль**.

   Пароль учетной записи администратора Sandbox будет изменен.

kaspersky

Администратору: работа в веб-интерфейсе программы

Этот раздел адресован специалистам, которые осуществляют установку и администрирование Kaspersky Endpoint Detection and Response, а также управление серверами PCN и SCN и организациями в режиме распределенного решения и multitenancy.

В этом разделе

Интерфейс Kaspersky Endpoint Detection and Response

Работа с программой осуществляется через веб-интерфейс. Разделы веб-интерфейса программы различаются в зависимости от роли пользователя – **Администратор** или **Старший сотрудник службы безопасности / Сотрудник службы безопасности** (см. раздел "**Сотруднику службы безопасности: работа в веб-интерфейсе программы**" на стр. 210).

Окно веб-интерфейса программы содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса программы;
- закладки в верхней части окна веб-интерфейса программы для некоторых разделов программы;
- рабочую область в нижней части окна веб-интерфейса программы.

Разделы окна веб-интерфейса программы

Веб-интерфейс программы для роли **Администратор** разделен на следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Endpoint Detection and Response.
- **Режим работы**. Содержит информацию о серверах PCN и SCN, об организациях в режиме распределенного решения и multitenancy.
- **Endpoint Agents**. Содержит информацию о подключенных компонентах Endpoint Agent и их параметры.

- **Параметры**. Содержит параметры сервера с компонентом Central Node.
- **Серверы Sandbox**. Содержит информацию о подключении компонента Central Node к компонентам Sandbox.
- **Внешние системы**. Содержит информацию об интеграции программы с почтовыми сенсорами.

Рабочая область окна веб-интерфейса программы

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса программы, а также элементы управления, с помощью которых вы можете настроить отображение информации.

kaspersky

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью графиков в разделе **Мониторинг** окна веб-интерфейса программы. Вы можете добавлять, удалять, перемещать графики, настраивать масштаб отображения графиков и выбирать период отображения данных.

В этом разделе

О графиках и схемах расположения графиков

С помощью графиков вы можете осуществлять мониторинг работы программы.

Схема расположения графиков – вид рабочей области окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать графики на схеме расположения графиков.

В программе доступны следующие графики:

- **Обработано**. Отображение состояния обработки трафика, поступающего от Endpoint Agent на сервер с компонентом Central Node.
- **Очереди**. Отображение сведений о количестве и объеме объектов, ожидающих проверки модулями и компонентами программы.
- **Время обработки в Sandbox** (см. раздел "**Мониторинг обработки данных компонентом Sandbox**" на стр. 178). Отображение среднего времени, за которое были получены результаты проверки объектов компонентом Sandbox.

Если вы используете режим multitenancy, в разделе отображаются данные по выбранной вами организации и серверу (см. раздел "Выбор организации и сервера для работы в разделе Мониторинг" на стр. 175).

kaspersky

Выбор организации и сервера для работы в разделе Мониторинг

Если вы используете режим multitenancy, перед началом работы в разделе **Мониторинг** вам нужно выбрать организацию и сервер, данные по которым вы хотите просмотреть.

► *Чтобы выбрать организацию и сервер для отображения данных в разделе **Мониторинг**, выполните следующие действия:*

1. В правой верхней части окна веб-интерфейса программы нажмите на стрелку рядом с именем сервера.
2. В раскрывшемся меню выберите организацию и нужный вам сервер из списка.

Отобразятся данные по выбранному вами серверу. Если вы хотите изменить организацию и сервер, вам нужно повторить действия по выбору организации и сервера.

Добавление графика на текущую схему расположения графиков

► *Чтобы добавить график на текущую схему расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на кнопку **Графики**.
5. В появившемся окне **Настроить графики** выполните следующие действия:
   - Если вы хотите добавить график **Очереди**, включите переключатель рядом с названием этого графика.
   - Если вы хотите добавить график **Время обработки в Sandbox**, включите переключатель рядом с названием этого графика.
   - Если вы хотите добавить график **Обработано**, нажмите на кнопку  рядом с названием этого графика.

Выбранный график будет добавлен на текущую схему расположения графиков.

Перемещение графика на текущей схеме расположения графиков

► *Чтобы переместить график на текущей схеме расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .

3. В раскрывающемся списке выберите **Изменить**.
4. Выберите график, который вы хотите переместить на схеме расположения графиков.
5. Нажав и удерживая левую клавишу мыши на верхней части графика, перетащите график на другое место схемы расположения графиков.
6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения графиков будет сохранена.

Удаление графика с текущей схемы расположения графиков

► *Чтобы удалить график с текущей схемы расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок × в правом верхнем углу графика, который вы хотите удалить со схемы расположения графиков.

   График будет удален из рабочей области окна веб-интерфейса программы.
5. Нажмите на кнопку **Сохранить**.

График будет удален с текущей схемы расположения графиков.

Сохранение схемы расположения графиков в PDF

► *Чтобы сохранить схему расположения графиков в PDF, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Сохранить как PDF**.

   Откроется окно **Сохранение в PDF**.
4. В нижней части окна в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.

   Схема расположения графиков в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.
6. Нажмите на кнопку **Закрыть**.

kaspersky

Настройка периода отображения данных на графиках

Вы можете настроить отображение данных на графиках за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

► *Чтобы настроить отображение данных на графиках за сутки (с 00:00 до 23:59), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за неделю (с понедельника по воскресенье), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за месяц (календарный месяц), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

Мониторинг приема и обработки входящих данных

На графике **Обработано** вы можете оценить статус обработки данных, поступающих от компонентов Sensor и Endpoint Agent на сервер с компонентом Central Node, и отследить ошибки обработки данных.

Вы можете выбрать компонент (Sensor или Endpoint Agent), поступление данных с которого вы хотите оценить, в раскрывающемся списке справа от названия графика **Обработано**.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия компонента

(Sensor или Endpoint Agent):

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на графиках (см. раздел "Настройка периода отображения данных на графиках" на стр. 177).

В левой части каждого графика отображается легенда графика по цветам, которые используются на самих графиках.

Если выбран тип отображения данных **Текущая загрузка**, справа от легенды отображается средняя скорость обработки данных за последние 5 минут.

Если выбран тип отображения данных **Выбранный период**, справа от легенды отображается средняя скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов за выбранный период.

Мониторинг очередей обработки данных модулями и компонентами программы

На графике **Очереди** вы можете оценить статус обработки данных модулями программы **YARA**, **AM Engine**, компонентом **Sandbox** и отследить объем необработанных данных.

Передача данных в очереди измеряется сообщениями.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия графика **Очереди**:

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на графиках.

В левой части графика отображается легенда графика по цветам, которые используются на графике.

На графике **Очереди** отображаются следующие данные:

- **Количество сообщений** и **Объем данных**, обработанных модулями и компонентами программы:
  - **YARA** – синим цветом.
  - **Sandbox** – фиолетовым цветом.
  - **AM Engine** – зеленым цветом.
- **Не обработано** – объем необработанных данных вертикальными линиями красного цвета.

При наведении курсора мыши на график появляется всплывающее окно, в котором отображается статус обработки данных модулями программы **YARA**, **AM Engine** и компонентом **Sandbox**, а также объем необработанных данных в определенное время.

Мониторинг обработки данных компонентом Sandbox

На графике **Время обработки в Sandbox** отображается среднее время, прошедшее от момента отправки данных на один или несколько серверов с компонентом Sandbox (включая время ожидания отправки) до отображения результатов обработки данных компонентом Sandbox в веб-интерфейсе Kaspersky Endpoint

Detection and Response в выбранный период.

Пример:

Если настроен период отображения данных на графиках **Месяц**, на графике **Время обработки в Sandbox** отображаются столбики оранжевого цвета на каждый день месяца.

При наведении курсора мыши на каждый столбик появляется всплывающее окно, в котором отображается среднее время, прошедшее от момента отправки данных на один или несколько серверов с компонентом Sandbox до отображения результатов обработки данных компонентом Sandbox в веб-интерфейсе Kaspersky Endpoint Detection and Response в выбранный день.

Вы можете увеличить скорость обработки данных компонентом Sandbox и пропускную способность компонента Sandbox, увеличив количество серверов с компонентом Sandbox и распределив по этим серверам данные, предназначенные для обработки.

Просмотр состояния работоспособности модулей и компонентов программы

Если в работе модулей и компонентов программы возникли проблемы, на которые администратору рекомендуется обратить внимание, в верхней части окна раздела **Мониторинг** веб-интерфейса программы отображается рамка желтого цвета с предупреждениями.

Пользователю с ролью **Локальный администратор** или **Администратор** доступна информация о работоспособности того сервера Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** доступна информация о работоспособности:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о работоспособности того сервера Central Node, на котором он сейчас работает.
- Если вы используете режим распределенного решения и multitenancy, и пользователь работает на сервере SCN, пользователю доступна информация о работоспособности этого сервера SCN в рамках тех организаций, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).
- Если вы используете режим распределенного решения и multitenancy, и пользователь работает на сервере PCN, пользователю доступна информация о работоспособности этого сервера PCN и всех серверов SCN, подключенных к этому серверу, в рамках тех организаций, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

► *Чтобы получить более подробную информацию о работоспособности модулей и компонентов программы,*

по ссылке **Просмотреть сведения** откройте окно **Работоспособность системы**.

В окне **Работоспособность системы** отображается следующая информация:

- Если модули и компоненты программы работают нормально, в строке отображается значок OK.

- Если обнаружены проблемы, на которые администратору рекомендуется обратить внимание, в строке отображается значок с количеством таких проблем (например,).

  В этом случае в правой части окна **Работоспособность системы** отображается подробная информация о проблемах.

Окно **Работоспособность системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов программы.

  Содержит информацию о статусе работы модулей и компонентов программы, карантина, а также обновления баз на всех серверах, на которых работает программа.

Пример:

Если базы одного или нескольких компонентов программы не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок  .

Для решения проблемы убедитесь, что серверы обновлений доступны (см. раздел "Выбор источника обновления баз" на стр. 208). Если для соединения с серверами обновлений вы используете прокси-сервер, убедитесь, что на прокси-сервере нет ошибок, связанных с подключением к серверам Kaspersky Endpoint Detection and Response.

- **Обработано** – состояние приема и обработки входящих данных. Статус формируется на основе следующих критериев:
  - Состояние получения данных с серверов с компонентом Sensor, с сервера или виртуальной машины с почтовым сенсором, с компонентов Endpoint Agent.
  - Информация о превышении максимально допустимого времени, которое объекты ожидают в очереди на проверку модулями и компонентами программы.
- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и multitenancy).

В случае обнаружения проблем в работоспособности модулей и компонентов программы, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. 492).

kaspersky

Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса программы

С помощью веб-интерфейса программы вы можете выполнять следующие действия с сервером, на котором установлен компонент Central Node:

- настраивать дату и время сервера;
- выключать и перезагружать сервер;
- генерировать или загружать самостоятельно подготовленный сертификат сервера;
- настраивать сетевые параметры сервера.

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

В этом разделе

Настройка даты и времени сервера

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить дату и время сервера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Дата и время**.
2. В раскрывающемся списке **Страна** выберите страну физического местоположения сервера с

установленным компонентом Central Node.

3. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, в котором находится сервер с установленным компонентом Central Node.

   Вы можете указать страну и часовой пояс, выбрав нужный регион на карте под раскрывающимися списками.

4. Настройте синхронизацию с NTP-серверами:
   - Включите переключатель рядом с названием параметра **Синхронизация с NTP-серверами**, если вы хотите включить синхронизацию.
   - Выключите переключатель рядом с названием параметра **Синхронизация с NTP-серверами**, если вы хотите отключить синхронизацию.
5. В блоке **NTP-серверы** выполните следующие действия:
   - Если вы хотите добавить новый NTP-сервер, выполните следующие действия:
     a. Нажмите на кнопку **Добавить**.
     b. В появившемся поле введите IP-адрес или доменное имя NTP-сервера.
     c. Справа от поля нажмите на кнопку ✓.
   - Если вы хотите изменить IP-адрес или доменное имя NTP-сервера, в строке с этим сервером нажмите на кнопку .
   - Если вы хотите удалить NTP-сервер, в строке с этим сервером нажмите на кнопку .
6. Если синхронизация с NTP-серверами отключена, укажите дату и время сервера вручную:
   - В поле **Дата** укажите текущую дату вручную или выберите ее в календаре по кнопке справа от поля.
   - В поле **Время** укажите текущее время.
7. Нажмите на кнопку **Применить**.

Дата и время сервера будут настроены.

Выключение и перезагрузка сервера

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы выключить или перезагрузить сервер через веб-интерфейс программы, выполните следующие:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Управление сервером** выполните следующие действия:
   - Если вы хотите выключить сервер, на котором установлен компонент Central Node, PCN или SCN, нажмите на кнопку **Выключить**.
   - Если вы хотите перезагрузить сервер, на котором установлен компонент Central Node, PCN или

SCN, нажмите на кнопку **Перезагрузить**.

3. В окне подтверждения нажмите на кнопку **Да**.

Сервер будет выключен или перезагружен.

Генерация или загрузка TLS-сертификата сервера

Если вы уже используете TLS-сертификат сервера и сгенерируете или загрузите новый сертификат, сертификат, который используется в программе, будет удален и заменен на новый сертификат. Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется:

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node (см. раздел "Настройка интеграции с внешними системами" на стр. 207).
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox (см. раздел "Настройка интеграции с компонентом Sandbox" на стр. 204).
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent (см. раздел "Настройка перенаправления трафика от Endpoint Agent на сервер Sensor" на стр. 137).
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory) (см. раздел "Подготовка и загрузка TLS-сертификата сервера Central Node в Active Directory" на стр. 124).

Удалите все правила изоляции хостов Endpoint Agent. Соединение с изолированными хостами будет разорвано, вы не сможете ими управлять.

Вы можете сгенерировать новый сертификат через веб-интерфейс сервера Central Node или загрузить самостоятельно созданный сертификат.

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы сгенерировать TLS-сертификат сервера Central Node, выполните следующие действия:*

1. Войдите в веб-интерфейс Kaspersky Endpoint Detection and Response (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
3. В разделе **TLS-сертификат** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

   Программа сгенерирует новый TLS-сертификат. Страница автоматически обновится.

   Связь с почтовыми сенсорами, компонентом Sandbox, компонентом Endpoint Agent будет прервана до повторной авторизации.

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс программы.

Файл TLS-сертификата, предназначенный для загрузки, должен удовлетворять следующим требованиям:

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

Подробнее о подготовке TLS-сертификатов к импорту см. в документации Open SSL.

Выполняйте действия по загрузке TLS-сертификат в веб-интерфейсе того сервера, на который вы хотите загрузить сертификат.

► *Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Endpoint Detection and Response, выполните следующие действия:*

1. Войдите в веб-интерфейс программы (см. раздел "Начало работы в веб-интерфейсе программы" на стр. 141) под учетной записью администратора (см. раздел "Создание учетной записи администратора веб-интерфейса программы" на стр. 146).
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
3. В разделе **TLS-сертификат** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
4. Выберите файл TLS-сертификата, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Endpoint Detection and Response.

Связь с почтовыми сенсорами, компонентом Sandbox, компонентом Endpoint Agent будет прервана до повторной авторизации.

Скачивание TLS-сертификата сервера на компьютер

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы скачать TLS-сертификат сервера на компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **TLS-сертификат** нажмите на кнопку **Скачать**.

Файл сертификата сервера будет сохранен в папке загрузки браузера.

kaspersky

Назначение DNS-имени сервера

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы назначить имя сервера для использования DNS-серверами, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В поле **Имя сервера (FQDN)** введите полное доменное имя сервера.

   Указывайте имя сервера в формате FQDN (например, `host.domain.com` или `host.domain.subdomain.com`).
3. Нажмите на кнопку **Применить**.

Имя хоста будет назначено.

Настройка параметров DNS

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить параметры DNS, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Если вы хотите настроить назначение DNS-адресов с помощью DHCP-сервера, выполните следующие действия:
   a. В блоке параметров **Параметры DNS** в строке **Режим** выберите **DHCP**.
   b. В раскрывающемся списке **Сетевой интерфейс** выберите имя сетевого интерфейса для соединения с DNS-сервером.
3. Если вы хотите настроить назначение статических DNS-адресов, выполните следующие действия:
   a. В блоке параметров **Параметры DNS** в строке **Режим** выберите **Статический**.
   b. В поле **Домены** укажите имя домена.
   c. В поле **Главный и дополнительный DNS-серверы** введите IP-адреса DNS-серверов.
4. Нажмите на кнопку **Применить**.

Параметры DNS будут настроены.

kaspersky

Настройка параметров сетевого интерфейса

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить параметры сетевого интерфейса, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Выберите сетевой интерфейс, параметры которого вы хотите настроить.

   Откроется окно **Изменить сетевой интерфейс**.
3. В строке **Режим** выберите один из следующих вариантов:
   - Если вы хотите, чтобы IP-адрес сетевого интерфейса был назначен с помощью DHCP-сервера, выберите **DHCP**.
   - Если вы хотите назначить сетевому интерфейсу статический IP-адрес, выберите **Статический**.
4. Если вы выбрали **Статический**, выполните следующие действия:
   a. В поле **IP** укажите IP-адрес сетевого интерфейса.
   b. В поле **Маска подсети** укажите маску подсети сетевого интерфейса.
5. Если вы хотите включить сетевой интерфейс, в строке **Состояние** переведите переключатель в положение **Включено**.
6. Нажмите на кнопку **Инициализировать**.

Параметры сетевого интерфейса будут настроены.

Настройка сетевого маршрута для использования по умолчанию

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить сетевой маршрут для использования по умолчанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В блоке параметров **Сетевой маршрут** в раскрывающемся списке **Сетевой интерфейс** выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
3. В строке **Режим** выберите один из следующих вариантов:
   - Если вы хотите настроить сетевой маршрут с помощью DHCP-сервера, выберите **DHCP**.
   - Если вы хотите настроить статический сетевой маршрут, выберите **Статический**.
4. Если вы выбрали **Статический**, в поле **Шлюз** введите IP-адрес шлюза.
5. Нажмите на кнопку **Применить**.

Сетевой маршрут для использования по умолчанию будет настроен.

Настройка параметров соединения с прокси-сервером

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Прокси-сервер** переведите переключатель в положение **Включено**.
3. В поле **Хост** укажите URL-адрес прокси-сервера.
4. В поле **Порт** укажите порт подключения к прокси-серверу.
5. В поле **Имя пользователя** укажите имя пользователя для аутентификации на прокси-сервере.
6. В поле **Пароль** укажите пароль для аутентификации на прокси-сервере.
7. Если вы не хотите использовать прокси-сервер при подключении к локальным адресам, установите флажок **Не использовать прокси-сервер для локальных адресов**.
8. Нажмите на кнопку **Применить**.

Параметры соединения с прокси-сервером будут настроены.

kaspersky

Управление компонентом Sensor

В Kaspersky Endpoint Detection and Response компонент Sensor может использоваться в качестве прокси-сервера при обмене данными между компонентами Endpoint Agent и компонентом Central Node, чтобы снизить нагрузку на компонент Central Node.

Вы можете установить компоненты Sensor и Central Node на одном сервере или на отдельных серверах. Если компонент Sensor установлен на отдельном сервере, необходимо подключить его к серверу с компонентом Central Node.

Если вы используете режим распределенного решения и multitenancy, выполняйте действия по подключения к серверам PCN или SCN.

В этом разделе

Обработка запроса на подключение от компонента Sensor

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Вы можете принять, отклонить или отозвать ранее принятый запрос на подключение от компонента Sensor.

► *Чтобы обработать запрос на подключение от компонента Sensor, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   В таблице **Список серверов** отобразятся уже подключенные компоненты Sensor, а также запросы на подключение.

2. В строке с запросом на подключение компонента Sensor выполните одно из следующих действий:

   - Если вы хотите подключить компонент Sensor, нажмите на кнопу **Принять**.
   - Если вы не хотите подключать компонент Sensor, нажмите на кнопку **Отклонить**.

3. В окне подтверждения нажмите на кнопку **Да**.

Запрос на подключение от компонента Sensor будет обработан.

kaspersky

Просмотр таблицы серверов с компонентом Sensor

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Таблица серверов с компонентом Sensor находится в разделе **Серверы Sensor** окна веб-интерфейса программы. В таблице содержится следующая информация:

- **IP/имя** – IP-адрес или доменное имя сервера с компонентом Sensor.
- **Тип** – тип компонента Sensor. Может принимать следующие значения:
  - **Central Node** – компонент Sensor установлен на том же сервере, что и компонент Central Node.
  - **Удаленный** – компонент Sensor установлен на другом сервере или в качестве компонента Sensor используется почтовый сенсор.
- **Отпечаток сертификата** – отпечаток TLS-сертификата, с помощью которого устанавливается шифрованное соединение между серверами с компонентами Sensor и Central Node.
- **KSN/KPSN** – состояние подключения к репутационным базам KSN/KPSN.
- **SPAN** – состояние обработки SPAN-трафика.
- **SMTP** – состояние интеграции с почтовым сервером по протоколу SMTP.
- **ICAP** – состояние интеграции с прокси-сервером по протоколу ICAP.
- **POP3** – состояние интеграции с почтовым сервером по протоколу POP3.
- **Состояние** – состояние запроса на подключение.

Включение интеграции с прокси-сервером по протоколу ICAP

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Если вы используете отдельный прокси-сервер, по умолчаниюKaspersky Endpoint Detection and Response не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов. Администратору программы необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером иKaspersky Endpoint Detection and Response с помощью туннелирования трафика или средствами iptables.

► *Чтобы включить интеграцию с прокси-сервером по протоколу ICAP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, для которого вы хотите настроить интеграцию с прокси-сервером по

протоколу ICAP.

Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **ICAP-интеграция с прокси-сервером**.
4. В поле **Состояние** переведите переключатель в положение **Включено**.

   В поле **Хост** отобразится URL-адрес службы Response Modification (RESPMOD), которая обрабатывает входящий трафик.

   Используйте этот URL-адрес для настройки интеграции cKaspersky Endpoint Detection and Response по протоколу ICAP на прокси-сервере, который используется в вашей организации.
5. Нажмите на кнопку **Применить**.

Интеграция с прокси-сервером по протоколу ICAP будет включена.

kaspersky

Работа с информацией о хостах с компонентом Endpoint Agent

Компонент Endpoint Agent устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**, **Локальный администратор** и **Администратор** могут оценить регулярность получения данных с хостов, на которых установлен компонент Endpoint Agent, на закладке **Endpoint Agents** окна веб-интерфейса программы в рамках тех организаций, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148). Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, то в веб-интерфейсе сервера PCN отображается список компонентов Endpoint Agent для PCN и всех подключенных SCN.

Пользователи с ролью **Локальный администратор** и **Администратор** могут настроить отображение регулярности получения данных с хостов, на которых установлен компонент Endpoint Agent, в рамках тех организаций, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети любой из хостов с компонентом Endpoint Agent в рамках тех организаций, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148). При этом соединение между сервером с компонентом Central Node и хостом с компонентом Endpoint Agent не будет прервано.

Для оказания поддержки при неполадках в работе компонента Endpoint Agent специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode (см. стр. 142)):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов программы.
- Изменить параметры хранения и отправки получаемой 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 т.д.), а также состав собираемых в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Собранная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка собранных данных в "Лабораторию Касперского" не выполняется.

kaspersky

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

kaspersky

Выбор организации для работы в разделе Endpoint Agent

Если вы используете режим multitenancy, перед началом работы в разделе **Endpoint Agents** вам нужно выбрать организацию, данные по которой вас интересуют.

► *Чтобы выбрать организацию для работы в разделе **Endpoint Agents**, выполните следующие действия:*

1. В верхней части меню веб-интерфейса программы нажмите на стрелку рядом с названием организации.
2. В раскрывшемся списке выберите организацию.

Отобразятся данные по выбранной вами организации. Если вы хотите изменить организацию, вам нужно повторить действия по выбору организации.

Просмотр таблицы хостов Endpoint Agent на отдельном сервере Central Node

Таблица хостов с компонентом Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса программы.

Если вы используете отдельный сервер Central Node, не используете режим распределенного решения (см. раздел «Распределенное решение и режим multitenancy» на стр. 76) и multitenancy, в таблице хостов с компонентом Endpoint Agent могут отображаться следующие данные:

- **Хост** – имя хоста с компонентом Endpoint Agent.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Agent.
- **Версия** – версия установленного компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Просмотр таблицы хостов Endpoint Agent в режиме распределенного решения и multitenancy

Таблица хостов с компонентом Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса

программы.

Если вы используете режим распределенного решения (см. раздел «Распределенное решение и режим multitenancy» на стр. 76) и multitenancy, в таблице содержится информация о компонентах Endpoint Agent, подключенных к PCN и всем серверам SCN. В таблице могут отображаться следующие данные:

- **Хост** – имя хоста с компонентом Endpoint Agent.

  По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Новое правило запрета**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Серверы** – имена серверов, к которым подключен хост с компонентом Endpoint Agent.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Agent.
- **Версия** – версия установленного компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

По ссылке с IP-адресом компьютера, на который установлен компонент Endpoint Agent, вы также можете выбрать действие **Найти обнаружения**.

Просмотр информации о хосте

► *Чтобы просмотреть информацию о хосте с компонентом Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.
2. Выберите хост, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- **Состояние** – состояние хоста с компонентом Endpoint Agent.

  Хост может находиться в одном из следующих состояний:

  - **Онлайн**.
  - **Отключено**.
- **Хост** – имя хоста компьютера с компонентом Endpoint Agent.

  По ссылке с именем хоста вы можете выполнить действие **Скопировать значение в буфер**.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, на компьютере, на который установлен компонент Endpoint Agent.
- **Защита** – состояние защиты хоста с компонентом Endpoint Agent.
- **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и multitenancy.
- **Имя сервера** – имя сервера Central Node.
- **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
- **Версия** – тип и версия установленного компонента Endpoint Agent.
- **Состояние** – состояние компонента Endpoint Agent.

Фильтрация и поиск хостов Endpoint Agent по имени хоста

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по имени хоста, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Agents**.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов имени хоста.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent, изолированных от сети

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent, изолированные от сети, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Установите флажок **Показывать только изолированные Endpoint Agents**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent по именам серверов PCN и SCN

Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, вы можете отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN, к которым подключены эти хосты.

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Серверы** откройте окно настройки фильтрации.
3. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с компонентом Endpoint Agent.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent по IP-адресу компьютера

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по IP-адресу компьютера, на котором установлен компонент Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **IP** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

kaspersky

Фильтрация и поиск хостов Endpoint Agent по версии операционной системы на компьютере

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии операционной системы, установленной на компьютере с компонентом Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **ОС** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов версии операционной системы.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent по версии Endpoint Agent

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии компонента Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Версия** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов версии компонента Endpoint Agent.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent по их активности

► *Чтобы отфильтровать или найти компоненты Endpoint Agent по их активности, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Активность** откройте окно настройки фильтрации.
3. Установите флажки рядом с одним или несколькими показателями активности компонента Endpoint Agent:
   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

kaspersky

Быстрое создание фильтра хостов Endpoint Agent

► *Чтобы быстро создать фильтр хостов с компонентом Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением графы таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра хостов Endpoint Agent

► *Чтобы сбросить фильтр хостов с компонентом Endpoint Agent по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.
2. Нажмите на кнопку справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Настройка показателей активности компонента Endpoint Agent

Пользователи с ролью **Локальный администратор** и **Администратор** могут определить, какой период бездействия компонентов Endpoint Agent считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности компонентов Endpoint Agent. Просматривать показатели активности Endpoint Agent могут все пользователи.

► *Чтобы настроить показатели активности компонентов Endpoint Agent, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью **Локальный администратор** или **Администратор**.
2. В окне веб интерфейса программы выберите раздел **Параметры**, подраздел **Endpoint Agents**.
3. В полях под названием раздела введите количество дней бездействия компьютеров с компонентом Endpoint Agent, которое вы хотите отображать как **Предупреждение** и **Критическое бездействие**.
4. Нажмите на кнопку **Применить**.

Пользователи с правами **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** смогут увидеть настроенные вами показатели активности компонентов Endpoint Agent в графе **Активность** таблицы хостов с компонентом Endpoint Agent в разделе **Endpoint Agents** окна веб-интерфейса программы.

Поддерживаемые интерпретаторы и процессы

Компонент Endpoint Sensors контролирует запуск скриптов следующими интерпретаторами:

- cmd.exe;
- reg.exe;
- regedit.exe;
- regedt32.exe;
- cscript.exe;
- wscript.exe;
- mmc.exe;
- msiexec.exe;
- mshta.exe;
- rundll32.exe;
- runlegacycplelevated.exe;
- control.exe;
- explorer.exe;
- regsvr32.exe;
- wwahost.exe;
- powershell.exe;
- java.exe и javaw.exe (только при запуске с опцией –jar);
- InstallUtil.exe;
- msdt.exe;
- python.exe;
- ruby.exe;

- rubyw.exe.

Информация о процессах, контролируемых компонентом Endpoint Sensor, представлена в таблице ниже.

Таблица 12. Процессы и расширения файлов, которые они открывают

Процесс	Расширения файлов
winword.exe	rtf doc dot docm docx dotx dotm docb
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf

Процесс	Расширения файлов
MicrosoftEdge.exe	pdf

Создание задачи для перезапуска компонентов Endpoint Agent в KSC

Вы можете создать групповую задачу для перезапуска компонентов Endpoint Agent на всех компьютерах в Консоли администрирования Kaspersky Security Center. Если интеграция программы с Kaspersky Security Center не настроена, вы можете использовать для перезапуска компонентов групповую политику Windows. Подробнее о групповых политиках см. в документации к операционной системе.

► *Чтобы создать групповую задачу для перезапуска компонентов Endpoint Agent, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке с управляемыми устройствами дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку со списком задач.
4. Нажмите на кнопку создания задачи.

   Запустится мастер создания задачи.
5. В окне выбора типа задачи выберите запуск или остановку программы.
6. Следуйте указаниям мастера создания задачи.

Задача для перезапуска службы компонентов Endpoint Agent будет создана. Подробнее о групповых задачах и запуске задач см. Справку Kaspersky Security Center https://help.kaspersky.com/KSC/SP3/ru-RU/5022.htm.

kaspersky

Настройка интеграции с компонентом Sandbox

Вы можете подключить один компонент Sandbox к нескольким компонентам Central Node.

Предусмотрен следующий порядок настройки соединения компонента Sandbox с компонентом Central Node:

a. **Создание запроса на подключение к компоненту Sandbox**

   Вы можете создать запрос в меню администратора или в веб-интерфейсе программы (см. раздел "Создание запроса на подключение к серверу с компонентом Sandbox" на стр. 204) под учетной записью администратора. Необходимо создавать запрос для каждого сервера с компонентом Central Node, который вы хотите подключить к компоненту Sandbox.

b. **Обработка запроса на подключение (см. раздел "Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox" на стр. 161) в веб-интерфейсе Sandbox**

   Вы можете принять или отклонить каждый запрос.

В этом разделе

Просмотр таблицы серверов с компонентом Sandbox

Таблица серверов с компонентом Sandbox находится на закладке **Серверы Sandbox** окна веб-интерфейса программы.

Таблица содержит следующую информацию:

- **IP и имя** – IP-адрес или полное доменное имя сервера с компонентом Sandbox.
- **Отпечаток сертификата** – отпечаток сертификата сервера с компонентом Sandbox.
- **Авторизация** – статус запроса на подключение к компоненту Sandbox.
- **Состояние** – состояние подключения к компоненту Sandbox.

Создание запроса на подключение к серверу с компонентом Sandbox

► *Чтобы создать запрос на подключение к серверу с компонентом Sandbox через веб-интерфейс программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sandbox**.

2. В правом верхнем углу окна нажмите на кнопку **Добавить**.

   Откроется окно **Подключение сервера Sandbox**.

3. В поле **IP** укажите IP-адрес сервера с компонентом Sandbox, к которому вы хотите подключиться.
4. Нажмите на кнопку **Получить отпечаток сертификата**.

   В рабочей области отобразится отпечаток сертификата сервера с компонентом Sandbox.

5. Сравните полученный отпечаток сертификата с отпечатком, указанным в веб-интерфейсе Sandbox в разделе **Авторизация KATA** в поле **Отпечаток сертификата**.

   Если отпечатки сертификата совпадают, выполните дальнейшие шаги инструкции.

   > Не рекомендуется подтверждать подключение при несовпадении отпечатков сертификата. Убедитесь в правильности введенных данных.

6. В поле **Имя** укажите имя компонента Sandbox, которое будет отображаться в веб-интерфейсе компонента Central Node.

   Это имя не связано с именем хоста, на котором установлен Sandbox.

7. Если вы хотите сделать соединение с Sandbox активным сразу после подключения, установите флажок **Включить**.
8. Нажмите на кнопку **Добавить**.

Запрос на подключение отобразится в веб-интерфейсе компонента Sandbox.

Включение и отключение соединения с компонентом Sandbox

► *Чтобы сделать соединение с компонентом Sandbox активным или отключить его, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sandbox**.

   Отобразится таблица серверов с компонентами Sandbox.

2. В строке с нужным сервером в графе **Состояние** выполните одно из следующих действий:
   - Если вы хотите сделать соединение с компонентом Sandbox активным, переведите переключатель в положение **Включено**.
   - Если вы хотите отключить соединение с компонентом Sandbox, переведите переключатель в положение **Отключено**.
3. Нажмите на кнопку **Применить**.

Соединение с компонентом Sandbox станет активным или будет отключено.

Удаление соединения с компонентом Sandbox

► *Чтобы удалить соединение с компонентом Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sandbox**.

   Отобразится таблица компьютеров, на которых установлен компонент Sandbox.

2. Установите флажок в строке с компонентом Sandbox, соединение с которым вы хотите удалить.
3. В правом верхнем углу окна нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**.

Соединение с компонентом Sandbox будет удалено.

kaspersky

Настройка параметров сервера для отправки уведомлений

Программа может отправлять уведомления об обнаружениях. Для этого необходимо настроить параметры сервера для отправки уведомлений.

► *Чтобы настроить параметры сервера для отправки уведомлений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сервер для отправки уведомлений**.
2. В поле **Хост** укажите IP-адрес почтового сервера.
3. В поле **Порт** укажите порт подключения к почтовому серверу.
4. В поле **Отправлять с адреса** укажите адрес электронной почты, с которого будут отправляться уведомления.
5. Если вы хотите включить проверку подлинности на почтовом сервере, установите флажок **Использовать SMTP-проверку подлинности получателей сообщений**.
6. В поле **Имя пользователя** укажите имя пользователя для аутентификации на сервере для отправки уведомлений.
7. В поле **Пароль** укажите пароль для аутентификации на сервере для отправки уведомлений.
8. Если вы хотите использовать TLS-шифрование при отправке уведомлений, установите флажок **Использовать TLS-шифрование**.
9. Если вы хотите проверить сертификат почтового сервера, установите флажок **Подтверждать TLS-шифрование**.

   В поле **Отпечаток сертификата** отобразится отпечаток сертификата почтового сервера.

   > Если флажок **Подтверждать TLS-шифрование** не установлен, программа будет считать любой сертификат почтового сервера доверенным.

10. Нажмите на кнопку **Применить**.

Параметры сервера для отправки уведомлений будут настроены.

Обновление баз программы

Базы программы (далее также "базы") представляют собой файлы с записями, на основании которых компоненты и модули программы обнаруживают события, происходящие в IT-инфраструктуре вашей организации.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, в том числе угроз "нулевого дня", создают для них идентифицирующие записи и включают их в пакеты обновлений баз (далее также "пакеты обновлений"). *Пакет обновлений* представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений.

При установке программы дата выпуска баз соответствует дате выпуска программы, поэтому базы нужно обновить сразу после установки программы.

Программа периодически автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского" (с периодичностью один раз в 30 минут). По умолчанию, если базы компонентов программы по каким-либо причинам не обновляются в течение 24 часов, Kaspersky Endpoint Detection and Response отображает эту информацию в разделе **Мониторинг** окна веб-интерфейса программы.

Выбор источника обновления баз

Вы можете выбрать источник, из которого программа будет загружать обновления баз. Источником обновлений может быть сервер "Лаборатории Касперского", а также сетевая или локальная папка одного из компьютеров вашей организации.

► *Чтобы выбрать источник обновления баз программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Обновление баз** в раскрывающемся списке **Источник обновлений** выберите одно из следующих значений:
   - **Сервер обновлений "Лаборатории Касперского"**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.
   - **Сервер обновлений "Лаборатории Касперского" (безопасное подключение)**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется выполнять обновления баз по протоколу HTTPS.
   - **Другой сервер**.

     Программа будет подключаться к папке с базами программы по протоколу HTTP и загружать актуальные базы.
3. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите URL-адрес пакета обновлений на вашем FTP- или HTTP-сервере или укажите полный путь к директории с пакетом обновлений.
4. Нажмите на кнопку **Применить**.

Источник обновления баз программы будет выбран.

Запуск обновления баз вручную

► *Чтобы запустить обновление баз программы вручную, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Обновление баз** нажмите на кнопку **Запустить**.

Обновление баз программы будет запущено. Справа от кнопки отобразится сообщение о результате выполнения обновления.

kaspersky

Создание списка паролей для архивов

Программа не проверяет архивы, защищенные паролем. Вы можете создать список наиболее часто встречающихся паролей для архивов, которые используются при обмене файлами в вашей организации. В этом случае при проверке архива программа будет проверять пароли из списка. Если какой-либо из паролей подойдет, архив будет разблокирован и проверен.

Список паролей, заданный в параметрах программы, также передается на сервер с компонентом Sandbox.

► *Чтобы создать список паролей для архивов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пароли к архивам**.
2. В поле **Пароли к архивам** введите пароли, которые программа будет использовать для архивов, защищенных паролем.

   Вводите каждый пароль с новой строки. Вы можете ввести до 50 паролей.
3. Нажмите на кнопку **Применить**.

Список паролей для архивов будет создан. При проверке файлов формата PDF, а также файлов программ Microsoft Word, Excel, PowerPoint, защищенных паролем, программа будет подбирать пароли из заданного списка.

kaspersky

Сотруднику службы безопасности: работа в веб-интерфейсе программы

Этот раздел адресован специалистам, в обязанности которых входит обеспечение безопасности данных организации. Он содержит информацию и инструкции по настройке средств для защиты IT-инфраструктуры организации и своевременного обнаружения угроз.

Программа допускает совместную работу нескольких специалистов по информационной безопасности.

В этом разделе

kaspersky

Интерфейс программы

Работа с программой осуществляется через веб-интерфейс. Разделы веб-интерфейса программы различаются в зависимости от роли пользователя – **Администратор** или **Старший сотрудник службы безопасности** / **Сотрудник службы безопасности** (см. раздел "**Сотруднику службы безопасности: работа в веб-интерфейсе программы**" на стр. 210).

Окно веб-интерфейса программы содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса программы;
- закладки в верхней части окна веб-интерфейса программы для некоторых разделов программы;
- рабочую область в нижней части окна веб-интерфейса программы.

Разделы окна веб-интерфейса программы

Веб-интерфейс программы для пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** разделен на следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Endpoint Detection and Response.
- **Обнаружения**. Содержит информацию об обнаружениях в сети вашей организации.
- **Поиск угроз**. Содержит информацию о событиях, найденных на хостах вашей организации.
- **Задачи**. Содержит информацию о задачах, с помощью которых вы можете работать с файлами и программами на хостах.
- **Политики**. Содержит информацию о политиках, с помощью которых вы можете управлять запретами запуска файлов на выбранных хостах.
- **Правила пользователей**: **TAA**, **IOC** и **YARA**. Содержит информацию для работы с пользовательскими правилами.
- **Хранилище**: **Файлы** и **Карантин** Содержит информацию для работы с объектами на карантине и в Хранилище.
- **Endpoint Agents**. Содержит информацию об управлении компонентом Endpoint Agent и просмотре данных.
- **Отчеты**: **Созданные отчеты** и **Шаблоны**. Содержит конструктор отчетов и список созданных отчетов об обнаружениях.
- **Параметры**: **Расписание IOC-проверки**, **Endpoint Agents**, **Репутационная база KPSN**, **Отправка уведомлений**, **Статус VIP**, **Белые списки**, **Пароли к архивам** и **Лицензия**. Содержит информацию о расписании IOC-проверки, параметрах публикации объектов в KPSN, присвоении обнаружениям статуса VIP на основе информации, содержащейся в обнаружениях, белом списке и исключениях TAA (IOA)-правил из проверки, паролях к архивам и добавленных ключах.

Рабочая область окна веб-интерфейса программы

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса программы, а также элементы управления, с помощью которых вы можете настроить отображение информации.

kaspersky

Включение и отключение сетевого интерфейса

Если вы используете режим распределенного решения и multitenancy, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы включить сетевой интерфейс, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Выберите сетевой интерфейс, который вы хотите включить.

   Откроется окно **Изменить сетевой интерфейс**.
3. В строке **Состояние** переведите переключатель в положение **Включено**.
4. Нажмите на кнопку **Сохранить**.

Сетевой интерфейс будет включен.

► *Чтобы отключить сетевой интерфейс, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Выберите сетевой интерфейс, который вы хотите отключить.

   Откроется окно **Изменить сетевой интерфейс**.
3. В строке **Состояние** переведите переключатель в положение **Отключено**.
4. Нажмите на кнопку **Сохранить**.

Сетевой интерфейс будет отключен.

Выбор организации для работы в веб-интерфейсе программы

Если вы используете режим multitenancy, перед началом работы с веб-интерфейсом вам нужно выбрать организацию, в рамках которой вы хотите работать с веб-интерфейсом программы.

► *Чтобы выбрать организацию для работы в веб-интерфейсе программы, выполните следующие действия:*

1. В верхней части меню веб-интерфейса программы нажмите на стрелку рядом с названием организации.
2. В раскрывшемся меню **Выберите организацию** выберите организацию из списка.

   Вы также можете ввести несколько символов названия организации в строку поиска и выбрать организацию из списка результатов поиска.

Все действия в веб-интерфейсе программы будут связаны с выбранной организацией. Если вы хотите изменить организацию, вам нужно повторить действия по выбору организации.

kaspersky

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью графиков в разделе **Мониторинг** окна веб-интерфейса программы. Вы можете добавлять, удалять, перемещать графики, настраивать масштаб отображения графиков и выбирать период отображения данных.

В этом разделе

О графиках и схемах расположения графиков

С помощью графиков вы можете осуществлять мониторинг работы программы.

Схема расположения графиков – вид рабочей области окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать графики на схеме расположения графиков, а также настраивать масштаб графиков.

Если вы используете режим распределенного решения и multitenancy, в разделе отображаются данные по выбранной вами организации (см. раздел «Выбор организации для работы в веб-интерфейсе программы» на стр. 213).

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

В разделе **Мониторинг** отображаются следующие графики:

- Обнаружения:
  - **Обнаружения по состоянию**. Отображение состояния обнаружения в зависимости от того, какой пользователь Kaspersky Endpoint Detection and Response его обрабатывает и от того, обработано это обнаружение или нет.
  - **Обнаружения по технологии**. Отображение названий модулей или компонентов программы, сделавших обнаружение.
  - **Обнаружения по вектору атаки**. Отображение обнаруженных объектов по направлению атаки.
  - **VIP-обнаружения по степени важности**. Отображение важности обнаружений со статусом VIP

в соответствии с тем, какое влияние они могут оказать на безопасность компьютера или локальной сети организации, по опыту "Лаборатории Касперского".

- **Обнаружения по степени важности**. Отображение важности обнаружений для пользователя Kaspersky Endpoint Detection and Response в соответствии с тем, какое влияние они могут оказать на безопасность компьютеров или локальной сети организации, по опыту "Лаборатории Касперского".

В левой части каждого графика перечислены векторы атаки, степени важности обнаружений, состояния обнаружений и технологии, выполнившие обнаружения. В правой части каждого графика отображается количество раз, которое программа обнаружила их за выбранный период отображения данных на графиках (см. раздел "Настройка периода отображения данных на графиках" на стр. 177).

По ссылке с названием вектора атаки, степенью важности обнаружений, состоянием обнаружений и технологией, выполнившей обнаружения, можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть связанные обнаружения. При этом обнаружения будут отфильтрованы по выбранному элементу.

- Топ 10:
  - **Домены**. 10 доменов, наиболее часто встречающихся в обнаружениях.
  - **IP-адреса**. 10 IP-адресов, наиболее часто встречающихся в обнаружениях.
  - **Хосты TAA**. 10 хостов, наиболее часто встречающихся в событиях и обнаружениях, выполненных технологией Targeted Attack Analyzer (TAA).
  - **Правила TAA**. 10 правил TAA (IOA), наиболее часто встречающихся в событиях и обнаружениях, выполненных технологией Targeted Attack Analyzer (TAA).

  В левой части каждого графика перечислены домены, адреса получателей, IP-адреса и адреса отправителей сообщений, имена хостов и названия правил TAA (IOA). В правой части каждого графика отображается количество раз, которое программа обнаружила их за выбранный период отображения данных на графиках (см. раздел "Настройка периода отображения данных на графиках" на стр. 177).

  По ссылке с именем каждого домена, адреса получателя, IP-адреса и адреса отправителя сообщений , именем хоста и названию правила TAA (IOA) можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть связанные обнаружения. При этом обнаружения будут отфильтрованы по выбранному элементу.

Добавление графика на текущую схему расположения графиков

► *Чтобы добавить график на текущую схему расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на кнопку **Графики**.
5. В появившемся окне **Настроить графики** включите переключатель рядом с графиком, который вы хотите добавить.

График будет добавлен на текущую схему расположения графиков.

Перемещение графика на текущей схеме расположения графиков

► *Чтобы переместить график на текущей схеме расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Выберите график, который вы хотите переместить на схеме расположения графиков.
5. Нажав и удерживая левую клавишу мыши на верхней части графика, перетащите график на другое место схемы расположения графиков.
6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения графиков будет сохранена.

Удаление графика с текущей схемы расположения графиков

► *Чтобы удалить график с текущей схемы расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок × в правом верхнем углу графика, который вы хотите удалить со схемы расположения графиков.

   График будет удален из рабочей области окна веб-интерфейса программы.
5. Нажмите на кнопку **Сохранить**.

График будет удален с текущей схемы расположения графиков.

Сохранение схемы расположения графиков в PDF

► *Чтобы сохранить схему расположения графиков в PDF, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Сохранить как PDF**.

Откроется окно **Сохранение в PDF**.

4. В нижней части окна в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.

   Схема расположения графиков в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.
6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на графиках

Вы можете настроить отображение данных на графиках за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

► *Чтобы настроить отображение данных на графиках за сутки (с 00:00 до 23:59), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за неделю (с понедельника по воскресенье), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за месяц (календарный месяц), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

kaspersky

Настройка масштаба отображения графиков

Вы можете настроить масштаб отображения графиков типа "Обнаружения". В правом верхнем углу графиков, масштаб отображения которых можно настроить, есть значок .

► *Чтобы настроить масштаб отображения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок в правом верхнем углу графика.
5. В раскрывшемся списке выберите один из следующих размеров отображения графика:
   - **1x1 размер**.
   - **2x1 размер**.
   - **3x1 размер**.

   Масштаб отображения выбранного графика изменится.
6. Повторите действия для всех графиков, масштаб отображения которых вы хотите изменить.
7. Нажмите на кнопку **Сохранить**.

Масштаб отображения графиков будет настроен.

Основные принципы работы с графиками типа "Обнаружения"

Для всех графиков типа "Обнаружения" можно настроить масштаб отображения (см. раздел "Настройка масштаба отображения графиков" на стр. 218).

В левой части каждого графика отображается легенда графика по цветам, которые используются на графиках.

Пример:

На графике **Обнаружения по степени важности** отображается количество обнаружений различной степени важности.

Важность – важность обнаружения для пользователя программы в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

На графике **Обнаружения по степени важности** важность обнаружений отмечена следующими цветами:

- красным – обнаружения высокой степени важности;
- оранжевым – обнаружения средней степени важности;
- зеленым – обнаружения низкой степени важности.

Справа от легенды отображается количество обнаружений каждого типа за выбранный период

отображения данных на графиках (см. раздел "Настройка периода отображения данных на графиках" на стр. 177).

По ссылке с типом каждого обнаружения можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть все обнаружения этого типа. При этом обнаружения будут отфильтрованы по данному типу.

В правой части каждого графика отображаются столбцы данных. На вертикальной оси отображается количество событий, на горизонтальной оси отображаются дата и время обнаружения. Вы можете изменить период отображения данных на графиках (см. раздел "Настройка периода отображения данных на графиках" на стр. 177) и выбрать организацию (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213), информация о которых должна быть представлена на графике.

При наведении курсора мыши на каждый столбец данных отображается количество обнаружений, подсчитанных за период, представленный этим столбцом. По умолчанию отображается количество необработанных обнаружений. Вы можете включить отображение обработанных обнаружений, установив флажок **Обработано** в правом верхнем углу окна. В этом случае будет отображаться количество всех обнаружений.

Просмотр состояния работоспособности модулей и компонентов программы

Если в работе модулей и компонентов программы возникли проблемы, на которые администратору рекомендуется обратить внимание, в верхней части окна раздела **Мониторинг** веб-интерфейса программы отображается рамка желтого цвета с предупреждениями.

Пользователю с ролью **Локальный администратор** или **Администратор** доступна информация о работоспособности того сервера Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** доступна информация о работоспособности:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о работоспособности того сервера Central Node, на котором он сейчас работает.
- Если вы используете режим распределенного решения и multitenancy, и пользователь работает на сервере SCN, пользователю доступна информация о работоспособности этого сервера SCN в рамках тех организаций, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).
- Если вы используете режим распределенного решения и multitenancy, и пользователь работает на сервере PCN, пользователю доступна информация о работоспособности этого сервера PCN и всех серверов SCN, подключенных к этому серверу, в рамках тех организаций, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

► *Чтобы получить более подробную информацию о работоспособности модулей и компонентов программы,*

по ссылке **Просмотреть сведения** откройте окно **Работоспособность системы**.

В окне **Работоспособность системы** отображается следующая информация:

- Если модули и компоненты программы работают нормально, в строке отображается значок OK.

- Если обнаружены проблемы, на которые администратору рекомендуется обратить внимание, в строке отображается значок с количеством таких проблем (например, 1).

  В этом случае в правой части окна **Работоспособность системы** отображается подробная информация о проблемах.

Окно **Работоспособность системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов программы.

  Содержит информацию о статусе работы модулей и компонентов программы, карантина, а также обновления баз на всех серверах, на которых работает программа.

Пример:

Если базы одного или нескольких компонентов программы не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок .

Для решения проблемы убедитесь, что серверы обновлений доступны (см. раздел "Выбор источника обновления баз" на стр. 208). Если для соединения с серверами обновлений вы используете прокси-сервер, убедитесь, что на прокси-сервере нет ошибок, связанных с подключением к серверам Kaspersky Endpoint Detection and Response.

- **Обработано** – состояние приема и обработки входящих данных. Статус формируется на основе следующих критериев:
  - Состояние получения данных с серверов с компонентом Sensor, с сервера или виртуальной машины с почтовым сенсором, с компонентов Endpoint Agent.
  - Информация о превышении максимально допустимого времени, которое объекты ожидают в очереди на проверку модулями и компонентами программы.
- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и multitenancy).

В случае обнаружения проблем в работоспособности модулей и компонентов программы, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. 492).

kaspersky

Таблица обнаружений

Kaspersky Endpoint Detection and Response обрабатывает данные из следующих источников:

- Данных о запущенных процессах, открытых сетевых соединениях и изменяемых файлах, полученных от отдельных компьютеров, которые входят в IT-инфраструктуру организации и работают под управлением операционной системы Microsoft Windows.

Kaspersky Endpoint Detection and Response отображает обнаруженные признаки целевых атак и вторжений в IT-инфраструктуру организации в виде таблицы обнаружений.

В таблице обнаружений не отображается информация об объектах, для которых выполняется хотя бы одно из следующих условий:

- Объект имеет репутацию *Доверенный* в базе KSN.
- Объект имеет цифровую подпись одного из доверенных производителей:
  - "Лаборатория Касперского".
  - Apple.
  - Google.

Информация об этих обнаружениях сохраняется в базе данных программы (на Central Node или SCN).

Информация об обнаружениях в базе данных ротируется ежедневно в ночное время при достижении максимально разрешенного количества обнаружений:

- Обнаружения, выполненные компонентами **(URL) URL Reputation** – 100000 обнаружений для каждого из компонентов.
- Все остальные обнаружения – 20000 обнаружений для каждого из модулей или компонентов.

Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, то ротация производится на всех SCN, а затем происходит синхронизация с PCN. После синхронизации все удаленные обнаружения автоматически удаляются также на PCN.

Таблица обнаружений находится в разделе **Обнаружения**.

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

Вы можете сортировать обнаружения в таблице (см. раздел "Сортировка обнаружений в таблице" на стр. 231) по графам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

В таблице обнаружений содержится следующая информация:

1. **VIP** – наличие у обнаружения статуса с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.
2. **Создано** – время, в которое программа выполнила обнаружение и **Обновлено** – время, в которое обнаружение было обновлено.

3. – важность обнаружения для пользователя программы в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

   Обнаружения могут принимать одну из следующих степеней важности:

   - **Высокая**, отмеченную знаком , – обнаружение высокой степени важности.
   - **Средняя**, отмеченную знаком , – обнаружение средней степени важности.
   - **Низкая**, отмеченную знаком , – обнаружение низкой степени важности.

4. **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если программа обнаружила файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
5. **Сведения** – краткая информация об обнаружении. Например, имя обнаруженного файла или URL-адрес вредоносной ссылки.
6. **Серверы** – имена серверов, на которых выполнено обнаружение. Серверы относятся к той организации, с которой вы работаете в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213). Информация о серверах отображается только когда вы работаете в режиме распределенного решения и multitenancy.
7. **Технологии** – названия модулей или компонентов программы, выполнивших обнаружение.

   В графе **Технологии** могут быть указаны следующие модули и компоненты программы:

   - **(YARA) YARA**.
   - **(SB) Sandbox**.
   - **(URL) URL Reputation**.
   - **(AM) Anti-Malware Engine**.
   - **(TAA) Targeted Attack Analyzer**.
   - **(IOC) IOC**.

8. **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь программы это обнаружение или нет.

   Обнаружения могут быть в одном из следующих состояний:

   - **Новое** – новые обнаружения.
   - **В обработке** – обнаружения, которые один из пользователей программы уже обрабатывает.
   - **Повторная проверка** – обнаружения, выполненные в результате повторной проверки объекта.

   Кроме того, в этой графе отображается имя пользователя, которому назначено данное обнаружение. Например, Administrator.

Если информация в графах таблицы отображается в виде ссылки, по ссылке раскрывается список, в котором вы можете выбрать действие над объектом. В зависимости от типа значения ячейки вы можете выполнить одно из следующих действий:

- Любой тип значения ячейки:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.

- MD5-хеш:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Найти события**.
  - **Найти на KL TIP**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- SHA256-хеш:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Найти события**.
  - **Найти на KL TIP**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- IP-адрес назначения: **Найти события**.
- Состояние обнаружения:
  - **Назначить мне**.
  - **Отметить как обработанное**.

kaspersky

Фильтрация, сортировка и поиск обнаружений

Вы можете отфильтровать обнаружения для отображения в таблице обнаружений по одной или нескольким графам таблицы или выполнить поиск обнаружений по некоторым графам таблицы по указанным вами показателям.

Вы можете создавать, сохранять и удалять фильтры, а также запускать фильтрацию и поиск обнаружений по условиям, заданным в сохраненных фильтрах.

Если вы используете режим распределенного решения и multitenancy, вы не сможете сохранять фильтры на PCN.

Фильтры сохраняются для каждого из пользователей на том сервере, на котором они созданы.

Вы также можете сортировать обнаружения в таблице (см. раздел "Сортировка обнаружений в таблице" на стр. 231) по графам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

В этом разделе

Фильтрация обнаружений по наличию статуса VIP

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю ☆ – наличие у обнаружения статуса с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.

► *Чтобы отфильтровать обнаружения по наличию статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Нажатием на заголовок столбца **VIP** раскройте список параметров фильтрации.
3. Настройте фильтрацию обнаружений:
   - Если вы хотите, чтобы в таблице обнаружений отобразились только обнаружения со статусом VIP, выберите **VIP**.
   - Если вы хотите, чтобы в таблице обнаружений отобразились все обнаружения, выберите **Все**.

   Если ни одно из значений не выбрано, в таблице отображаются все обнаружения.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по времени

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Создано** – время, в которое произошло обнаружение, а также **Обновлено** – время, в которое обнаружение было обновлено.

► *Чтобы отфильтровать или найти обнаружения по времени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Создано** раскройте список периодов отображения обнаружений.
3. В списке **Время** выберите один из следующих периодов отображения обнаружений:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все обнаружения.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице обнаружения, произошедшие за последний час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице обнаружения, произошедшие за последний день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице обнаружения, произошедшие за указанный вами период.
4. Если вы выбрали период отображения событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения обнаружений.

b. Нажмите на кнопку **Применить**.

Календарь закроется.

5. Если вы хотите отфильтровать обнаружения по времени изменения обнаружений, нажмите на **Переключиться на время обновления** в верхней части списка и выполните действия по выбору периода отображения обнаружений.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация обнаружений по степени важности

Вы можете отфильтровать события, обнаруженные программой, а также осуществить поиск событий в таблице событий по показателю **Важность** – важность обнаружения для пользователя программы в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

► *Чтобы отфильтровать обнаружения по степени важности, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По значку раскройте список параметров фильтрации.
3. Выберите одну или несколько из следующих степеней важности обнаружений:
   - **Низкая** – обнаружение низкой степени важности.
   - **Средняя** – обнаружение средней степени важности.
   - **Высокая** – обнаружение высокой степени важности.

   Если ни одно из значений не выбрано, в таблице отображаются обнаружения всех степеней важности.
4. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по категориям обнаруженных объектов

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Обнаружено** – одна или несколько категорий объекта, обнаруженного в событии. Например, если вы хотите, чтобы программа отображала в таблице обнаружения файлов, зараженных определенным вирусом, вы можете задать фильтр по названию этого вируса.

► *Чтобы отфильтровать или найти обнаружения по категориям обнаруженных объектов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке **Обнаружено** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода введите название категории (например, Trojan) или несколько символов из названия категории.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по полученной информации

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Сведения** – краткая информация об обнаружении. Например, имя обнаруженного файла или URL-адрес вредоносной ссылки.

► *Чтобы отфильтровать или найти обнаружения по полученной информации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Сведения** откройте окно настройки фильтрации.
3. В левом раскрывающемся списке выберите один из следующих критериев поиска:
   - **Сведения**. Поиск будет осуществляться по всем сведениям об обнаруженном объекте.
   - **ID**.
   - **Имя файла**.
   - **Тип файла**.
   - **MD5**.
   - **SHA256**.
   - **URL**.
   - **Домен**.
   - **Агент пользователя**.
   - **Тема**.
   - **HTTP-статус**.
   - **Источник объекта**.
   - **Тип объекта**.
4. В правом раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:

- **Содержит**.
- **Не содержит**.
- **Равняется**.
- **Не равняется**.

5. В поле ввода укажите один или несколько символов информации об обнаружении.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по адресу источника

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Адрес источника** – адрес источника обнаружения. Например, адрес электронной почты, с которого был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

► *Чтобы отфильтровать или найти обнаружения по адресу источника, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Адрес источника** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
4. В поле ввода укажите один или несколько символов адреса источника обнаружения.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по адресу назначения

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Адрес назначения** – адрес назначения обнаруженного объекта. Например, IP-адрес

компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

► *Чтобы отфильтровать или найти обнаружения по адресу назначения, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Адрес назначения** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
4. В поле ввода укажите один или несколько символов адреса назначения обнаруженного объекта.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по имени сервера

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Серверы** – имена серверов, на которых выполнено обнаружение.

Если вы используете режим распределенного решения и multitenancy, серверы относятся к той организации, с которой вы работаете в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213). Фильтрация доступна только на PCN.

► *Чтобы отфильтровать или найти обнаружения по имени сервера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Серверы** раскройте список серверов, на которых выполнены обнаружения.
3. Установите флажки рядом с одним или несколькими именами серверов.
4. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по названию технологии

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Технологии** – названия модулей или компонентов программы, выполнивших обнаружение.

► *Чтобы отфильтровать обнаружения по названию технологии, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**, если вы хотите, чтобы программа отображала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Не содержит**, если вы хотите, чтобы программа скрывала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Равняется**, если вы хотите, чтобы программа отображала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Не равняется**, если вы хотите, чтобы программа скрывала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
4. В раскрывающемся списке справа от выбранного вами оператора фильтрации обнаружений выберите название технологии, по которой вы хотите отфильтровать обнаружения:
   - **(YARA) YARA**.
   - **(SB) Sandbox**.
   - **(URL) URL Reputation**.
   - **(AM) Anti-Malware Engine**.
   - **(TAA) Targeted Attack Analyzer**.
   - **(IOC) IOC**.

   Например, если вы хотите, чтобы программа отобразила в списке обнаружения, выполненные компонентом Sandbox, выберите оператор фильтрации **Содержит** и название компонента **(SB) Sandbox**.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по состоянию их обработки пользователем

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь

программы это обнаружение или нет.

► *Чтобы отфильтровать или найти обнаружения по состоянию их обработки пользователем программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Если вы хотите включить в фильтр обработанные обнаружения, включите переключатель **Обработано** в правом верхнем углу окна.
3. По ссылке **Состояние** раскройте список вариантов обнаружений в зависимости от состояния их обработки пользователем программы.
4. Выберите одно из следующих значений:
   - **Новое**, если вы хотите, чтобы программа отображала новые обнаружения, которые ни один из пользователей еще не начал обрабатывать.
   - **В обработке**, если вы хотите, чтобы программа отображала обнаружения, которые один из пользователей программы уже обрабатывает.
   - **Повторная проверка**, если вы хотите, чтобы программа отображала обнаружения, произошедшие в результате повторной проверки.
5. В поле **Имя пользователя** введите имя пользователя, если вы хотите найти обнаружения, назначенные определенному пользователю **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности**.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Сортировка обнаружений в таблице

Вы можете сортировать обнаружения в таблице по графам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

► *Чтобы отсортировать обнаружения в таблице обнаружений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Если вы хотите отсортировать обнаружения по дате, справа от названия графы **Создано** (если в таблице отображается дата создания обнаружений) или **Обновлено** (если в таблице отображается дата обновления обнаружений) нажмите на один из значков:
   - ↑ – новые обнаружения отобразятся вверху таблицы.
   - ↓ – старые обнаружения отобразятся вверху таблицы.
3. Если вы хотите отсортировать обнаружения по степени важности, справа от значка нажмите на один из значков:
   - ↑ – обнаружения высокой степени важности отобразятся вверху таблицы.
   - ↓ – обнаружения низкой степени важности отобразятся вверху таблицы.

4. Если вы хотите отсортировать обнаружения по адресу источника обнаруженного объекта, справа от названия графы **Адрес источника** нажмите на один из значков:
   - ↑ – сортировка выполнится по алфавиту A-Z.
   - ↓ – сортировка выполнится по алфавиту Z-A.
5. Если вы хотите отсортировать обнаружения по состоянию их обработки пользователем, справа от названия графы **Состояние** нажмите на один из значков:
   - ↑ – обнаружения будут отсортированы по порядку их обработки **Новое** - **Повторная проверка** - **В обработке** - **Обработано**.
   - ↓ – обнаружения будут отсортированы по порядку их обработки **Обработано** - **В обработке** - **Повторная проверка** - **Новое**.

Быстрое создание фильтра обнаружений

► *Чтобы быстро создать фильтр обнаружений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:
   a. Наведите курсор мыши на ссылку с тем значением графы таблицы, которое вы хотите добавить в качестве условия фильтрации.
   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.
   c. В открывшемся списке выберите одно из следующих действий:
      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.
3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Сброс фильтра обнаружений

► *Чтобы сбросить фильтр обнаружений по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Нажмите на кнопку ⊠ справа от того заголовка графы таблицы обнаружений, условия фильтрации по которому вы хотите сбросить.

Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

kaspersky

Просмотр обнаружений

В веб-интерфейсе программы отображаются следующие типы обнаружений, на которые пользователю программы рекомендуется обратить внимание:

- На компьютере локальной сети организации были запущены процессы. Программа обнаружила эти процессы с помощью компонента Endpoint Agent (ранее Endpoint Sensors), установленного на компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows.

Если обнаружен файл, в зависимости от того, какие модули или компоненты программы выполнили обнаружение, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и обнаруженном файле (например, IP-адрес компьютера, на котором обнаружен файл, имя обнаруженного файла);
- результаты антивирусной проверки файла, выполненной ядром AM Engine;
- результаты проверки файла на наличие признаков вторжения в IT-инфраструктуру организации, выполненной модулем YARA;
- результаты исследования поведения файла при попадании в операционные системы Windows XP SP3, 64-разрядную Windows 7 и 64-разрядную Windows 10, выполненного компонентом Sandbox;
- результаты анализа исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения.

Если обнаружена ссылка на веб-сайт, в зависимости от того, какие модули или компоненты программы выполнили обнаружение, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и обнаруженной ссылке на веб-сайт (например, IP-адрес компьютера, на котором обнаружена ссылка на веб-сайт, адрес ссылки на веб-сайт);
- результаты проверки ссылки на наличие признаков вредоносного, фишингового URL-адреса или URL-адреса, который ранее использовался злоумышленниками для целевых атак на IT-инфраструктуру организаций, выполненной модулем URL Reputation.

Если обнаружены процессы, запущенные на компьютере локальной сети организации, на котором установлен компонент Endpoint Agent, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и процессах, запущенных на этом компьютере;
- результаты исследования сетевой активности компьютера, выполненного по правилам TAA (IOA) "Лаборатории Касперского";
- результаты исследования сетевой активности компьютера, выполненного по пользовательским правилам TAA (IOA), IOC.

kaspersky

В этом разделе

Просмотр информации об обнаружении

► *Чтобы просмотреть информацию об обнаружении, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об обнаружении.

Общая информация об обнаружении любого типа

Независимо от того, какой технологией выполнено обнаружение - в заголовке окна с информацией об обнаружении отображается идентификатор обнаружения. Рядом с состоянием отображается значок ☆ или ★ в зависимости от наличия у обнаружения статуса VIP.

В верхней части окна с информацией об обнаружении может отображаться следующая общая информация об обнаружении:

- **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь программы это обнаружение или нет.
- **Важность** – важность обнаружения для пользователя программы в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
- **Сервер** – имя сервера, на котором выполнено обнаружение. Серверы относятся к той организации, с которой вы работаете в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).
- **Хост** – доменное имя компьютера, на котором произошло обнаружение.

- **Источник данных** – источник данных. Например, SMTP Sensor или SPAN Sensor.
- **Время создания** – время, когда было выполнено обнаружение.
- **Время обновления** – время, когда была обновлена информация об обнаружении.

Информация в блоке Информация об объекте

В блоке **Информация об объекте** может отображаться следующая информация об обнаруженном файле:

- Имя файла.

  По ссылке с именем файла раскрывается действие **Скопировать значение в буфер**.

- Тип файла. Например, ExecutableWin32.

  Кнопка **Найти на KL TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла (см. раздел "Создание правила запрета" на стр. 318).

  Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

  Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.

- Размер файла в килобайтах.
- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на KL TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- **SHA256** – SHA256-хеш файла.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на KL TIP**.
  - **Найти на virustotal.com**.
  - **Найти события**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

Информация в блоке Информация об обнаружении

В блоке **Информация об обнаружении** может отображаться следующая информация об обнаружении:

- , или – важность обнаружения для пользователя программы в соответствии с тем, какое

влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

- **Время** – время, в которое программа выполнила обнаружение.
- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если программа обнаружила файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
- **URL** – обнаруженный URL-адрес. Может также содержать код ответа.

  По ссылке с **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на KL TIP по URL**.
  - **Найти на KL TIP по имени домена**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **IP назначения** – IP-адрес ресурса, к которому обращался пользователь или программа.

  По ссылке с **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на KL TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Имя пользователя** – имя учетной записи пользователя, действия которого привели к возникновению события.
- **Запрос/Ответ** – длина запроса и ответа.

Информация в блоке Результаты проверки

В блоке **Результаты проверки** могут отображаться следующие результаты проверки обнаружения:

- Названия модулей или компонентов программы, выполнивших обнаружение.
- Одна или несколько категорий обнаруженного объекта. Например, может отображаться название вируса Virus.Win32.Chiton.i.
- Версии баз модулей и компонентов программы, выполнивших обнаружение.
- Результаты проверки обнаружений модулями и компонентами программы:
  - **YARA** – категория обнаруженного файла в правилах YARA (например, может отображаться название категории susp_fake_Microsoft_signer).

    Кнопка **Найти на KL TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

    Кнопка **Создать правило запрета** позволяет запретить запуск файла (см. раздел "Создание правила запрета" на стр. 318).
  - **SB** (Sandbox) – результаты исследования поведения файла, выполненного компонентом

Sandbox.

Нажатием на кнопку **Sandbox-обнаружение** вы можете открыть окно с подробной информацией о результатах исследования поведения файла (см. раздел "Результаты проверки в Sandbox" на стр. 239).

Кнопка **Найти на KL TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** позволяет запретить запуск файла (см. раздел "Создание правила запрета" на стр. 318).

Вы можете загрузить подробный журнал исследования поведения файла во всех операционных системах нажав на кнопку **Скачать сведения об отладке**.

Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя проверенного файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.

> По умолчанию максимальный объем жесткого диска для хранения журналов исследования поведения файлов во всех операционных системах составляет 300 ГБ. По достижении этого ограничения программа удаляет журналы исследования поведения файлов, созданные раньше остальных, и заменяет их новыми журналами.

- **URL** (URL Reputation) – категория обнаруженного вредоносного, фишингового URL-адреса или URL-адреса, который ранее использовался злоумышленниками для целевых атак на IT-инфраструктуру организаций.
- **AM** (Anti-Malware Engine) – категория обнаруженного объекта по антивирусной базе. Например, может отображаться название вируса Virus.Win32.Chiton.i.

  По ссылке открывается информация о категории объекта в базе угроз "Лаборатории Касперского" Kaspersky Threats.

  Кнопка **Найти на KL TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла (см. раздел "Создание правила запрета" на стр. 318).

  Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.
- **TAA** (Targeted Attack Analyzer) – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.
- **IOC** – Название IOC-файла, по которому было выполнено обнаружение.

  При выборе IOC-файла открывается окно с результатами IOC-проверки (см. раздел "Результаты IOC-проверки" на стр. 240).

  По ссылке **Найти события** в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **MD5**, **FileFullName**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

Результаты проверки в Sandbox

В окне результатов проверки объекта в Sandbox могут отображаться следующие сведения об обнаружении:

- **Файл** – полное имя и путь проверенного файла.
- **Размер файла** – размер файла.
- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на KL TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если программа обнаружила файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
- **Время обработки** – время выполнения проверки файла.
- **Версии баз** – версии баз модулей и компонентов программы, выполнивших обнаружение.

Информация о результатах исследования поведения файла приводится для каждой операционной системы, в которой компонент Sandbox выполнил проверку. Для операционной системы Windows 79 (64-разрядная) вы можете просмотреть журналы активности файла для двух режимов проверки компонента Sandbox – **Режим быстрой проверки** и **Режим ведения полного журнала**.

Для каждого режима проверки могут быть доступны следующие журналы активности:

- **Список активностей** – действия файла внутри операционной системы.
- **Дерево активностей** – графическое представление процесса исследования файла.
- **Журнал HTTP-активности** – журнал HTTP-активности файла. Содержит следующую информацию:
  - **IP назначения** – IP-адрес, на который файл пытается перейти из операционной системы.
  - **Метод** – метод HTTP-запроса, например, GET или POST.
  - **URL** – URL-адрес ссылки на веб-сайт, которую файл пытается открыть из операционной системы.

  По ссылкам **IP назначения** и **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на KL TIP**.
  - **Найти события**.
  - **Скопировать значение в буфер**.
- **Журнал DNS-активности** – журнал DNS-активности файла. Содержит следующую информацию:
  - Тип запроса (Request или Response)
  - **DNS-имя** – доменное имя сервера.

- **Тип** – тип DNS-запроса.
- **Ответ** – имя, тип ответа от DNS-сервера, а также имя хоста или IP-адрес компьютера, с которого был получен ответ.

- **Скачать полный журнал** – журнал исследования поведения файла в каждой операционной системе.

Результаты IOC-проверки

В окне результатов обработки IOC-обнаружения отображается следующая информация:

- В блоке **Файл**:
  - **Размер файла**.
  - **Полный путь**. По ссылке **Полный путь** раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события**.
    - **Найти обнаружения**.
    - **Завершить процесс**.
    - **Удалить файл**.
    - **Получить файл**.
    - **Поместить файл на карантин**.
    - **Скопировать значение в буфер**.
  - **SHA256**. По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти на KL TIP**.
    - **Найти на virustotal.com**.
    - **Найти события**.
    - **Найти обнаружения**.
    - **Создать правило запрета**.
    - **Скопировать значение в буфер**.
  - **MD5**. По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти на KL TIP**.
    - **Найти события**.
    - **Найти обнаружения**.
    - **Создать правило запрета**.
    - **Скопировать значение в буфер**.
- В блоке **IOC** приведен XML-код IOC-файла. Критерий, по которому было выполнено обнаружение, выделен желтым цветом.

Информация в блоке Хосты

В блоке **Хосты** отображается следующая информация о хостах, на которых сработало IOA-правило:

- **Имя хоста** – IP-адрес или доменное имя компьютера, на котором произошло событие. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного IOA-правила и выбранный хост.
- **Количество событий** – количество событий, произошедших на хосте.
- **Найти события**. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного IOA-правила.

Информация в блоке Журнал изменений

В блоке **Журнал изменений** может отображаться следующая информация об обнаружении:

- Дата и время изменения обнаружения.
- Автор изменений.

  Например, **Система** или имя пользователя программы.
- Изменение, произошедшее с обнаружением.

  Например, обнаружению может быть присвоена принадлежность группе VIP, или оно может быть отмечено как обработанное.

Отправка данных об обнаружении

Вы можете предоставить в "Лабораторию Касперского" данные об обнаружении (кроме технологий URL Reputation и IOC) для дальнейшего исследования.

Для этого необходимо скопировать данные об обнаружении в буфер обмена, а затем отправить их в "Лабораторию Касперского" по электронной почте.

Данные об обнаружении могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Вам необходимо самостоятельно согласовать отправку этих данных для дальнейшего исследования в "Лабораторию Касперского" со Службой безопасности вашей организации.

► *Чтобы скопировать данные об обнаружении в буфер обмена, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об обнаружении.
3. Нажмите на ссылку **Предоставить данные об обнаружении в "Лабораторию Касперского"** в

нижней части окна с информацией об обнаружении.

Откроется окно **Подробнее**.

4. Просмотрите данные об обнаружении для отправки в "Лабораторию Касперского".
5. Если вы хотите скопировать эти данные, нажмите на кнопку **Скопировать в буфер**.

   Данные об обнаружении будут скопированы в буфер обмена. Вы сможете отправить их в "Лабораторию Касперского" для дальнейшего исследования.

kaspersky

Рекомендации по обработке обнаружений

В составе информации об обнаружениях, выполненных технологиями AM (Anti-Malware Engine), SB (Sandbox), YARA и IOC в правой части окна отображаются рекомендации по обработке этих обнаружений.

► *Чтобы просмотреть информацию об обнаружении, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об обнаружении.

В этом разделе

Рекомендации по обработке AM-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Адрес источника** (см. раздел "**Фильтрация и поиск обнаружений по адресу источника**" на стр. 228). Имя хоста из обнаружения, над которым вы

работаете, выделено желтым цветом.

- **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - URL-адресу из обнаружения, над которым вы работаете.

- В разделе **Оценка** выберите **Найти похожие KES-события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.
- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

Рекомендации по обработке SB-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Адрес источника** (см. раздел "**Фильтрация и поиск обнаружений по адресу источника**" на стр. 228). Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.
  - **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - URL-адресу из обнаружения, над которым вы работаете.

- В разделе **Оценка** выберите **Найти похожие KES-события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5

файла из обнаружения.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

Рекомендации по обработке YARA-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.
  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Адрес источника** (см. раздел "**Фильтрация и поиск обнаружений по адресу источника**" на стр. 228). Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.
  - **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - URL-адресу из обнаружения, над которым вы работаете.
- В разделе **Оценка** выберите **Найти похожие KES-события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.
- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

kaspersky

Рекомендации по обработке IOC-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

► *Вы можете выполнить следующие рекомендации:*

- В разделе **Оценка** выберите **Найти похожие обнаружения по имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Адрес источника** (см. раздел "**Фильтрация и поиск обнаружений по адресу источника**" на стр. 228). Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.
- В разделе **Оценка** выберите **Найти похожие обнаружения по IOC**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Обнаружено** (см. раздел "**Фильтрация и поиск обнаружений по адресу источника**" на стр. 228) - имени IOC-файла из обнаружения, над которым вы работаете.
- В разделе **Сдерживание** выберите **Изолировать <имя хоста>**. Откроется окно создания правила сетевой изоляции.

► *Чтобы создать правило сетевой изоляции хоста, настройте следующие параметры:*

1. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.
2. В блоке параметров **Исключения для правила изоляции хоста** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.
3. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.
4. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.
5. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия 5–7.
6. Нажмите на кнопку **Сохранить**.

Хост будет изолирован от сети.

kaspersky

Действия пользователей над обнаружениями

При работе в веб-интерфейсе программы под учетной записью с ролью **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** вы можете выполнять следующие действия над обнаружениями:

- Назначить обнаружение себе или другому пользователю веб-интерфейса программы.

  Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 230).

- Отметить обнаружение как обработанное.

  Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 230).

- Добавить комментарий к обнаружению.

  Вы можете найти обнаружения, содержащие комментарий, по ключевым словам комментария, используя фильтр обнаружений по полученной информации (см. раздел "Фильтрация и поиск обнаружений по полученной информации" на стр. 227).

- Присвоить обнаружению статус VIP.

  Это действие доступно только пользователям с ролью **Старший сотрудник службы безопасности**. Пользователи с этой ролью могут просмотреть все обнаружения со статусом VIP, используя фильтр обнаружений по наличию статуса VIP (см. раздел "Фильтрация обнаружений по наличию статуса VIP" на стр. 225).

В этом разделе

Назначение нескольких обнаружений определенному пользователю

► *Чтобы назначить обнаружение себе или другому пользователю веб-интерфейса программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, которые вы хотите назначить пользователю.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. В появившейся панели в нижней части окна нажатием на стрелку справа от кнопки **Отметить как обработанное** раскройте список пользователей.
4. Выберите пользователя, которому вы хотите назначить обнаружения.

   Откроется окно подтверждения действия.

5. Нажмите на кнопку **Продолжить**

Обнаружения будут назначены выбранному пользователю.

Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 230).

Назначение обнаружений себе или другому пользователю

► *Чтобы назначить одно или несколько обнаружений себе или другому пользователю, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, которые вы хотите назначить себе или другому пользователю.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. В появившейся панели в нижней части окна нажмите на кнопку **Отметить как обработанное**.
4. Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

5. Нажмите на кнопку **Продолжить**.

Обнаружение будет назначено выбранному пользователю.

Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем.

Отметка о завершении обработки одного обнаружения

► *Чтобы отметить в таблице обнаружений одно обнаружение, назначенное вам, как обработанное, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. В графе **Состояние** того обнаружения, которое вы хотите отметить как обработанное, левой кнопкой мыши нажмите на ваше имя пользователя.
3. В списке действий выберите **Отметить как обработанное**.

Обнаружение будет отмечено как обработанное.

► *Чтобы отметить обнаружение как обработанное в процессе работы с этим обнаружением, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Откройте обнаружение, которое вы хотите отметить как обработанное.
3. В правом верхнем углу окна нажатием на стрелку справа от кнопки со статусом обнаружения раскройте список действий.
4. В списке действий выберите **Отметить как обработанное**.

Обнаружение будет отмечено как обработанное. Если обнаружение было назначено другому пользователю, оно будет отмечено как обработанное вами.

Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем.

Отметка о завершении обработки обнаружений

► *Чтобы отметить одно или несколько обнаружений как обработанные, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, которые вы хотите отметить как обработанные.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. В появившейся панели в нижней части окна нажмите на кнопку **Отметить как обработанное**.

   Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

4. Нажмите на кнопку **Продолжить**.

Выбранные обнаружения будут отмечены как обработанные. Если обнаружения были назначены другим пользователям, они будут отмечены как обработанные вами.

Вы можете просмотреть все обработанные обнаружения, используя фильтр обнаружений по состоянию их обработки пользователем (см. раздел "Фильтрация и поиск обнаружений по состоянию их обработки пользователем" на стр. 230).

Изменение статуса VIP обнаружений

Пользователи с ролью **Старший сотрудник службы безопасности** могут присваивать обнаружениям статус VIP и лишать обнаружения статуса VIP.

► *Чтобы изменить статус VIP обнаружений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, статус VIP которых вы хотите изменить.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. Выполните одно из следующих действий:

   - Если вы хотите присвоить обнаружениям статус VIP, в появившейся панели в нижней части окна нажмите на кнопку **Присвоить статус VIP**.
   - Если вы хотите лишить обнаружения статуса VIP, в появившейся панели в нижней части окна в раскрывающемся списке **Присвоить статус VIP** выберите пункт **Лишить статуса VIP**.

   Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

4. Нажмите на кнопку **Продолжить**

Статус VIP обнаружений будет изменен.

Пользователи с ролью **Старший сотрудник службы безопасности** могут просмотреть все обнаружения со статусом VIP, используя фильтр обнаружений по наличию статуса VIP (см. раздел "Фильтрация обнаружений по наличию статуса VIP" на стр. 225).

Добавление комментария к обнаружению

► *Чтобы добавить комментарий к обнаружению, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Выберите обнаружение, к которому вы хотите добавить комментарий.

   Откроется окно с информацией об обнаружении.

3. В поле добавления комментария под названием блока **Журнал изменений** введите комментарий к обнаружению.

4. Нажмите на кнопку **Добавить**.

Комментарий к обнаружению будет добавлен и отобразится в блоке **Журнал изменений** этого обнаружения.

Вы можете найти обнаружения, содержащие комментарий, по ключевым словам комментария, используя фильтр обнаружений по полученной информации (см. раздел "Фильтрация и поиск обнаружений по полученной информации" на стр. 227).

kaspersky

Поиск угроз по базе событий

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** могут формировать поисковые запросы и использовать IOC-файлы и IOA-правила для поиска угроз по базе событий в рамках тех организаций, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

Для формирования поисковых запросов по базе событий вы можете использовать *режим конструктора* или *режим исходного кода*.

В режиме конструктора вы можете создавать и изменять поисковые запросы с помощью раскрывающихся списков с вариантами типа значения поля и операторов.

В режиме исходного кода (см. раздел "Поиск событий с помощью режима исходного кода" на стр. 253) вы можете создавать и изменять поисковые запросы с помощью текстовых команд.

Вы можете загрузить IOC-файл и искать события по условиям, заданным в этом IOC-файле.

Вы также можете создавать IOA-правила (см. раздел "Создание пользовательского правила TAA (IOA) на основе условий поиска событий" на стр. 257) на основе условий поиска событий.

В этом разделе

Поиск событий с помощью режима конструктора

► *Чтобы задать условия поиска событий в режиме конструктора, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.
2. В раскрывающемся списке выберите критерий для поиска событий в одной из следующих групп:
   - **Общие сведения**.
   - **Свойства TAA**.
   - **Свойства файла**.
   - **Запущен процесс**.
   - **Удаленное соединение**.

- **Изменение в реестре**.
- **Событие в журнале Windows**.
- **Изменено имя хоста**.
- **Обнаружение и результат обработки**.
- **Интерактивный ввод команд в консоли**.

3. В раскрывающемся списке выберите один из следующих операторов сравнения:
   - **=**.
   - **!=**.
   - **CONTAINS**.
   - **!CONTAINS**.
   - **STARTS**.
   - **!STARTS**.
   - **ENDS**.
   - **!ENDS**.
   - **>**.
   - **<**.

   Для каждого типа значения поля будет доступен свой релевантный набор операторов сравнения. Например, при выборе типа значения поля **EventType** будут доступны операторы **=** и **!=**.
4. В зависимости от выбранного типа значения поля выполните одно из следующих действий:
   - Укажите в поле один или несколько символов, по которым вы хотите выполнить поиск событий.
   - В раскрывающемся списке выберите вариант значения поля, по которому вы хотите выполнить поиск событий.

   Например, для поиска полного совпадения по имени пользователя введите имя пользователя.
5. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.
6. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.
7. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.
8. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **За все время** выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.

9. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
10. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям поиска.

Поиск событий с помощью режима исходного кода

► *Чтобы задать условия поиска событий в режиме исходного кода, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Редактор кода**.

   Откроется форма с полем ввода условий поиска событий в режиме исходного кода.
2. Введите условия поиска событий, используя команды, логические операторы `OR` и `AND`, а также скобки для создания групп условий.

   Команды должны соответствовать следующему синтаксису: `<тип поля> <оператор сравнения> <значение поля>`.

Пример:

```
EventType = "filechange"
AND (
    FileName CONTAINS "example"
    OR UserName = "example"
)
```

3. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.
4. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

b. Нажмите на кнопку **Применить**.

Календарь закроется.

5. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям поиска.

Изменение условий поиска событий

► *Чтобы изменить условия поиска событий, выполните следующие действия в разделе **Поиск угроз** окна веб-интерфейса программы:*

1. Нажмите на форму с условиями поиска событий в верхней части окна.
2. Выберите одну из следующих закладок:
   - **Конструктор**, если вы хотите изменить условия поиска событий в режиме конструктора.
   - **Редактор кода**, если вы хотите изменить условия поиска событий в режиме исходного кода.
3. Внесите необходимые изменения.
4. Нажмите на одну из следующих кнопок:
   - **Обновить**, если вы хотите обновить текущий поиск событий новыми условиями.
   - **Новый поиск**, если вы хотите выполнить новый поиск событий.

Отобразится таблица событий, соответствующих условиям поиска.

Поиск событий по результатам их обработки в Kaspersky Endpoint Security

► *Чтобы выполнить поиск событий по результатам их обработки в Kaspersky Endpoint Security в режиме конструктора, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.
2. Если вы хотите выполнить поиск событий по статусу обработки, выполните следующие действия:
   a. В раскрывающемся списке критериев поиска событий в группе **Обнаружение и результат обработки** выберите критерий **ThreatStatus**.
   b. В раскрывающемся списке операторов сравнения выберите один из вариантов:
      - **=** (равно);
      - **!=** (не равно).
   c. В раскрывающемся списке статусов обработки события выберите один из вариантов:
      - **Объект чистый**.
      - **Объект вылечен**.
      - **Ложное срабатывание**.

- **Объект добавлен пользователем**.
- **Объект добавлен в исключения**.
- **Объект удален**.
- **Объект помещен на карантин**.
- **Объект не найден**.
- **Выполнен откат к предыдущему состоянию**.
- **Обработка прервана**.
- **Объект не поддается обработке**.
- **Объект не обработан**.
- **Нет данных**.

3. Если вы хотите выполнить поиск событий по причинам, по которым они не были обработаны, выполните следующие действия:
   a. В раскрывающемся списке критериев поиска событий в группе **Обнаружение и результат обработки** выберите критерий **UntreatedReason**.
   b. В раскрывающемся списке операторов сравнения выберите один из вариантов:
      - **=** (равно);
      - **!=** (не равно).
   c. В раскрывающемся списке причин, по которым события не были обработаны, выберите один из вариантов:
      - **Объект уже был обработан**.
      - **Обработка отменена**.
      - **Не удалось создать резервную копию объекта**.
      - **Не удалось создать копию объекта**.
      - **Устройство не готово**.
      - **Объект заблокирован**.
      - **Нет прав на выполнение действия**.
      - **Объект невозможно вылечить**.
      - **Объект невозможно перезаписать**.
      - **Объект не найден**.
      - **Нет места на диске**.
      - **Действие отложено**.
      - **Ошибка чтения данных**.
      - **Программа работает в режиме Только отчет**.
      - **Объект является критическим системным**.
      - **Задача на обработку прервана**.
      - **Ошибка записи данных**.

- **Запись данных не поддерживается**.
- **Объект защищен от записи**.

4. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.
5. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.
6. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.
7. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **За все время** выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.
8. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
9. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям поиска.

Загрузка IOC-файла и поиск событий по условиям, заданным в IOC-файле

► *Чтобы загрузить IOC-файл и искать события по условиям, заданным в этом IOC-файле, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.
2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файлов.
3. Выберите IOC-файл, который хотите загрузить, и нажмите на кнопку **Открыть**.

   IOC-файл загрузится.

   На закладке **Редактор кода** в форме с условиями поиска событий отобразятся условия, заданные в загруженном IOC-файле.

Вы можете искать события по этим условиям. Вы также можете изменить условия, заданные в загруженном IOC-файле, или добавить условия поиска событий в режиме исходного кода.

4. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.
5. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
6. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям, заданным в IOC-файле.

Создание пользовательского правила TAA (IOA) на основе условий поиска событий

► *Чтобы создать пользовательское правило TAA (IOA) на основе условий поиска событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.
2. Выполните поиск событий с помощью режима конструктора или режима исходного кода.
3. Нажмите на кнопку **Сохранить как правило TAA (IOA)**.

   Откроется окно **Сохранить**.
4. В поле **Имя** введите имя правила.
5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В таблице правил TAA (IOA) раздела **Правила пользователей**, подразделе **TAA** веб-интерфейса отобразится новое правило с заданным именем.

Не рекомендуется в условиях поиска событий, сохраняемых как пользовательское правило TAA (IOA), использовать следующие поля:

- IOAId.

- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

На момент сохранения пользовательского правила TAA (IOA) в программе может не быть событий, содержащих данные для этих полей. Когда события с этими данными появятся, пользовательское правило TAA (IOA), созданное ранее, не сможет разметить события по этим полям.

kaspersky

Информация о событиях

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут просматривать информацию о событиях в рамках тех организаций, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

В информации о событиях отображаются локальные метки времени того компьютера с компонентом Endpoint Agent, на котором было обнаружено событие. Администратору программы необходимо контролировать актуальность времени на компьютерах с компонентом Endpoint Agent.

Если вы используете режим распределенного решения и multitenancy, в разделе отображаются данные по выбранной вами организации (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).

► *Чтобы включить отображение событий по всем организациям,*

включите переключатель **Искать по всем организациям**.

kaspersky

В этом разделе

Просмотр таблицы событий

Таблица событий отображается в разделе **Поиск угроз** окна веб-интерфейса программы после выполнения поиска угроз по базе событий.

События сгруппированы по хостам выбранных серверов и организаций. В таблице событий содержится следующая информация:

1. **Время события** – дата и время обнаружения события.
2. **Событие** – тип события.
3. **Хост** – имя хоста, на котором было обнаружено событие.
4. **Сведения** – сведения о событии.
5. **Имя пользователя** – имя пользователя компьютера с компонентом Endpoint Agent, под учетной записью которого было обнаружено событие.

У каждого типа событий есть свой набор данных в графе таблицы событий **Сведения** (см. таблицу ниже).

*Таблица 13. Набор данных в графе **Сведения** для каждого типа событий в графе **Событие***

Событие	Сведения
Запущен процесс	Имя файла процесса, который был запущен. SHA256- и MD5-хеш. Важность события.

Событие	Сведения
Загружен модуль	Имя динамической библиотеки, которая была загружена. SHA256- и MD5-хеш. Важность события.
Удаленное соединение	IP- или URL-адрес, к которому была произведена попытка удаленного подключения. Имя файла, который пытался осуществить удаленное подключение. Важность события.
Правило запрета	Имя файла приложения, запуск которого был заблокирован. SHA256- и MD5-хеш. Важность события.
Заблокирован документ	Имя документа, запуск которого был заблокирован. SHA256- и MD5-хеш. Важность события.
Создан файл	Имя созданного файла. SHA256- и MD5-хеш. Важность события.
Событие в журнале Windows	Важность события.
Изменение в реестре	Имя ключа в реестре. `<имя переменной в ключе>=<значение переменной>`. Важность события.
Прослушан порт	Адрес сервера и порт. Имя файла процесса, который осуществляет прослушивание порта. Важность события.
Загружен драйвер	Имя файла драйвера, который был загружен. SHA256- и MD5-хеш. Важность события.
Изменено имя хоста	Старое имя хоста. Новое имя хоста. Важность события.
Обнаружение	Путь к обнаруженному файлу. SHA256- и MD5-хеш. Категория обнаруженного объекта (например, название вируса). Важность события.
Результат обработки обнаружения	Путь к обнаруженному файлу. SHA256- и MD5-хеш. Категория обнаруженного объекта (например, название вируса). Важность события.
Интерпретированный запуск файла	Важность события.
Интерактивный ввод команд в консоли	Важность события.

По ссылке с названием типа события, сведениями, дополнительной информацией и именем пользователя раскрывается список, в котором вы можете выбрать действие над объектом. В зависимости от типа значения ячейки вы можете выполнить одно из следующих действий:

- Любой тип значения ячейки:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- Имя файла:

  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Поместить файл на карантин**.
- MD5-хеш:
  - **Найти на KL TIP**.
  - **Создать правило запрета**.
  - **Найти в хранилище**.
- SHA256-хеш:
  - **Найти на KL TIP**.
  - **Найти на virustotal.com**.
  - **Создать правило запрета**.
  - **Найти в хранилище**.

Просмотр информации о событии

► *Чтобы просмотреть информацию о событии, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Конструктор** или **Редактор кода**.

   Откроется форма поиска событий.
2. Если вы используете режим распределенного решения и multitenancy и хотите включить отображение событий по всем организациям, включите переключатель **Искать по всем организациям**.
3. Выполните поиск событий с помощью режима конструктора или режима исходного кода (см. раздел "Поиск событий с помощью режима исходного кода" на стр. 253).

   Отобразится таблица событий.
4. Выберите событие, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о событии.

Рекомендации по обработке событий

В окне события в рамке между деревом событий и текстовой информацией отображаются рекомендации по обработке этого события.

Вы можете выполнить следующие рекомендации:

- **Изолировать <имя хоста>** – изолировать хост (см. раздел "Сетевая изоляция хостов Endpoint Agent" на стр. 296) с Endpoint Agent, на котором обнаружено событие, от сети. Для всех типов событий.
- **Создать правило запрета** – запретить запуск файла (см. раздел "Работа с политиками (правилами

запрета)" на стр. 315), обнаруженного в событии. Для всех типов событий кроме **Событие в журнале Windows** и **Изменено имя хоста**.

- **Создать задачу** – создать задачу. Для всех типов событий кроме **Событие в журнале Windows** и **Изменено имя хоста**.

► *Чтобы изолировать хост от сети, выполните следующие действия:*

1. В рамке с рекомендациями выберите **Изолировать <имя хоста>**.

   Откроется окно параметров изоляции хоста из события, с которым вы работаете.

2. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.
3. В блоке параметров **Исключения для правила изоляции хоста** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.
4. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.
5. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.
6. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия 5–7.
7. Нажмите на кнопку **Сохранить**.

Хост будет изолирован от сети.

Информация об изоляции хоста отобразится в разделе **Endpoint Agents** веб-интерфейса (см. раздел «Сетевая изоляция хостов Endpoint Agent» на стр. 296).

Вы также можете создать правило сетевой изоляции по ссылке **Изолировать <имя хоста>** в информации об обнаружении (см. раздел «Просмотр информации об обнаружении» на стр. 235) и в разделе **Endpoint Agents** веб-интерфейса (см. раздел «Сетевая изоляция хостов Endpoint Agent» на стр. 296).

► *Чтобы создать запрет запуска файла, выполните следующие действия:*

1. В рамке с рекомендациями выберите **Создать правило запрета**.

   Откроется окно создания правила запрета с MD5- или SHA256-хешем файла из события, с которым вы работаете.

2. Задайте значения следующих параметров:
   a. **Состояние** – состояние правила запрета:
      - Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
      - Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.

   b. **Имя** – имя правила запрета.

   c. Если вы хотите, чтобы программа выводила уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показать пользователю уведомление о выполнении задачи**.

   d. Если вы хотите изменить область применения правила запрета, настройте параметр **Запрет**

для:

- Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

  Этот вариант доступен только при включенном режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy.
- Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

3. Нажмите на кнопку **Добавить**.

Запрет на запуск файла будет создан.

Информация о созданном запрете отобразится в разделе **Политики** веб-интерфейса (см. раздел "Работа с политиками (правилами запрета)" на стр. 315).

Если вы установили флажок **Показать пользователю уведомление о выполнении задачи**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.

► *Чтобы создать задачу, выполните следующие действия:*

1. В рамке с рекомендациями по ссылке **Создать задачу** раскройте список типов задач.
2. Выберите один из типов задач:
   - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
   - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
   - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
   - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
   - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).

   Откроется окно создания задачи с предзаполненными данными (например, путем к файлу, MD5- или SHA256-хешем файла) из события, с которым вы работаете.
3. Если вы хотите добавить комментарий к задаче, введите его в поле **Описание**.
4. Если вы хотите изменить область применения задачи, настройте параметр **Задача для**:
   - Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
   - Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

     Этот вариант доступен только при включенном режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy.

- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

5. Если вы не хотите запускать программы от имени текущего пользователя и хотите запустить ее от имени другого пользователя установите флажок **Выполнить под учетной записью** в полях **Пользователь** и **Пароль** введите учетные данные пользователя, от имени которого программа будет запущена.

   По умолчанию флажок снят. Программа будет запущена от имени текущего пользователя.

6. Нажмите на кнопку **Добавить**.

Задача будет создана.

Информация о созданной задаче отобразится в разделе **Задачи** веб-интерфейса (см. раздел "Работа с задачами" на стр. 299).

Информация о событии Запущен процесс

В окне с информацией о событиях типа **Запущен процесс** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).

- Раздел **Запущен процесс**:

  - **Имя IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

  - **Время события** – время запуска процесса.
  - **Файл** – имя файла процесса.
  - **Параметры запуска** – параметры запуска процесса.
  - **Время завершения** – время завершения процесса.
  - **ID процесса** – идентификатор процесса.
  - **Тип учетной записи** – тип учетной записи, под которой был запущен процесс. Например, администратор.
  - **Тип входа в систему** – каким образом был совершен вход в систему.
  - **Имя хоста** – имя хоста Endpoint Agent, на котором был запущен процесс.
  - **Имя пользователя** – имя пользователя, запустившего процесс.

- Раздел **Родительский процесс**:

  - **Файл** – путь к файлу родительского процесса.

- **MD5** – MD5-хеш файла родительского процесса.
- **SHA256** – SHA256-хеш файла родительского процесса.
- **ID процесса** – идентификатор родительского процесса.

- Раздел **Файл**:
  - **MD5** – MD5-хеш файла процесса.
  - **SHA256** – SHA256-хеш файла процесса.
  - **Размер** – размер файла процесса.
  - **Название программы**. Например, название операционной системы.
  - **Производитель**. Например, производитель операционной системы.
  - **Описание файла**. Например, Example File.
  - **Исходное имя файла**. Например, ExampleFile.exe.
  - **Организация** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи**. Например, подпись недействительна или подпись OK.
  - **Свойства** – атрибут файла по классификации Windows. Например, A (архив), D (директория) или S (системный).
  - **Время создания** – время создания файла процесса.
  - **Время изменения** – время последнего изменения файла процесса.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.

- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти на virustotal.com**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

Информация о событии Загружен модуль

В окне с информацией о событиях типа **Загружен модуль** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).
- Раздел **Загружен модуль**:
  - **Время события** – время загрузки модуля.
  - **Файл** – имя файла загруженного модуля.
  - **Имя хоста** – имя хоста, на котором был загружен модуль.
  - **Имя пользователя** – имя пользователя, загрузившего модуль.
- Раздел **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

- Раздел **Файл**:
  - **MD5** – MD5-хеш файла загруженного модуля.
  - **SHA256** – SHA256-хеш файла загруженного модуля.
  - **Размер** – размер загруженного модуля.
  - **Название программы**. Например, название операционной системы.
  - **Производитель**. Например, производитель операционной системы.
  - **Описание файла**. Например, Example File.
  - **Исходное имя файла**. Например, ExampleFile.exe.
  - **Организация** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи**. Например, подпись недействительна или подпись OK.
  - **Время создания** – время создания загруженного модуля.
  - **Время изменения** – дата последнего изменения загруженного модуля.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.

- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти на virustotal.com**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

Информация о событии Удаленное соединение

В окне с информацией о событиях типа **Удаленное соединение** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).
- Раздел **Удаленное соединение**:
  - **Время события** – время попытки удаленного соединения.
  - **Направление соединения** – направление соединения (Входящее или Исходящее).
  - **Удаленный IP-адрес** – IP-адрес хоста, на который была произведена попытка удаленного соединения.
  - **Локальный IP-адрес** – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
  - **Имя хоста** – имя хоста, с которого была произведена попытка удаленного соединения.
  - **Имя пользователя** – имя пользователя, который пытался установить удаленное соединение.
- Раздел **Родительский процесс**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих

действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти на virustotal.com**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

kaspersky

Информация о событии Правило запрета

В окне с информацией о событиях, в которых сработали правила запрета (см. раздел «Работа с политиками (правилами запрета)» на стр. 315) - событиях типа **Правило запрета** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).

- Раздел **Правило запрета**:
  - **Время события** – время срабатывания запрета запуска файла (см. раздел "Работа с политиками (правилами запрета)" на стр. 315).
  - **Файл** – имя файла, запуск которого был запрещен.
  - **Параметры запуска** – параметры, с которыми была произведена попытка запуска файла.
  - **Имя хоста** – имя хоста, на котором сработал запрет запуска файла.
  - **Имя пользователя** – имя пользователя, попытавшегося запустить файл.
- Раздел **Родительский процесс**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
- Раздел **Файл**:
  - **MD5** – MD5-хеш файла, запуск которого был запрещен.
  - **SHA256** – SHA256-хеш файла, запуск которого был запрещен.
  - **Размер** – размер файла, запуск которого был запрещен.
  - **Название программы**. Например, название операционной системы.
  - **Производитель**. Например, производитель операционной системы.
  - **Описание файла**. Например, Example File.
  - **Исходное имя файла**. Например, ExampleFile.exe.
  - **Организация** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи**. Например, подпись недействительна или подпись OK.
  - **Время создания** – время создания файла, запуск которого был запрещен.
  - **Время изменения** – дата последнего изменения файла, запуск которого был запрещен.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).

- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти на virustotal.com**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

Информация о событии Заблокирован документ

В окне с информацией о событиях типа **Заблокирован документ** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).
- Раздел **Заблокирован документ**:
  - **Время события** – время блокирования документа.
  - **Файл** – имя заблокированного документа.
  - **MD5** – MD5-хеш заблокированного документа.
  - **Файл процесса** – имя файла процесса, который попытался открыть документ.
  - **MD5 процесса** – MD5-хеш процесса, который попытался открыть документ.
  - **SHA256 процесса** – SHA256-хеш процесса, который попытался открыть документ.
  - **ID процесса** – идентификатор процесса, который попытался открыть документ.
  - **Имя хоста** – имя хоста, на котором был заблокирован документ.
  - **Имя пользователя** – имя пользователя, попытавшегося открыть документ.
- Раздел **Родительский процесс**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).

- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти на virustotal.com**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

Информация о событии Создан файл

В окне с информацией о событиях типа **Создан файл** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).
- Раздел **Создан файл**:
  - **Время события** – время обнаружения события.
  - **Файл** – имя созданного файла.

- **MD5** – MD5-хеш созданного файла.
- **SHA256** – SHA256-хеш созданного файла.
- **Размер** – размер созданного файла.
- **Время создания** – время создания файла.
- **Время изменения** – время последнего изменения файла.
- **Имя хоста** – имя хоста, на котором был создан файл.
- **Имя пользователя** – имя пользователя, создавшего файл.

- Раздел **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).

- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти на virustotal.com**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

Информация о событии Событие в журнале Windows

В окне с информацией о событиях типа **Событие в журнале Windows** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).
- Раздел **Событие в журнале Windows**:
  - **Время события** – время обнаружения события.
  - **ID события безопасности** – идентификатор типа события безопасности в журнале Windows.
  - **Имя хоста** – имя хоста, на котором произошло событие.
- Блоки параметров **System** и **EventData**, содержащие данные из системного журнала Windows. Состав данных зависит от типа события Windows.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).

- **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
- **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).

- **Скопировать значение в буфер**.

Информация о событии Изменение в реестре

В окне с информацией о событиях типа **Изменение в реестре** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).
- Раздел **Изменение в реестре**:
  - **Время события** – время внесения изменения в реестр.
  - **Путь к разделу реестра** – путь к разделу реестра, в котором было произведено изменение.
  - **Имя параметра реестра** – имя параметра реестра.
  - **Параметр реестра** – значение параметра реестра.
  - **Имя хоста** – имя хоста, на котором было произведено изменение в реестре.
  - **Имя пользователя** – имя пользователя, совершившего изменение в реестре.
- Раздел **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

По ссылке с путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).

- **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
- **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).

- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти на virustotal.com**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

Информация о событии Прослушан порт

В окне с информацией о событиях типа **Прослушан порт** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- Рекомендации по обработке события (см. раздел "Рекомендации по обработке событий" на стр. 262).
- Раздел **Прослушан порт**:
  - **Время события** – время прослушивания порта.
  - **Локальный порт** – порт, который был прослушан.
  - **Локальный IP-адрес** – IP-адрес сетевого интерфейса, порт которого был прослушан.
  - **Имя хоста** – имя хоста, порт которого был прослушан.
  - **Имя пользователя** – имя пользователя, от имени которого было совершено прослушивание порта.
- Раздел **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

По ссылке с путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- Выполнить задачи:
  - **Завершить процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Завершить уникальный процесс** (см. раздел "**Создание задачи завершения процесса**" на стр. 302).
  - **Удалить файл** (см. раздел "**Создание задачи удаления файла**" на стр. 306).
  - **Получить файл** (см. раздел "**Создание задачи получения файла**" на стр. 305).
  - **Поместить файл на карантин** (см. раздел "**Создание задачи помещения файла на карантин**" на стр. 306).
  - **Выполнить программу** (см. раздел "**Создание задачи выполнения программы**" на стр. 303).
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события** (см. раздел "**Поиск угроз по базе событий**" на стр. 251).
- **Найти обнаружения** (см. раздел "**Таблица обнаружений**" на стр. 221).
- **Найти на KL TIP**.
- **Найти на virustotal.com**.
- **Найти в хранилище** (см. раздел "**Работа с объектами в Хранилище и на карантине**" на стр. 347).
- **Создать правило запрета** (см. раздел "**Работа с политиками (правилами запрета)**" на стр. 315).
- **Скопировать значение в буфер**.

Информация о загрузке драйвера

В окне с информацией о событиях типа **Загружен драйвер** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- **Загружен драйвер**:
  - **Время события** – время загрузки драйвера.
  - **Файл** – имя файла загруженного драйвера.
  - **MD5** – MD5-хеш файла загруженного драйвера.
  - **SHA256** – SHA256-хеш файла загруженного драйвера.
  - **Имя хоста** – имя хоста, на который был загружен драйвер.
  - **Размер** – размер загруженного драйвера.
  - **Время создания** – время создания загруженного драйвера.
  - **Время изменения** – время последнего изменения загруженного драйвера.

Информация об изменении имени хоста

В окне с информацией о событиях типа **Изменено имя хоста** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- **Изменено имя хоста**:
  - **Время события** – время изменения имени хоста.
  - **Имя хоста** – новое имя хоста.
  - **Имя пользователя** – имя пользователя, изменившего имя хоста.
  - **Старое имя хоста** – старое имя хоста.

Информация о событии Обнаружение

В окне с информацией о событии типа **Обнаружение** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- На закладке **Сведения** в блоке параметров **Обнаружение**:
  - **Время события** – дата и время события.
  - **Обнаружено** – имя обнаруженного объекта. Вы можете нажать на имя объекта и по ссылке **Найти события** найти все события, в которых был обнаружен этот объект.
  - **Последнее действие** – последнее действие над обнаруженным объектом.
  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.

- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
- **Тип объекта** – тип объекта (например, файл).
- **Имя объекта** – полное имя файла, в котором обнаружен объект.
- **MD5** – MD5-хеш файла, в котором обнаружен объект.
- **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
- **Режим обнаружения** – режим проверки, в котором выполнено обнаружение.
- **ID записи** – идентификатор записи об обнаружении в базе.
- **Версия баз** – версия баз, с помощью которых выполнено обнаружение.

- На закладке **Сведения** в блоке параметров **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.
- На закладке **История** в таблице:
  - **Тип** – тип события: **Обнаружение** и **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время обнаружения и результата обработки обнаружения.

Информация о результатах обработки обнаружения

В окне с информацией о событии типа **Результат обработки обнаружения** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- На закладке **Сведения** в блоке параметров **Результат обработки обнаружения**:
  - **Время события** – дата и время события.
  - **Обнаружено** – имя обнаруженного объекта. Вы можете нажать на имя объекта и по ссылке **Найти события** найти все события, в которых был обнаружен этот объект.
  - **Последнее действие** – последнее действие над обнаруженным объектом.
  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.
  - **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
  - **Тип объекта** – тип объекта (например, файл).

- **Имя объекта** – полное имя файла, в котором обнаружен объект.
- **MD5** – MD5-хеш файла, в котором обнаружен объект.
- **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
- **Режим обнаружения** – режим проверки, в котором выполнено обнаружение.
- **ID записи** – идентификатор записи об обнаружении в базе.
- **Версия баз** – версия баз, с помощью которых выполнено обнаружение.

- На закладке **Сведения** в блоке параметров **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.
- На закладке **История** в таблице:
  - **Тип** – тип события **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время результата обработки обнаружения.

kaspersky

Работа с информацией о хостах с компонентом Endpoint Agent

Компонент Endpoint Agent устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**, **Локальный администратор** и **Администратор** могут оценить регулярность получения данных с хостов, на которых установлен компонент Endpoint Agent, на закладке **Endpoint Agents** окна веб-интерфейса программы в рамках тех организаций, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148). Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, то в веб-интерфейсе сервера PCN отображается список компонентов Endpoint Agent для PCN и всех подключенных SCN.

Пользователи с ролью **Локальный администратор** и **Администратор** могут настроить отображение регулярности получения данных с хостов, на которых установлен компонент Endpoint Agent, в рамках тех организаций, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети любой из хостов с компонентом Endpoint Agent в рамках тех организаций, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148). При этом соединение между сервером с компонентом Central Node и хостом с компонентом Endpoint Agent не будет прервано.

Для оказания поддержки при неполадках в работе компонента Endpoint Agent специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode (см. стр. 142)):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов программы.
- Изменить параметры хранения и отправки получаемой 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 т.д.), а также состав собираемых в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Собранная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка собранных данных в "Лабораторию Касперского" не выполняется.

kaspersky

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

Просмотр таблицы хостов Endpoint Agent на отдельном сервере Central Node

Таблица хостов с компонентом Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса программы.

Если вы используете отдельный сервер Central Node, не используете режим распределенного решения (см. раздел «Распределенное решение и режим multitenancy» на стр. 76) и multitenancy, в таблице хостов с компонентом Endpoint Agent могут отображаться следующие данные:

- **Хост** – имя хоста с компонентом Endpoint Agent.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Agent.
- **Версия** – версия установленного компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent. Может принимать следующие

значения:

- **Нормальная активность** – хосты, от которых последние данные были получены недавно.
- **Предупреждение** – хосты, от которых последние данные были получены давно.
- **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Просмотр таблицы хостов Endpoint Agent в режиме распределенного решения и multitenancy

Таблица хостов с компонентом Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса программы.

Если вы используете режим распределенного решения (см. раздел «Распределенное решение и режим multitenancy» на стр. 76) и multitenancy, в таблице содержится информация о компонентах Endpoint Agent, подключенных к PCN и всем серверам SCN. В таблице могут отображаться следующие данные:

- **Хост** – имя хоста с компонентом Endpoint Agent.

  По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Новое правило запрета**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Серверы** – имена серверов, к которым подключен хост с компонентом Endpoint Agent.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Agent.
- **Версия** – версия установленного компонента Endpoint Agent.
- **Активность** – показатель активности компонента Endpoint Agent. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

По ссылке с IP-адресом компьютера, на который установлен компонент Endpoint Agent, вы также можете выбрать действие **Найти обнаружения**.

Просмотр информации о хосте

► *Чтобы просмотреть информацию о хосте с компонентом Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.
2. Выберите хост, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- **Состояние** – состояние хоста с компонентом Endpoint Agent.

  Хост может находиться в одном из следующих состояний:

  - **Онлайн**.
  - **Отключено**.
- **Хост** – имя хоста компьютера с компонентом Endpoint Agent.

  По ссылке с именем хоста вы можете выполнить действие **Скопировать значение в буфер**.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Agent.
- **ОС** – версия операционной системы, на компьютере, на который установлен компонент Endpoint Agent.
- **Защита** – состояние защиты хоста с компонентом Endpoint Agent.
- **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и multitenancy.
- **Имя сервера** – имя сервера Central Node.
- **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
- **Версия** – тип и версия установленного компонента Endpoint Agent.
- **Состояние** – состояние компонента Endpoint Agent.

Фильтрация и поиск хостов Endpoint Agent по имени хоста

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по имени хоста, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Agents**.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов имени хоста.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent, изолированных от сети

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent, изолированные от сети, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Установите флажок **Показывать только изолированные Endpoint Agents**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

kaspersky

Фильтрация и поиск хостов Endpoint Agent по именам серверов PCN и SCN

Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, вы можете отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN, к которым подключены эти хосты.

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по именам серверов PCN и SCN, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Серверы** откройте окно настройки фильтрации.
3. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с компонентом Endpoint Agent.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent по IP-адресу компьютера

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по IP-адресу компьютера, на котором установлен компонент Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **IP** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.

6. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent по версии операционной системы на компьютере

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии операционной системы, установленной на компьютере с компонентом Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **ОС** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов версии операционной системы.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent по версии Endpoint Agent

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Agent по версии*

компонента Endpoint Agent, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Версия** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов версии компонента Endpoint Agent.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов Endpoint Agent по их активности

► *Чтобы отфильтровать или найти компоненты Endpoint Agent по их активности, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. По ссылке **Активность** откройте окно настройки фильтрации.
3. Установите флажки рядом с одним или несколькими показателями активности компонента Endpoint Agent:
   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра хостов Endpoint Agent

► *Чтобы быстро создать фильтр хостов с компонентом Endpoint Agent, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением графы таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра хостов Endpoint Agent

► *Чтобы сбросить фильтр хостов с компонентом Endpoint Agent по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.
2. Нажмите на кнопку справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

kaspersky

Настройка показателей активности компонента Endpoint Agent

Пользователи с ролью **Локальный администратор** и **Администратор** могут определить, какой период бездействия компонентов Endpoint Agent считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности компонентов Endpoint Agent. Просматривать показатели активности Endpoint Agent могут все пользователи.

► *Чтобы настроить показатели активности компонентов Endpoint Agent, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью **Локальный администратор** или **Администратор**.
2. В окне веб интерфейса программы выберите раздел **Параметры**, подраздел **Endpoint Agents**.
3. В полях под названием раздела введите количество дней бездействия компьютеров с компонентом Endpoint Agent, которое вы хотите отображать как **Предупреждение** и **Критическое бездействие**.
4. Нажмите на кнопку **Применить**.

Пользователи с правами **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** смогут увидеть настроенные вами показатели активности компонентов Endpoint Agent в графе **Активность** таблицы хостов с компонентом Endpoint Agent в разделе **Endpoint Agents** окна веб-интерфейса программы.

Поддерживаемые интерпретаторы и процессы

Компонент Endpoint Sensors контролирует запуск скриптов следующими интерпретаторами:

- cmd.exe;
- reg.exe;
- regedit.exe;
- regedt32.exe;
- cscript.exe;
- wscript.exe;
- mmc.exe;
- msiexec.exe;
- mshta.exe;
- rundll32.exe;
- runlegacycplelevated.exe;
- control.exe;
- explorer.exe;
- regsvr32.exe;
- wwahost.exe;
- powershell.exe;
- java.exe и javaw.exe (только при запуске с опцией –jar);

- InstallUtil.exe;
- msdt.exe;
- python.exe;
- ruby.exe;
- rubyw.exe.

Информация о процессах, контролируемых компонентом Endpoint Sensor, представлена в таблице ниже.

Таблица 14. Процессы и расширения файлов, которые они открывают

Процесс	Расширения файлов
winword.exe	rtf doc dot docm docx dotx dotm docb
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm

Процесс	Расширения файлов
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

kaspersky

Сетевая изоляция хостов Endpoint Agent

Сетевая изоляция доступна для хостов с компонентом Endpoint Sensors версии 3.5 и 3.6 и с компонентом Endpoint Agent версии 3.7.

При включении правила сетевой изоляции на хосте прерываются все текущие соединения, а также становится недоступно VPN-подключение.

Программа блокирует соединение изолированных хостов с сервером Active Directory. Если параметры операционной системы требуют подключения к службам Active Directory для авторизации, то пользователь изолированного хоста не сможет войти в систему.

Если администратор программы заменяет сертификат сервера с компонентом Central Node при включенном правиле сетевой изоляции, то отключение правила становится недоступно.

Для корректной работы изолированного хоста рекомендуется выполнять следующие условия:

- Создать на хосте учетную запись локального администратора или сохранить данные доменной учетной записи в кеш перед включением правила сетевой изоляции.
- Не заменять сертификат и IP-адрес сервера с компонентом Central Node при включенном правиле сетевой изоляции.

Изолированным хостам доступны по сети следующие ресурсы:

- Сервер с компонентом Central Node.
- Источник обновлений баз программы (сервер обновлений "Лаборатории Касперского" или пользовательский источник).
- Серверы службы KSN.
- Хосты, добавленные в исключения правила сетевой изоляции.

Если соединение между изолированным хостом и сервером с компонентом Central Node отсутствует более 5 часов, правило сетевой изоляции автоматически отключается.

kaspersky

В этом разделе

Создание правила сетевой изоляции

► *Чтобы создать правило сетевой изоляции, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.
2. Выберите хост, для которого вы хотите включить или отключить правило сетевой изоляции.

   Откроется окно с информацией о хосте.
3. Нажмите на кнопку **Изолировать**.
4. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.
5. В блоке параметров **Исключения для правила изоляции хоста** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.
6. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.
7. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.
8. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия 5–7.
9. Нажмите на кнопку **Сохранить**.

Хост будет изолирован от сети.

Вы также можете создать правило сетевой изоляции по ссылке **Изолировать <имя хоста>** в информации о событии (см. раздел "Просмотр информации о событии" на стр. 262) и в информации об обнаружении (см. раздел "Просмотр информации об обнаружении" на стр. 235).

Добавление исключения из правила сетевой изоляции

► *Чтобы добавить исключение в ранее созданное правило сетевой изоляции, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выберите хост, изолированный от сети, для которого вы хотите создать исключение из правила сетевой изоляции.

   Откроется окно с информацией о хосте.

3. По ссылке **Добавить в исключения** раскройте блок параметров **Исключения для правила изоляции хоста**.
4. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.
5. Выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.
6. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.
7. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.
8. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия 5–7.
9. Нажмите на кнопку **Сохранить**.

Исключение из правила сетевой изоляции будет добавлено.

Удаление правила сетевой изоляции

► *Чтобы удалить правило сетевой изоляции, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Нажатием левой клавиши мыши по имени хоста, для которого вы хотите удалить правило сетевой изоляции, раскройте меню действий над этим хостом.
3. Выберите действие **Удалить правило изоляции хоста**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило сетевой изоляции хоста будет удалено.

kaspersky

Работа с задачами

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** могут работать с файлами и программами на хостах путем создания и удаления задач: **Завершить процесс**, **Выполнить программу**, **Получить файл**, **Удалить файл**, **Поместить файл на карантин**, **Восстановить файл из карантина**.

Задачи **Завершить процесс**, **Выполнить программу**, **Удалить файл**., **Поместить файл на карантин**, **Восстановить файл из карантина** могут быть одного из следующих типов:

- **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (если вы используете режим распределенного решения и multitenancy).
- **Глобальный** – созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).

Задача **Получить файл** выполняется только на указанном хосте независимо от режима работы с программой.

Пользователи с ролью **Старший сотрудник службы безопасности** могут работать со всеми задачами в рамках тех организаций, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Максимальное время выполнение задачи составляет 24 часа. Если за это время задача не успела завершиться, ее выполнение останавливается.

kaspersky

В этом разделе

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Задачи** окна веб-интерфейса программы. Вы можете просматривать все задачи или только задачи, созданные вами (текущим пользователем).

► *Чтобы включить отображение задач, созданных только текущим пользователем,*

включите переключатель **Только мои** в правом верхнем углу окна.

Отображение задач, созданных текущим пользователем, по умолчанию включено.

В таблице задач содержится следующая информация:

1. **Время создания** – дата и время создания задачи.
2. **Тип** – тип задачи по области распространения задачи.

   Задачи могут быть одного из следующих типов:

   - **Глобальный** – созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу

PCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).

- **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (если вы используете режим распределенного решения и multitenancy).

3. **Имя** – название задачи.

   Задача может быть иметь одно из следующих названий:

   - **Завершить процесс**.
   - **Выполнить программу**.
   - **Получить файл**.
   - **Удалить файл**.
   - **Поместить файл на карантин**.
   - **Восстановить файл из карантина**.

   По ссылке с названием типа задачи раскрывается список, в котором вы можете выбрать одно из следующих действий:

   - **Добавить в фильтр**.
   - **Исключить из фильтра**.
   - **Скопировать значение в буфер**.

4. **Сведения** – полный путь к файлу или потоку данных, для которого создана задача.

   По ссылке со сведениями о пути к файлу или потоку данных раскрывается список, в котором вы можете выбрать одно из следующих действий:

   - **Добавить в фильтр**.
   - **Исключить из фильтра**.
   - **Скопировать значение в буфер**.

5. **Серверы** – имя сервера с ролью PCN или SCN, на котором выполняется задача.

   Поле отображается только если вы используете режим распределенного решения и multitenancy.

6. **Хосты** – имя хоста, на котором выполняется задача.

   Поле отображается только если вы используете отдельный сервер Central Node.

7. **Автор** – имя пользователя, создавшего задачу.

   Если вы включили отображение задач, созданных только текущим пользователем, эта графа не будет отображаться.

8. **Состояние** – статус выполнения задачи.

   Задача может иметь один из следующих статусов:

   - **Ожидает**.

- **В обработке**.
- **Завершено**.

Просмотр информации о задаче

► *Чтобы просмотреть информацию о задаче, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Выберите задачу, информацию о которой вы хотите просмотреть.

Откроется окно с информацией о задаче.

Окно может содержать следующую информацию в зависимости от типа задачи:

- **Состояние** – статус выполнения задачи.
- **Описание** – описание задачи.
- **Путь к файлу** – путь к файлу или потоку данных.
- **SHA256** – SHA256-хеш файла, который вы хотите получить.
- **Команда** – команда запуска программы.
- **Запущено от имени** – параметр запуска программы: от имени текущего пользователя или от имени локальной системы.
- **Автор** – имя пользователя, создавшего задачу.
- **Организация** – название организации, отображается только когда вы используете режим распределенного решения и multitenancy.
- **Время создания** – время создания задачи.
- **Время завершения** – время завершения задачи.
- **Отчет** – результат выполнения задачи на выбранных хостах.

Создание задачи завершения процесса

Если вы считаете, что запущенный на компьютере процесс может угрожать безопасности компьютера или локальной сети организации, вы можете завершить его.

► *Чтобы создать задачу завершения процесса, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Завершить процесс**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу процесса, который вы хотите завершить.

Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будут завершены только процессы указанного потока данных. Процессы остальных потоков этого файла будут выполняться.

b. **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, который вы хотите завершить. Поле не является обязательным.

c. **Описание** – описание задачи. Поле не является обязательным.

d. Если вы хотите, чтобы пользователю компьютера, на котором выполняется задача, отображалось уведомление о запуске задачи, справа от названия параметра **Уведомление** установите флажок **Показать пользователю уведомление о выполнении задачи**.

e. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача завершения процесса.

Создание задачи выполнения программы

Вы можете выполнить задачу запуска программы или выполнения команды.

Если при выполнении задачи файл стандартного вывода или файл вывода ошибок достигает размера 100 КБ, часть данных из файла удаляется. Файл будет содержать не все данные.

► *Чтобы создать задачу запуска программы или выполнения команды, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Выполнить программу**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. В поле **Команда** введите команду выполнения программы.

   b. В поле **Описание** введите описание задачи. Поле не является обязательным.

   c. Если вы не хотите запускать программы от имени текущего пользователя и хотите запустить ее от имени другого пользователя установите флажок **Выполнить под учетной записью** в полях

Пользователь и **Пароль** введите учетные данные пользователя, от имени которого программа будет запущена.

По умолчанию флажок снят. Программа будет запущена от имени текущего пользователя.

d. Настройте параметр **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача запуска программы или выполнения команды.

Пример:

► *Чтобы полностью отключить сетевые интерфейсы хоста с помощью выполнения команды от имени текущего пользователя на всех хостах, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Выполнить программу**.

   Откроется окно создания задачи.
3. Задайте значения следующих параметров:

   a. В блоке параметров **Параметры** в поле **Команда** введите команду `netsh interface set interface <Имя интерфейса> admin=disable`.

   b. В поле **Описание** введите описание задачи.

   c. Выберите область применения задачи **Всех хостов**.
4. Нажмите на кнопку **Добавить**.

   Выполняйте задачу для отключения каждого сетевого интерфейса.

   Сетевой интерфейс, соединяющий хост с компонентом Central Node, отключайте в последнюю очередь.

После успешного выполнения задачи сетевые интерфейсы хоста будут отключены.

kaspersky

Создание задачи получения файла

► *Чтобы создать задачу получения файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Получить файл**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите получить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае вы получите только указанный поток.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите получить. Поле не является обязательным.

      При указании этого параметра может быть получено более одного файла.

   c. Если вы хотите отказаться от проверки файла, снимите флажок **Отправить на проверку**.

      По умолчанию флажок установлен.

   d. **Описание** – описание задачи. Поле не является обязательным.

   e. **Хост** – имя хоста или IP-адрес сервера, с которого вы хотите получить файл.

4. Нажмите на кнопку **Добавить**.

Будет создана задача получения файла. Файл, полученный в результате выполнения задачи, будет помещен в Хранилище.

Если задача получения файла завершилась успешно, вы можете скачать полученный файл на ваш локальный компьютер.

► *Чтобы скачать полученный файл на локальный компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу получения файла, который вы хотите скачать.

3. В нижней части окна **Получить файл** нажмите на имя хоста или IP-адрес.

   Откроется окно с информацией о файле.

4. Нажмите на кнопку **Скачать**.

Файл будет сохранен на ваш локальный компьютер в папку загрузки браузера.

Создание задачи удаления файла

► *Чтобы создать задачу удаления файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Удалить файл**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите удалить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будет удален только указанный поток данных. Остальные потоки данных этого файла останутся без изменений.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите удалить. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

   d. Если вы хотите, чтобы пользователю компьютера, на котором выполняется задача, отображалось уведомление о запуске задачи, справа от названия параметра **Уведомление** установите флажок **Показать пользователю уведомление о выполнении задачи**.

   e. **Задача для** – область применения задачи:

      - Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
      - Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

        Этот вариант доступен только при включенном режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy.

      - Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача удаления файла.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки хоста. Рекомендуется проверить успешность удаления файла после перезагрузки хоста.
Удаление файла с подключенного сетевого диска не поддерживается.

Создание задачи помещения файла на карантин

Если вы считаете, что на компьютере с компонентом Endpoint Agent находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив на карантин. Файл будет удален из папки компьютера, в которой он находится, и перемещен на карантин Endpoint Agent в директорию карантина на

этом компьютере, указанную при настройке Endpoint Agent.

► *Чтобы создать задачу помещения файла на карантин, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Поместить файл на карантин**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. В поле **Путь к файлу** введите путь к файлу, который вы хотите поместить на карантин.

   b. В поле **MD5/SHA256** введите MD5- или SHA256-хеш файла, который вы хотите поместить на карантин. Поле не является обязательным.

   c. В поле **Описание** введите описание задачи. Поле не является обязательным.

   d. Если вы не хотите запускать программы от имени текущего пользователя и хотите запустить ее от имени другого пользователя установите флажок **Выполнить под учетной записью**. в полях **Пользователь** и **Пароль** введите учетные данные пользователя, от имени которого программа будет запущена.

      По умолчанию флажок снят. Программа будет запущена от имени текущего пользователя.

   e. В поле **Хосты** введите символы поиска имени хоста, файл на котором вы хотите поместить на карантин, и выберите имя хоста из списка. Повторите действия для каждого добавляемого хоста.

      Выбранные хосты добавятся в список.

4. Нажмите на кнопку **Добавить**.

   Будет создана задача помещения файла на карантин. В результате выполнения задачи:

   - Файл будет удален из папки компьютера с компонентом Endpoint Agent, в которой он находился, и перемещен на карантин Endpoint Agent в директорию карантина на этом компьютере, указанную при настройке Endpoint Agent.
   - В списке задач раздела **Задачи** веб-интерфейса программы появится информация о выполнении этой задачи.
   - В списке файлов раздела **Хранилище** подраздела **Карантин** появится информация о помещении файла на карантин.

> Если файл заблокирован другим процессом, то задача будет отображаться со статусом Выполнено, но сам файл будет помещен на карантин только после перезагрузки хоста. Рекомендуется проверить успешность выполнения задачи после перезагрузки хоста.

Создание задачи восстановления файла из Карантина

Если вы считаете, что изолированный ранее файл безопасен, вы можете восстановить его из Карантина на хост.

► *Чтобы создать задачу восстановления файла из Карантина, выполните следующие*

действия:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Восстановить файл из карантина**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Описание** – описание задачи. Поле не является обязательным.

   b. Если вы хотите, чтобы пользователю компьютера, на котором выполняется задача, отображалось уведомление о запуске задачи, справа от названия параметра **Уведомление** установите флажок **Показать пользователю уведомление о выполнении задачи**.

   c. **Поиск файлов** – имя файла, находящегося в Карантине.

4. Нажмите на кнопку **Добавить**.

Будет создана задача восстановления файла из Карантина.

После восстановления файла из Карантина на хост метаданные о файле останутся в таблице объектов, помещенных в Хранилище.

Создание копии задачи

► *Чтобы скопировать задачу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу, которую вы хотите скопировать.

3. Нажмите на кнопку **Скопировать**.

   Откроется окно создания задачи. Все параметры задачи будут скопированы.

4. Нажмите на кнопку **Добавить**.

Будет создана копия выбранной задачи.

Удаление задачи

Если вы удалите задачу в процессе ее выполнения, результат выполнения задачи может не сохраниться.
Если вы удалите успешно выполненную задачу скачивания файла, файл будет удален.

► *Чтобы удалить задачу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу, которую вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Задача будет удалена.

Фильтрация задач по времени создания

► *Чтобы отфильтровать задачи по времени их создания, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Время создания** откройте меню фильтрации задач.
3. Выберите один из следующих периодов отображения задач:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все созданные задачи.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за указанный вами период.
4. Если вы выбрали период отображения задач **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения задач.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по типу

Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, вы можете отфильтровать задачи по их типу.

► *Чтобы отфильтровать задачи по их типу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Тип** откройте меню фильтрации задач.
3. Выберите один из следующих вариантов отображения задач:
   - **Все**, если вы хотите, чтобы отображались все задачи независимо от типа.
   - **Глобальный**, если вы хотите, чтобы отображались только задачи, созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).
   - **Локальный**, если вы хотите, чтобы отображались только задачи, созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (если вы используете режим распределенного решения и multitenancy)..

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени

► *Чтобы отфильтровать задачи по имени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Имя** откройте меню фильтрации задач.
3. Установите один или несколько флажков:
   - **Получить файл**.
   - **Завершить процесс**.
   - **Удалить файл**.
   - **Поместить файл на карантин**.
   - **Восстановить файл**.
   - **Выполнить программу**.
4. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

kaspersky

Фильтрация задач по имени и пути к файлу

Вы можете фильтровать задачи по показателю **Сведения** – имя и путь к файлу или потоку данных.

► *Чтобы отфильтровать задачи по имени и пути к файлу или потоку данных, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Сведения** откройте окно настройки фильтрации задач.
3. В правом раскрывающемся списке выберите **Сведения**.
4. В левом раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
5. В поле ввода укажите один или несколько символов имени или пути к файлу.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по описанию

Вы можете фильтровать задачи по показателю **Описание** – описание задачи, которое было добавлено на этапе создания задачи.

► *Чтобы отфильтровать задачи по описанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Сведения** откройте окно настройки фильтрации задач.
3. В левом раскрывающемся списке выберите **Описание**.
4. В правом раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.

- **Равняется**.
- **Не равняется**.

5. В поле ввода укажите один или несколько символов имени или пути к файлу.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени сервера

Если вы используете режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, вы можете отфильтровать задачи по серверам, на которые распространяется действие задач.

► *Чтобы отфильтровать задачи по серверам, на которые распространяется действие задач, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Серверы** откройте меню фильтрации задач.
3. Установите флажки рядом с именами тех серверов, задачи по которым вы хотите отобразить.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени пользователя, создавшего задачу

Фильтрация задач по имени пользователя, создавшего задачу, доступна только при отображении всех задач. Если вы включили отображение задач, созданных только текущим пользователем, фильтрация задач по имени пользователя недоступна.

► *Чтобы отфильтровать задачи по имени пользователя, создавшего задачу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Автор** откройте меню фильтрации задач.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по состоянию обработки

► *Чтобы отфильтровать задачи по состоянию их обработки пользователем, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Состояние** откройте меню фильтрации задач.
3. Установите один или несколько флажков:
   - **Ожидает**.
   - **В обработке**.
   - **Завершено**.
4. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра задач

► *Чтобы сбросить фильтр задач по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

Откроется таблица задач.

2. Нажмите на кнопку справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

kaspersky

Работа с политиками (правилами запрета)

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** могут управлять правилами запрета запуска файлов и процессов на выбранных хостах с помощью политик. Например, вы можете запретить запуск программ, использование которых считаете небезопасным, на выбранном хосте с компонентом Endpoint Agent. Программа идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Вы можете создавать, удалять и изменять запреты.

Правила запрета могут быть следующих типов:

- **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (если вы используете режим распределенного решения и multitenancy).
- **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, редактировать, удалять, включать и отключать правила запрета в рамках тех организаций, к данным которых у них есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета.

Все изменения в правилах запрета применяются на хостах после установки авторизованного соединения с выбранными хостами. Если соединение с хостами отсутствует, на хостах продолжают действовать старые правила запрета. Изменения в правилах запрета не влияют на уже запущенные процессы.

Если попытка запуска файла будет совершена до запуска компонента Endpoint Agent или после завершения работы компонента Endpoint Agent на хосте, то запуск файла будет заблокирован. На компьютере пользователя отобразится уведомление о запрете запуска файла, когда компонент Endpoint Agent будет запущен.

На каждый хеш файла можно создать только одно правило запрета.

kaspersky

В этом разделе

Просмотр таблицы правил запрета

Таблица правил запрета находится в разделе **Политики** окна веб-интерфейса программы.

В таблице содержится следующая информация:

1. **Тип** – тип правила запрета. Правила запрета могут быть следующих типов:
   - **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).
   - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (если вы используете режим распределенного решения и multitenancy).
2. **Имя** – имя правила запрета.
3. **Серверы** – имена серверов с ролью PCN или SCN, на которые распространяется правило запрета (если вы используете режим распределенного решения и multitenancy).

   Поле отображается только когда вы используете режим распределенного решения и multitenancy.
4. **Хосты** – имя сервера с компонентом Central Node, на хосты которого распространяется правило запрета.

   Поле отображается только когда вы используете отдельный сервер Central Node.
5. **Хеш файла** – алгоритм хеширования, применяющийся для идентификации файла.

   Идентификация файла может осуществляться по одному из следующих алгоритмов хеширования:
   - **MD5**.
   - **SHA256**.

По ссылке с названием алгоритма хеширования раскрывается список, в котором вы можете посмотреть хеш файла, а также выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Найти на KL TIP**.
- **Найти события**.

  В результате выполнения этого действия откроется раздел **Поиск угроз** с событиями, уже отфильтрованными по выбранному вами хешу.
- **Найти обнаружения**.

  В результате выполнения этого действия откроется раздел **Обнаружения** с обнаружениями, уже отфильтрованными по выбранному вами хешу.
- **Включить правило запрета**.
- **Отключить правило запрета**.
- **Удалить правило запрета**.
- **Скопировать значение в буфер**.

6. **Состояние** – текущее состояние правила запрета.

   Правило запрета может находиться в одном из следующих состояний:

   - **Включено**.
   - **Отключено**.

Просмотр правила запрета

► *Чтобы просмотреть правило запрета, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Выберите правило запрета, которое вы хотите просмотреть.

Правило запрета содержит следующую информацию:

- **События** – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранное вами правило запрета.
- **Состояние** – текущее состояние правила запрета.

  Правило запрета может находиться в одном из следующих состояний:

  - **Включено**.
  - **Отключено**.
- Закладка **Сведения** со следующей информацией:
  - **MD5/SHA256** – хеш файла, запрещенного к запуску.
  - **Имя** – имя правила запрета или файла, запрещенного к запуску.

- **Тип** – тип правила запрета. Правила запрета могут быть одного из следующих типов:
  - **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).
  - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (если вы используете режим распределенного решения и multitenancy).
- **Уведомление** – состояние параметра **Показать пользователю уведомление о выполнении задачи**.
- **Запрет для** – список хостов, на которые распространяется правило запрета.

  Если запрет действует на всех хостах, отображается надпись **Всех хостов**.

- Закладка **Журнал изменений** содержит список изменений запрета: время изменения, имя пользователя, изменившего запрет, и действия над запретом.

Создание правила запрета

► *Чтобы создать правило запрета, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку **Добавить**.

   Откроется окно создания правила запрета.

3. Задайте значения следующих параметров:
   a. **Состояние** – состояние правила запрета:
      - Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
      - Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.
   b. **MD5/SHA256** – MD5- или SHA256-хеш файла или потока данных, запуск которого вы хотите запретить.
   c. **Имя** – имя правила запрета.
   d. Если вы хотите, чтобы программа выводила уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показать пользователю уведомление о выполнении задачи**.
   e. **Запрет для** – область применения правила запрета:
      - Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.
      - Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

Этот вариант доступен только при включенном режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy.

- Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создан запрет на запуск файла.

Если вы установили флажок **Показать пользователю уведомление о выполнении задачи**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.

Включение и отключение запрета

► *Чтобы включить или отключить правило запрета, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. В строке с правилом запрета, которое вы хотите включить или отключить, в графе **Состояние** выполните одно из следующих действий:

   - Если вы хотите включить правило запрета, переведите переключатель в положение **Включено**.

     Выбранное вами правило запрета будет включено.

   - Если вы хотите отключить правило запрета, переведите переключатель в положение **Отключено**.

     Выбранное вами правило запрета будет отключено.

Удаление правила запрета

► *Чтобы удалить правило запрета, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на правило запрета, которое вы хотите удалить.

   Откроется окно сведений о правиле запрета.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило запрета будет удалено.

Фильтрация правил запрета по имени

► *Чтобы отфильтровать правила запрета по имени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Имя** откройте меню фильтрации запретов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени правила запрета.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по типу

Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, вы можете отфильтровать правила запрета по их типу.

► *Чтобы отфильтровать правила запрета по типу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Тип** откройте меню фильтрации правил запрета.
3. Выберите один из следующих вариантов отображения правил запрета:
   - **Все**, если вы хотите, чтобы отображались все правила запрета независимо от типа.
   - **Глобальный**, если вы хотите, чтобы отображались только правила запрета, созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).
   - **Локальный**, если вы хотите, чтобы отображались только правила запрета, созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (если вы используете режим распределенного решения

и multitenancy).

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по хешу файла

► *Чтобы отфильтровать правила запрета по хешу файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Хеш файла** откройте меню фильтрации правил запрета.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов хеша файла.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по имени сервера

Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, вы можете отфильтровать правила запрета по серверам, на которые распространяется действие правил запрета.

► *Чтобы отфильтровать правила запрета по имени сервера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Серверы** откройте меню фильтрации правил запрета.

3. Установите флажки напротив тех серверов, по которым вы хотите отфильтровать правила запрета.
4. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил запрета

► *Чтобы сбросить фильтр правил запрета по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку ⊠ справа от того заголовка графы таблицы правил запрета, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Работа с пользовательскими правилами

Пользователи с ролью Сотрудник службы безопасности и Старший сотрудник службы безопасности могут работать с пользовательскими правилами **TAA**, **IOC** и **YARA**: загружать и удалять файлы правил, просматривать таблицы загруженных правил в разделе **Правила пользователей**, а также работать с правилами **TAA**, добавленными в исключения, в разделе **Параметры**, подразделе **Белые списки** веб-интерфейса программы.

kaspersky

Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз

Kaspersky Endpoint Detection and Response использует для поиска угроз два типа индикаторов – *IOC* (Indicator of Compromise, или индикатор компрометации) и *IOA* (Indicator of Attack, или индикатор атаки).

Индикатор IOC – это набор данных о вредоносном объекте или действии.Kaspersky Endpoint Detection and Response использует IOC-файлы открытого стандарта описания индикаторов компрометации OpenIOC. IOC-файлы содержат набор индикаторов, при совпадении с которыми программа считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

Индикатор IOA – это правило (далее также "правило TAA (IOA)"), содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки.Kaspersky Endpoint Detection and Response проверяет базу событий (см. раздел "Поиск угроз по базе событий" на стр. 251) программы и отмечает события, которые совпадают с поведением, описанным в правилах TAA (IOA). При проверке используется технология *потокового сканирования*, при которой объекты, загружаемые из сети, проверяются непрерывно в режиме реального времени.

Правила TAA (IOA), сформированные специалистами "Лаборатории Касперского", используются в работе технологии TAA (Targeted Attack Analyzer) и обновляются вместе с базами программы. Они не отображаются в интерфейсе программы и не могут быть отредактированы.

Вы можете добавлять пользовательские правила TAA (IOA) (см. раздел "Импорт пользовательского правила TAA (IOA)" на стр. 331) в виде IOC-файлов открытого стандарта описания OpenIOC, а также создавать правила TAA (IOA) на основе условий поиска по базе событий (см. раздел "Создание пользовательского правила TAA (IOA) на основе условий поиска событий" на стр. 257).

Сравнительные характеристики индикаторов компрометации (IOC) и атаки (IOA) приведены в таблице ниже.

Таблица 15. Сравнительные характеристики индикаторов IOC и IOA

Сравнительная характеристика	Индикаторы IOC в пользовательских правилах IOC	Индикаторы IOA в пользовательских правилах TAA (IOA)	Индикаторы IOA в правилах TAA (IOA), сформированных специалистами "Лаборатории Касперского"
Область проверки	Компьютеры с компонентом Endpoint Agent	Компьютеры с компонентом Endpoint Agent	База событий программы
Механизм проверки	Периодическое сканирование	Периодическое сканирование	Потоковое сканирование
Предустановленные индикаторы от специалистов "Лаборатории Касперского"	Нет	Нет	Есть
Возможность добавить в исключения из проверки	Нет		Есть

Если вы используете режим распределенного решения и multitenancy, в разделе отображаются данные по выбранной вами организации (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213).

kaspersky

Работа с пользовательскими правилами TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать (см. раздел "Создание пользовательского правила TAA (IOA) на основе условий поиска событий" на стр. 257), импортировать (см. раздел "Импорт пользовательского правила TAA (IOA)" на стр. 331), удалять (см. раздел "Удаление пользовательских правил TAA (IOA)" на стр. 333), включать и отключать (см. раздел "Включение и отключение использования правил TAA (IOA)" на стр. 332) правила TAA (IOA), а также добавлять правила TAA (IOA) "Лаборатории Касперского" в исключения из проверки (см. раздел "Добавление правила TAA (IOA) в исключения" на стр. 386). Пользователи с ролями **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** могут использовать правила TAA (IOA) для поиска признаков целевых атак (см. раздел "Поиск обнаружений и событий, в которых сработали правила TAA (IOA)" на стр. 329), зараженных и возможно зараженных объектов в базе событий и обнаружений, а также просматривать таблицу правил TAA (IOA) (см. раздел "Просмотр таблицы правил TAA (IOA)" на стр. 327) и информацию о правилах TAA (IOA) (см. раздел "Просмотр информации о пользовательском правиле TAA (IOA)" на стр. 327).

Различия между пользовательскими правилами и правилами "Лаборатории Касперского" представлены в таблице ниже.

Таблица 16. Сравнительные характеристики правил TAA (IOA)

Сравнительная характеристика	Пользовательские правила TAA (IOA)	Правила TAA (IOA) "Лаборатории Касперского"
Наличие рекомендаций по реагированию на событие	Нет	Есть Вы можете посмотреть рекомендации в информации об обнаружении (см. раздел "Информация в блоке Результаты проверки" на стр. 237)
Соответствие технике в базе MITRE ATT&CK	Нет	Есть Вы можете посмотреть описание техники по классификации MITRE в информации об обнаружении (см. раздел "Информация в блоке Результаты проверки" на стр. 237)
Отображение в таблице IOA-правил (см. раздел "Просмотр таблицы правил TAA (IOA)" на стр. 327)	Да	Нет
Способ отключить проверку базы по этому правилу	Отключить правило (см. раздел "Включение и отключение использования правил TAA (IOA)" на стр. 332)	Добавить правило в белый список (см. раздел "Добавление правила TAA (IOA) в исключения" на стр. 386)

Сравнительная характеристика	Пользовательские правила ТАА (IOA)	Правила ТАА (IOA) "Лаборатории Касперского"
Возможность удалить или добавить правило	Вы можете удалить (см. раздел "Удаление пользовательских правил ТАА (IOA)" на стр. 333) или добавить правило (см. раздел "Создание пользовательского правила ТАА (IOA) на основе условий поиска событий" на стр. 257) в веб-интерфейсе программы	Правила обновляются вместе с базами программы и не могут быть удалены пользователем
Поиск обнаружений и событий, в которых сработали правила ТАА (IOA) (на стр. 329)	По ссылкам **Обнаружения** и **События** в окне с информацией о правиле ТАА (IOA) (см. раздел "Просмотр информации о пользовательском правиле ТАА (IOA)" на стр. 327)	По ссылкам **Обнаружения** и **События** в окне с информацией об обнаружении (см. раздел "Просмотр информации об обнаружении" на стр. 235)

В зависимости от режима работы программы и сервера, на котором создаются правила ТАА (IOA), пользовательские правила ТАА (IOA) могут быть одного из следующих типов:

- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (в режиме распределенного решения и multitenancy).
- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (в режиме распределенного решения и multitenancy).

В этом разделе

Просмотр таблицы правил TAA (IOA)

Таблица пользовательских правил TAA (IOA) содержит информацию о правилах TAA (IOA), используемых для проверки событий и создания обнаружений, и находится в разделе **Правила пользователей**, подразделе **TAA** окна веб-интерфейса программы.

В таблице содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого правила TAA (IOA).

   Степень важности может иметь одно из следующих значений:

   - – **Низкая**.
   - – **Средняя**.
   - – **Высокая**.

2. **Тип** – тип правила в зависимости от роли сервера, на котором оно создано, в режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76):

   - **Глобальный** – правило создано на сервере PCN.
   - **Локальный** – правило создано на сервере SCN.

3. **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:

   - **Высокая**.
   - **Средняя**.
   - **Низкая**.

   Чем выше надежность, тем меньше вероятность ложных срабатываний

4. **Имя** – название правила.
5. **Серверы** – имя сервера с компонентом Central Node, на котором применяется правило.
6. **Обнаружения** – требование сохранять информацию об обнаружении на основе совпадения события из базы с критериями правила.

   - **Включено** – для события создается запись в таблице обнаружений с указанием технологии Targeted Attack Analyzer (TAA).
   - **Отключено** – не отображается в таблице обнаружений.

7. **Состояние** – состояние использования правила при проверке событий:

   - **Включено** – правило используется.
   - **Отключено** – правило не используется.

Просмотр информации о пользовательском правиле TAA (IOA)

► *Чтобы просмотреть информацию о правиле TAA (IOA), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Обнаружения**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по графе **Технологии** (см. раздел "**Фильтрация и поиск обнаружений по названию технологии**" на стр. 230) и графе **Сведения** (см. раздел "**Фильтрация и поиск обнаружений по полученной информации**" на стр. 227) - технологии Targeted Attack Analyzer и имени правила TAA (IOA), с которым вы работаете.
- **Найти события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз** (см. раздел "**Просмотр таблицы событий**" на стр. 260), отфильтрованных по имени правила.
- **Выполнить запрос**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз** (см. раздел "**Просмотр таблицы событий**" на стр. 260), отфильтрованных по имени правила. В условиях поиска событий указаны данные из правила TAA (IOA), с которым вы работаете. Например, `EventType=Запущен процесс AND FileName CONTAINS <имя правила, с которым вы работаете>`. Вы можете отредактировать запрос на поиск событий (см. раздел "Поиск угроз по базе событий" на стр. 251).
- **IOA ID**. По ссылке открывается идентификатор, присваиваемый программой каждому правилу.

  Изменение идентификатора недоступно. Вы можете скопировать идентификатор по кнопке **Скопировать значение в буфер**.
- **Состояние** – использование правила при проверке базы событий.

На закладке **Сведения** отображается следующая информация:

- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Описание** – любая дополнительная информация о правиле, которую вы указали.
- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, указанная пользователем при добавлении правила.
- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, заданный пользователем при добавлении правила.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (в режиме распределенного решения и multitenancy).
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (в режиме распределенного решения и multitenancy).
- **Область применения** – имена серверов с компонентом Central Node, на которых применяется правило.

На закладке **Запрос** отображается исходный код запроса, по которому осуществляется проверка. По ссылке **Выполнить запрос** в верхней части окна вы можете перейти в раздел **Поиск угроз** и выполнить запрос на поиск событий.

Поиск обнаружений и событий, в которых сработали правила TAA (IOA)

► *Чтобы найти и просмотреть обнаружения и события, при создании которых сработало пользовательское правило TAA (IOA), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, результат срабатывания которого вы хотите просмотреть.

   Откроется окно с информацией о правиле.

3. Выполните одно из следующих действий:

   - Если вы хотите просмотреть обнаружения, при создании которых сработало правило TAA (IOA), по ссылке **Обнаружения** перейдите в базу обнаружений.

     Откроется новая закладка браузера с таблицей найденных обнаружений.

   - Если вы хотите просмотреть события, при создании которых сработало правило TAA (IOA), по ссылке **События** перейдите в базу событий.

     Откроется новая закладка браузера с таблицей найденных событий.

► *Чтобы найти и просмотреть обнаружения и события, при создании которых сработало правило TAA (IOA) "Лаборатории Касперского", выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке в графе **Технологии** откройте окно настройки фильтрации.
3. В левом раскрывающемся списке выберите **Содержит**.
4. В правом раскрывающемся списке выберите технологию **(TAA) Targeted Attack Analyzer**.
5. Нажмите на кнопку **Применить**.

   В таблице отобразятся обнаружения, выполненные технологией TAA на основе правил TAA (IOA).

6. Выберите обнаружение, для которого в графе **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об обнаружении.

7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.
8. Выполните одно из следующих действий:

   - Если вы хотите просмотреть обнаружения, при создании которых сработало правило TAA (IOA), по ссылке **Обнаружения** перейдите в базу обнаружений.

     Откроется новая закладка браузера с таблицей найденных обнаружений.

   - Если вы хотите просмотреть события, при создании которых сработало правило TAA (IOA), по ссылке **События** перейдите в базу событий.

     Откроется новая закладка браузера с таблицей найденных событий.

Фильтрация и поиск правил TAA (IOA)

► *Чтобы отфильтровать или найти правила TAA (IOA) по требуемым критериям, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Выполните следующие действия в зависимости от критерия фильтрации:
   - **По степени важности**
   - **По типу правила**
   - **По уровню надежности**
   - **По имени правила**
   - **По имени сервера**
   - **По созданию обнаружений на основе правила**
   - **По состоянию правила**

   В таблице отобразятся только правила, соответствующие заданным условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил TAA (IOA)

► *Чтобы сбросить фильтр правил TAA (IOA) по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Нажмите на кнопку ⊠ справа от того заголовка графы таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

   Выбранные фильтры будут сброшены.

   В таблице отобразятся только правила, соответствующие заданным условиям.

Создание пользовательского правила TAA (IOA) на основе условий поиска событий

► *Чтобы создать пользовательское правило TAA (IOA) на основе условий поиска событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

Откроется форма поиска событий.

2. Выполните поиск событий с помощью режима конструктора или режима исходного кода.
3. Нажмите на кнопку **Сохранить как правило TAA (IOA)**.

   Откроется окно **Сохранить**.
4. В поле **Имя** введите имя правила.
5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В таблице правил TAA (IOA) раздела **Правила пользователей**, подразделе **TAA** веб-интерфейса отобразится новое правило с заданным именем.

Не рекомендуется в условиях поиска событий, сохраняемых как пользовательское правило TAA (IOA), использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

На момент сохранения пользовательского правила TAA (IOA) в программе может не быть событий, содержащих данные для этих полей. Когда события с этими данными появятся, пользовательское правило TAA (IOA), созданное ранее, не сможет разметить события по этим полям.

Импорт пользовательского правила TAA (IOA)

Вы можете импортировать файл формата IOC и использовать его для проверки событий и создания обнаружений Targeted Attack Analyzer.

Настоятельно рекомендуется проверить работу пользовательских правил в тестовой среде перед импортом. Пользовательские правила TAA (IOA) могут вызвать проблемы производительности, в случае которых стабильная работа программы не гарантируется

► *Чтобы импортировать правило TAA (IOA), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файла на вашем локальном компьютере.
3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

   Откроется окно **Новое правило TAA (IOA)**.
4. Включите или выключите переключатель **Состояние**, если вы хотите изменить состояние использования правила при проверке базы событий.
5. На закладке **Сведения** В поле **Имя** введите имя правила.
6. В поле **Описание** введите любую дополнительную информацию о правиле.

7. В раскрывающемся списке **Важность** выберите степень важности, которая будет присвоена обнаружению, выполненному по этому правилу TAA (IOA):
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.
8. В раскрывающемся списке **Надежность** выберите уровень надежности этого правила, по вашей оценке:
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.
9. В блоке параметров **Область применения** установите флажки напротив тех серверов, на которых вы хотите применить правило.
10. На закладке **Запрос** проверьте заданные условия поиска. Если требуется, внесите изменения.
11. Нажмите на кнопку **Сохранить**.

Пользовательское правило TAA (IOA) будет импортировано в программу.

Вы также можете добавить правило TAA (IOA), сохранив условия поиска по базе событий в разделе **Поиск угроз**.

Включение и отключение использования правил TAA (IOA)

Вы можете включить или отключить использование одного или нескольких правил, а также всех правил сразу.

► *Чтобы включить или отключить использование правила TAA (IOA) при проверке событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. В строке с нужным правилом в графе **Состояние** включите или выключите переключатель.

Использование правила при проверке событий будет включено или отключено.

► *Чтобы включить или отключить использование всех или нескольких правил TAA (IOA) при проверке событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).
2. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками граф.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование всех правил.

Использование выбранных правил при проверке событий будет включено или отключено.

Эти изменения не влияют на работу правил TAA (IOA) "Лаборатории Касперского". Если вы не хотите использовать при проверке правило TAA (IOA) "Лаборатории Касперского", вам требуется добавить его в исключения (см. раздел "Добавление правила TAA (IOA) в исключения" на стр. 386).

Изменение пользовательского правила TAA (IOA)

Вы можете изменять только пользовательские правила TAA (IOA). Изменение правил "Лаборатории Касперского" недоступно.

При работе в режиме распределенного решения и multitenancy вы можете изменять только те правила TAA (IOA), которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно изменение только правил, созданных на PCN. В веб-интерфейсе SCN доступно изменение только правил, созданных на SCN.

► *Чтобы изменить IOA-правило, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, которое вы хотите изменить.

   Откроется окно с информацией об этом правиле.

3. Внесите необходимые изменения.
4. Нажмите на кнопку **Сохранить**.

Параметры правила будут изменены.

Удаление пользовательских правил TAA (IOA)

Вы можете удалить одно или несколько пользовательских правил TAA (IOA), а также все правила сразу.

При работе в режиме распределенного решения вы можете удалять только те правила TAA (IOA), которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно удаление только правил, созданных на PCN. В веб-интерфейсе SCN доступно удаление только правил, созданных на SCN.

► *Чтобы удалить пользовательское правило TAA (IOA), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **TAA**.

Откроется таблица правил ТАА (IOA).

2. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией об этом правиле.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило будет удалено.

► *Чтобы удалить все или несколько пользовательских правил ТАА (IOA), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **ТАА**.

   Откроется таблица правил ТАА (IOA).

2. Установите флажки слева от правил, которые вы хотите удалить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками граф.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Вы не можете удалять правила ТАА (IOA) "Лаборатории Касперского". Если вы не хотите использовать при проверке правило ТАА (IOA) "Лаборатории Касперского", вам требуется добавить его в исключения (см. раздел "Добавление правила ТАА (IOA) в исключения" на стр. 386).

kaspersky

Работа с пользовательскими правилами IOC

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут использовать IOC-файлы для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и обнаружений, а также для проверки компьютеров с установленным компонентом Endpoint Agent.

В зависимости от режима работы программы и сервера, на который загружаются IOC-файлы, загруженные IOC-файлы могут быть одного из следующих типов:

- **Локальный** – загруженные на сервер SCN. По этим IOC-файлам производится проверка событий на этом сервере SCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (в режиме распределенного решения и multitenancy).
- **Глобальный** – загруженные на сервер PCN. По этим IOC-файлам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (в режиме распределенного решения и multitenancy).

Пользователи с ролью **Старший сотрудник службы безопасности** могут управлять проверкой событий по IOC-файлам: добавлять, изменять, удалять и скачивать IOC-файлы на компьютер, включать и отключать проверку событий по IOC-файлам, а также управлять параметрами проверки объектов.

Пользователи с ролью **Сотрудник службы безопасности** могут только просматривать информацию об IOC-файлах и скачивать IOC-файлы на компьютер.

Если вы работаете с событиями, уже обнаруженными программой ранее, повторное совпадение данных этих событий с индикаторами компрометации не всегда свидетельствует о возможном обнаружении.

kaspersky

В этом разделе

Просмотр таблицы IOC-файлов

Таблица IOC-файлов содержит информацию об IOC-файлах, используемых для проверки на компьютерах с компонентом Endpoint Agent, и находится в разделе **Правила пользователей**, подразделе **IOC** окна веб-интерфейса программы.

В таблице IOC-файлов содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

   Степень важности может иметь одно из следующих значений:

   - – низкая важность.
   - – средняя важность.
   - – высокая важность.

2. **Тип** – тип загруженного IOC-файла в зависимости от режима работы программы и сервера, на который загружен IOC-файл. IOC-файлы могут быть одного из следующих типов:

   - **Глобальный** – загруженные на сервер PCN. По этим IOC-файлам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (в режиме распределенного решения и multitenancy).
   - **Локальный** –загруженные на сервер SCN. По этим IOC-файлам производится проверка событий на этом сервере SCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (см. раздел "Выбор организации для работы в веб-интерфейсе программы" на стр. 213) (в режиме распределенного решения и multitenancy).

3. **Имя** – имя IOC-файла.
4. **Серверы** – имя сервера с компонентом Central Node, на котором производится проверка событий по

этому IOC-файлу.

5. **Автоматическая проверка** – использование IOC-файла при автоматической проверке событий.

   Проверка событий с использованием этого IOC-файла может находиться в одном из следующих состояний:

   - **Включено**.
   - **Отключено**.

Просмотр информации об IOC-файле

► *Чтобы просмотреть информацию об IOC-файле, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об IOC-файле.

Окно содержит следующую информацию:

- **Найти обнаружения**. По ссылке открывается раздел **Обнаружения** с условием фильтрации, содержащим выбранный вами IOC-файл.
- **Найти события**. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный вами IOC-файл.
- **Скачать**. По ссылке открывается окно скачивания IOC-файла.
- **Автоматическая проверка** – использование IOC-файла при автоматической проверке событий.

  Проверка событий с использованием этого IOC-файла может находиться в одном из следующих состояний:

  - **Включено**.
  - **Отключено**.
- **Имя** – имя IOC-файла.
- **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

  Степень важности может иметь одно из следующих значений:

  - – низкая важность.
  - – средняя важность.
  -  – высокая важность.
- **Область применения**. Отображает название организации и имена серверов, к которым относятся события, проверяемые по этому IOC-файлу (в режиме распределенного решения и multitenancy).
- **XML**. Отображает содержимое IOC-файла в формате XML.

Загрузка IOC-файла

IOC-файлы со свойствами UserItem для доменных пользователей не поддерживаются.

► *Чтобы загрузить IOC-файл, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла на вашем локальном компьютере.
3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.
4. Укажите следующие параметры:
   a. **Автоматическая проверка** – использование IOC-файла при автоматической проверке событий:
      - **Включено**.
      - **Отключено**.
   b. **Имя** – имя IOC-файла.
   c. **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла:
      - **Низкая**.
      - **Средняя**.
      - **Высокая**.
   d. **Область применения** – название организации и имена серверов, на которых вы хотите проверять события по этому IOC-файлу (в режиме распределенного решения и multitenancy).
5. Нажмите на кнопку **Сохранить**.

IOC-файл будет загружен в формате XML.

Скачивание IOC-файла на компьютер

Вы можете скачать ранее загруженный IOC-файл на компьютер.

► *Чтобы скачать IOC-файл на компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, который вы хотите скачать.

   Откроется окно с информацией об IOC-файле.
3. В зависимости от параметров вашего браузера, по ссылке **Скачать** сохраните файл в папку по умолчанию или укажите папку для сохранения файла.

IOC-файл будет сохранен на компьютер в папку загрузки браузера.

Включение и отключение автоматического использования IOC-файла при проверке событий

Вы можете включить или отключить автоматическое использование IOC-файла при проверке событий.

► *Чтобы включить или отключить автоматическое использование IOC-файла при проверке событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. В строке с IOC-файлом, использование которого вы хотите включить или отключить, в графе **Автоматическая проверка** переведите переключатель в одно из следующих положений:
   - **Включено**.
   - **Отключено**.
3. Нажмите на кнопку **Сохранить**.

Автоматическое использование IOC-файла при проверке событий будет включено или отключено.

Удаление IOC-файла

► *Чтобы удалить IOC-файл, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, который вы хотите удалить.

   Откроется окно с информацией об IOC-файле.
3. Нажмите на кнопку **Удалить**.

IOC-файл будет удален.

Поиск результатов IOC-проверки

► *Чтобы найти и просмотреть результаты IOC-проверки, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **IOC**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, для которого вы хотите просмотреть результаты проверки.

   Откроется окно с информацией об IOC-файле.
3. Выполните одно из следующих действий:
   - Если вы хотите просмотреть обнаружения, найденные с помощью IOC-файла, по ссылке **Найти обнаружения** перейдите в базу обнаружений.

     Откроется новая закладка браузера с таблицей найденных обнаружений.
   - Если вы хотите просмотреть события, найденные с помощью IOC-файла, по ссылке **Найти события** перейдите в базу событий.

Откроется новая закладка браузера с таблицей найденных событий.

Фильтрация и поиск IOC-файлов

► *Чтобы отфильтровать или найти IOC-файлы по требуемым критериям, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выполните следующие действия в зависимости от критерия фильтрации:
   - **По степени важности**
   - **По имени файла**
   - **По состоянию автоматической проверки (включена / выключена)**

В таблице IOC-фалов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра IOC-файлов

► *Чтобы сбросить фильтр IOC-файлов по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Нажмите на кнопку ⊠ справа от того заголовка графы таблицы IOC-файлов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице IOC-фалов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Настройка расписания IOC-проверки

Вы можете настроить расписание IOC-проверки компьютеров, на которых установлен компонент Endpoint Agent.

► *Чтобы настроить расписание IOC-проверки, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Расписание IOC-проверки**.

2. В раскрывающихся списках **Время запуска** выберите время начала проверки.
3. В раскрывающемся списке **Максимальное время проверки** выберите ограничение по времени выполнения проверки.

   Если проверка не завершится за указанное время, некоторые события могут быть не найдены.
4. Нажмите на кнопку **Сохранить**.

Новое расписание IOC-проверки начнет действовать сразу после сохранения изменений. Результаты IOC-проверки будут отображаться в таблице обнаружений.

Поддерживаемые индикаторы компрометации OpenIOC

Kaspersky Endpoint Detection and Response поддерживает индикаторы компрометации открытого стандарта OpenIOC, приведенные в таблице ниже.

Таблица 17. Поддерживаемые индикаторы компрометации

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
FileItem/FileName	Нет значения.
FileItem/Md5sum	Нет значения.
FileItem/FilePath	Не поддерживается раскрытие user-specific переменных окружения. Например, `%APPDATA%`, `%UserName%`.
FileItem/SizeInBytes	Нет значения.
RegistryItem/KeyPath	Нет значения.
RegistryItem/Path	Не поддерживаются сканирование user-specific ключей через HKEY_CURRENT_USER и HKEY_CLASSES_ROOT для неавторизованных пользователей.
RegistryItem/Value	Нет значения.
FileItem/PEInfo/PETimeStamp	Нет значения.
FileItem/FullPath	Не поддерживается раскрытие user-specific переменных окружения. Например, `%APPDATA%`, `%UserName%`.
PortItem/remoteIP	Нет значения.
FileItem/PEInfo/DetectedAnomalies/string	Поддерживается только checksum_is_zero.
FileItem/FileExtension	Нет значения.
DnsEntryItem/RecordName	Нет значения.
ProcessItem/name	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
RegistryItem/ValueName	Нет значения.
RegistryItem/Text	Нет значения.
ServiceItem/name	Нет значения.
FileItem/PEInfo/Exports/ExportedFunctions/string	Нет значения.
FileItem/PEInfo/Exports/DllName	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/OriginalFilename	Нет значения.
FileItem/PEInfo/ImportedModules/Module/ImportedFunctions/string	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileDescription	Нет значения.
ProcessItem/arguments	Нет значения.
PortItem/remotePort	Нет значения.
DnsEntryItem/RecordData/IPv4Address	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/InternalName	Нет значения.
FileItem/PEInfo/Exports/NumberOfFunctions	Нет значения.
FileItem/PEInfo/DigitalSignature/SignatureExists	Нет значения.
ProcessItem/SectionList/MemorySection/Name	Нет значения.
FileItem/PEInfo/Type	Нет значения.
ProcessItem/path	Нет значения.
PortItem/localPort	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/CompanyName	Нет значения.
ProcessItem/SectionList/MemorySection/Md5sum	Нет значения.
DnsEntryItem/Host	Нет значения.
PortItem/protocol	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductName	Нет значения.
ServiceItem/description	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Name	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Language	Нет значения.
ServiceItem/descriptiveName	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Language	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalCopyright	Нет значения.
FileItem/PEInfo/ImportedModules/Module/Name	Нет значения.
ServiceItem/serviceDLL	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileVersion	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
FileItem/PEInfo/Sections/Section/Name	Нет значения.
FileItem/PEInfo/DigitalSignature/SignatureVerified	Нет значения.
ServiceItem/path	Нет значения.
FileItem/PEInfo/Subsystem	Нет значения.
FileItem/Sha256sum	Нет значения.
RegistryItem/Type	Нет значения.
FileItem/PEInfo/DigitalSignature/CertificateSubject	Нет значения.
EventLogItem/EID	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Type	Нет значения.
VolumeItem/Name	Нет значения.
EventLogItem/source	Нет значения.
PortItem/state	Нет значения.
UserItem/Username	Сканируются только локальные пользователи. Сканирование доменных пользователей не поддерживается.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductVersion	Нет значения.
DnsEntryItem/RecordType	Нет значения.
VolumeItem/VolumeName	Нет значения.
PortItem/localIP	Нет значения.
ProcessItem/parentpid	Нет значения.
FileItem/PEInfo/DigitalSignature/CertificateIssuer	Нет значения.
ProcessItem/SectionList/MemorySection/Protection	Нет значения.
ProcessItem/SectionList/MemorySection/Sha256sum	Нет значения.
FileItem/PEInfo/Exports/ExportsTimeStamp	Нет значения.
ProcessItem/Username	Нет значения.
ServiceItem/status	Нет значения.
ArpEntryItem/CacheType	Нет значения.
ArpEntryItem/IPv4Address	Нет значения.
ArpEntryItem/Interface	Нет значения.
ArpEntryItem/PhysicalAddress	Нет значения.
DnsEntryItem/DataLength	Нет значения.
DnsEntryItem/Flags	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
DnsEntryItem/RecordData/Host	Нет значения.
DnsEntryItem/RecordName	Нет значения.
DnsEntryItem/TimeToLive	Нет значения.
VolumeItem/ActualAvailableAllocationUnits	Нет значения.
VolumeItem/BytesPerSector	Нет значения.
VolumeItem/CreationTime	Нет значения.
VolumeItem/DevicePath	Нет значения.
VolumeItem/DriveLetter	Нет значения.
VolumeItem/FileSystemFlags	Нет значения.
VolumeItem/FileSystemName	Нет значения.
VolumeItem/IsMounted	Нет значения.
VolumeItem/SectorsPerAllocationUnit	Нет значения.
VolumeItem/SerialNumber	Нет значения.
VolumeItem/TotalAllocationUnits	Нет значения.
VolumeItem/Type	Нет значения.
UserItem/LastLogin	Нет значения.
UserItem/SecurityID	Нет значения.
UserItem/SecurityType	Нет значения.
UserItem/description	Нет значения.
UserItem/disabled	Нет значения.
UserItem/fullname	Нет значения.
UserItem/homedirectory	Нет значения.
UserItem/lockedout	Нет значения.
UserItem/passwordrequired	Нет значения.
UserItem/scriptpath	Нет значения.
UserItem/userpasswordage	Нет значения.
PortItem/CreationTime	Нет значения.
PortItem/path	Нет значения.
PortItem/pid	Нет значения.
PortItem/process	Нет значения.
EventLogItem/log	Нет значения.
EventLogItem/index	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
EventLogItem/user	Нет значения.
EventLogItem/genTime	Нет значения.
EventLogItem/machine	Нет значения.
EventLogItem/CorrelationActivityId	Нет значения.
EventLogItem/CorrelationRelatedActivityId	Нет значения.
EventLogItem/ExecutionProcessId	Нет значения.
EventLogItem/ExecutionThreadId	Нет значения.
RegistryItem/Hive	Не поддерживаются сканирование user-specific ключей через HKEY_CURRENT_USER и HKEY_CLASSES_ROOT для неавторизованных пользователей.
ServiceItem/pid	Нет значения.
ServiceItem/type	Нет значения.
ServiceItem/startedAs	Нет значения.
ServiceItem/arguments	Нет значения.
ServiceItem/mode	Нет значения.
ProcessItem/pid	Нет значения.
ProcessItem/startTime	Нет значения.
ProcessItem/SectionList/MemorySection/RegionSize	Нет значения.
ProcessItem/SectionList/MemorySection/RegionStart	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Comments	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalTrademarks	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/PrivateBuild	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/SpecialBuild	Нет значения.
FileItem/PEInfo/BaseAddress	Нет значения.
FileItem/PEInfo/Exports/NumberOfNames	Нет значения.
FileItem/PEInfo/ImportedModules/Module/NumberOfFunctions	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Size	Нет значения.
FileItem/PEInfo/Sections/ActualNumberOfSections	Нет значения.
FileItem/PEInfo/Sections/NumberOfSections	Нет значения.
FileItem/PEInfo/Sections/Section/SizeInBytes	Нет значения.

kaspersky

Работа с правилами YARA

В качестве баз модуля YARA используются файлы правил YARA.

Вы можете создавать свои правила YARA и добавлять файл правил через веб-интерфейс программы.

Подробнее о создании и обновлении правил YARA версии 3.7.0 и выше см. в документации правил YARA или на веб-сайте http://yararules.com/.

Загрузка правил YARA

► *Чтобы загрузить правила YARA, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **YARA**.
2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
3. Выберите файл правил YARA, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

Окно выбора файлов закроется. Отобразится следующая информация о загруженных правилах YARA:

- **Размер файла** – размер файла правил.
- **Время загрузки** – дата и время последней загрузки файла правил.

Обновление правил YARA

► *Чтобы обновить правила YARA, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **YARA**.
2. Нажмите на кнопку **Заменить**.

   Откроется окно выбора файлов.
3. Выберите файл правил YARA, которым вы хотите заменить текущий файл, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Загруженный файл правил заменит предыдущий файл.

Удаление правил YARA

► *Чтобы удалить правила YARA, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила пользователей**, подраздел **YARA**.
2. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
3. Нажмите на кнопку **Да**.

Правила YARA будут удалены.

kaspersky

Работа с объектами в Хранилище и на карантине

Вы можете поместить копии объектов, которые хотите проверить, в специальное Хранилище.

Хранилище расположено на сервере Central Node.

Вы можете управлять объектами в Хранилище: удалять, скачивать, загружать, отправлять на проверку, а также фильтровать списки объектов.

Kaspersky Endpoint Detection and Response отображает объекты в Хранилище в виде таблицы объектов.

Если вы используете режим распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76) и multitenancy, Хранилище расположено на серверах PCN и SCN. В веб-интерфейсе сервера PCN отображается информация о Хранилище всех подключенных SCN в рамках тех организаций, к данным которых у пользователя есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

Пользователь с ролью **Старший сотрудник службы безопасности** может поместить копии объектов в Хранилище с помощью задачи **Получить файл** или загрузив объект в Хранилище вручную (см. раздел "Загрузка объектов в Хранилище" на стр. 351) на том сервере PCN или SCN, с которым он работает в рамках тех организаций, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

Пользователь с ролью **Сотрудник службы безопасности** может работать только с файлами, полученными в результате выполнения задач, которые он сам создал на том сервере PCN или SCN, с которым он работает в рамках тех организаций, к данным которых у него есть доступ (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

Если вы считаете объект опасным, вы можете поместить его на карантин на компьютере с компонентом Endpoint Agent. Метаданные объекта, помещенного на карантин, отобразятся в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса программы.

Карантин на компьютерах с компонентом Endpoint Agent – это специальное хранилище на каждом компьютере, на котором был обнаружен опасный объект. На карантин помещаются объекты, возможно зараженные вирусами или неизлечимые на момент обнаружения. Объекты на карантине хранятся в зашифрованном виде и не угрожают безопасности компьютера.

При помещении объекта на карантин на компьютере с компонентом Endpoint Agent выполняется его перемещение, а не копирование: объект удаляется из той директории, в которой он был обнаружен и помещается в директорию карантина, указанную в параметрах Endpoint Agent.

Карантин на сервереKaspersky Endpoint Detection and Response – это область Хранилища серверной части решения, предназначенная для хранения метаданных объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса программы.

Вы можете управлять объектами на карантине: восстанавливать объекты из карантина, а также загружать копии объектов, помещенных на карантин на компьютерах с компонентом Endpoint Agent, в ХранилищеKaspersky Endpoint Detection and Response.

Kaspersky Endpoint Detection and Response отображает объекты, помещенные на карантин, в виде таблицы объектов.

По умолчанию максимальный объем Хранилища (помимо Карантина) составляет 10 ГБ. Как только объем

Хранилища превышает заданное по умолчанию пороговое значение, программа начинает удалять из Хранилища самые старые копии объектов. Когда объем Хранилища снова становится меньше порогового значения, программа прекращает удалять копии объектов из Хранилища.

Максимальный объем Карантина составляет 10 ГБ. Если объем Карантина превысит заданное по умолчанию пороговое значение, вы не сможете помещать в него новые объекты, пока не удалите часть старых объектов.

Максимальный размер объекта, который можно поместить на карантин, составляет 100 МБ.

Реальный размер объекта может быть больше видимого размера объекта из-за метаданных, необходимых для восстановления объекта из карантина. При помещении на карантин учитывается реальный размер объекта. Зашифрованные файлы могут передаваться в расшифрованном виде (в зависимости от параметров шифрования), сжатые файлы передаются в исходном виде.

В этом разделе

Просмотр таблицы объектов, помещенных в Хранилище

Таблица объектов, помещенных в Хранилище, находится в разделе **Хранилище**, подразделе **Файлы** веб-интерфейса программы.

В таблице объектов, помещенных в Хранилище, содержится следующая информация:

1. **Тип** – расположение объекта в Хранилище.

   Возможны следующие типы объектов:

   - – объект помещен в хранилище одним из следующих способов:

- выполнена задача **Поместить файл на карантин** в разделе **Задачи**;
- выполнена задача **Получить файл** в разделе **Задачи**;
- получена копия объекта, помещенного на карантин на компьютерах с компонентом Endpoint Agent (в разделе **Хранилище**, подразделе **Карантин** в меню, раскрывшемся по ссылке с директорией объекта, выбрано действие **Получить файл из карантина**).

- – объект загружен пользователем вручную в разделе **Хранилище**, подразделе **Файлы**.

2. **Объект** – информация об объекте. Например, имя файла или путь к файлу.
3. **Результаты проверки** – результат проверки объекта.

   Результат проверки отображается в виде одного из следующих значений:

   - **Не обнаружено** – в результате проверки программа не обнаружила признаков целевой атаки, возможно зараженных объектов или подозрительной активности.
   - **С ошибкой** – проверка объекта завершилась с ошибкой.
   - **Выполняется** – проверка объекта еще не завершилась.
   - **Не выполнялась** – объект не был отправлен на проверку.
   - **Обнаружено** – в результате проверки программа обнаружила признаки целевой атаки, возможно зараженный объект или подозрительную активность.
4. **Серверы** – имя сервера Central Node, PCN или SCN. К этому серверу подключен хост, с которого получен объект.
5. **Адрес источника** – IP-адрес или имя хоста, с которого получен объект, или имя учетной записи пользователя, загрузившего объект.
6. **Время** – дата и время помещения объекта в Хранилище.

Просмотр информации об объекте в Хранилище

► *Чтобы просмотреть информацию об объекте в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. В таблице выберите объект, информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- **Имя файла** – имя файла.

  По ссылке рядом с **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Размер** – размер файла.

- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на KL TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **SHA256** – SHA256-хеш файла.

  По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на KL TIP**.
  - **Найти на virustotal.com**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **Время** – время помещения объекта в Хранилище.
- **Время загрузки** – время загрузки для объектов, загруженных пользователем вручную.
- **Организация** – название организации, к которой относится сервер Central Node, PCN или SCN.
- **Сервер** – имя сервера Central Node, PCN или SCN. К этому серверу подключен хост, с которого получен объект.
- **Хост** – имя хоста, с которого получен объект.
- **Имя пользователя** – имя учетной записи пользователя, загрузившего объект в Хранилище вручную.
- **Результаты проверки** – результат проверки объекта программой.

Скачивание объектов из Хранилища

Если вы считаете объект в Хранилище безопасным, вы можете скачать его на локальный компьютер.

Скачивание зараженных объектов может угрожать безопасности вашего локального компьютера.

► *Чтобы скачать объект из Хранилища, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. В правой части строки с именем объекта, который вы хотите скачать, нажмите на кнопку 

Объект будет сохранен на ваш локальный компьютер в папку загрузки браузера. Файл загружается в формате ZIP-архива, защищенного паролем infected.

Загрузка объектов в Хранилище

Если вам требуется запустить проверку определенного объекта, вы можете загрузить этот объект в Хранилище и отправить его на проверку (см. раздел "Проверка объектов из Хранилища" на стр. 351).

► *Чтобы загрузить объект в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. В правом верхнем углу окна нажмите на кнопу **Загрузить**.

   Откроется окно выбора файла.
3. Выберите объект, который вы хотите загрузить в Хранилище, и нажмите на кнопку **Open**.

Объект будет загружен в Хранилище и отобразится в таблице объектов.

Проверка объектов из Хранилища

Вы можете проверить объекты, помещенные в Хранилище, компонентом Central Node с помощью технологий Anti-Malware Engine и YARA, а также компонентом Sandbox.

Рекомендуется отправлять объекты из Хранилища на проверку в следующих случаях:

- проверка при помещении в Хранилище была отключена;
- базы программы были обновлены;
- объект был загружен в Хранилище вручную.

► *Чтобы отправить объект из Хранилища на проверку, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. Нажмите на объект, который вы хотите проверить.

   Откроется окно сведений об объекте.
3. Нажмите на кнопку **Проверить**.

Запустится проверка объекта.

После завершения проверки объекта его статус отобразится в таблице объектов.

Удаление объектов из Хранилища

► *Чтобы удалить объект из Хранилища, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

Откроется таблица объектов.

2. Нажмите на объект, который вы хотите удалить.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Объект будет удален из Хранилища.

Фильтрация объектов в Хранилище по типу объекта

► *Чтобы отфильтровать объекты в Хранилище по их типу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Тип** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:
   - **Файл, помещенный в хранилище по задаче**, если вы хотите, чтобы программа отображала в таблице объекты, содержащиеся в Хранилище, но не помещенные на карантин.
   - **Метаданные объекта на карантине**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные на карантин.
   - **Файл, загруженный вручную**, если вы хотите, чтобы программа отображала в таблице объекты, загруженные пользователем вручную.
4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по описанию объекта

► *Чтобы отфильтровать объекты в Хранилище по описанию объекта, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Объект** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих вариантов:
   - **Путь к файлу**.

- **MD5**.
- **SHA256**.

4. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
5. В поле ввода укажите один или несколько символов описания объекта.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по результатам проверки

► *Чтобы отфильтровать объекты в Хранилище по результатам проверки этих объектов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Результаты проверки** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:
   - **Не обнаружено**.
   - **С ошибкой**.
   - **Выполняется**.
   - **Не выполнялась**.
   - **Обнаружено**.
4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по имени сервера Central Node, PCN или SCN

► *Чтобы отфильтровать объекты в Хранилище по имени сервера Central Node, PCN или SCN, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Серверы** откройте меню фильтрации объектов.
3. Установите один или несколько флажков напротив тех серверов, по которым вы хотите отфильтровать объекты в Хранилище.
4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по источнику объекта

► *Чтобы отфильтровать объекты в Хранилище по источнику, с которого они были получены, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Адрес источника** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов IP-адреса, имени хоста или имени учетной записи пользователя, загрузившего объект вручную.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов по времени помещения в Хранилище

► *Чтобы отфильтровать объекты по времени помещения в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Время** откройте меню фильтрации объектов.
3. Выберите один из следующих периодов отображения объектов:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все помещенные в Хранилище объекты.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище за указанный вами период.
4. Если вы выбрали период отображения объектов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения объектов.
   b. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра объектов в Хранилище

► *Чтобы сбросить фильтр объектов в Хранилище по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. Нажмите на кнопку ⊠ справа от того заголовка графы таблицы объектов в Хранилище, условия фильтрации по которому вы хотите сбросить.

Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

kaspersky

Работа с отчетами

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** могут управлять отчетами об обнаружениях программы: создавать шаблоны отчетов (см. раздел "Создание шаблона" на стр. 358), создавать отчеты по шаблону (см. раздел "Создание отчета по шаблону" на стр. 359), просматривать и удалять отчеты и шаблоны отчетов.

Отчет формируется на основе выборки обнаружений за указанный период. Если вы используете режим распределенного решения и multitenancy, выборка данных осуществляется также по организации и серверам этой организации.

Управление шаблонами отчетов и отчетами доступно во всех режимах работы программы в соответствии с лицензией.

Выполняйте действия по созданию отчета в следующем порядке:

a. **Создайте шаблон отчета (см. раздел "Создание шаблона" на стр. 358).**

b. **Создайте отчет на основе шаблона (см. раздел "Создание отчета по шаблону" на стр. 359).**

В этом разделе

kaspersky

Создание шаблона

При создании шаблона отчета вам нужно указать всю информацию, которую вы хотите отображать в отчете: имя отчета, его описание, наличие таблицы, графика или изображения. Также вы можете выбрать данные, которые вы хотите отображать в отчете и задать расположение элементов отчета. Создание отчета (см. раздел "Создание отчета по шаблону" на стр. 359) в разделе **Отчеты**, подразделе **Созданные отчеты** интерфейса позволяет только выбрать шаблон для создания отчета и период отображения данных.
Создавайте новый шаблон отчета для каждой выборки данных.

► *Чтобы создать шаблон, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Нажмите на кнопку **Добавить**.

   Откроется окно создания шаблона. Окно содержит тело отчета и конструктор отчета в плавающем окне. Вы можете перемещать конструктор отчета по рабочей области окна веб-интерфейса.

3. В поле **Имя шаблона** в правом верхнем углу окна введите имя, которое вы хотите присвоить отчетам, создаваемым по этому шаблону. Например, **Обнаружения по технологии**.

   Это имя отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов на этом шаблоне.

4. Вместо текста **Заголовок отчета** введите имя отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять имя отчета, вы можете стереть текст **Заголовок отчета** и оставить этот раздел отчета пустым.

   Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.

5. Вместо текста **Описание отчета** введите описание отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять описание отчета, вы можете стереть текст **Описание отчета** и оставить этот раздел отчета пустым.

   Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.

6. Используя конструктор отчета, добавьте один или несколько элементов отчета:

   - **Таблица**.
   - **Диаграмма**.
   - **Изображение**.

7. Если вы выбрали добавление изображения, откроется окно **Изображение**. Выполните следующие действия:

   a. Нажмите на кнопку **Загрузить**.

   b. Загрузите изображение. Например, вы можете загрузить логотип вашей организации.

   c. В списке справа от кнопки загрузки выберите выравнивание изображения на странице отчета: **По левому краю**, **По правому краю** или **По центру**.

   d. Нажмите на кнопку **Применить**.

8. Если вы выбрали добавление диаграммы, откроется окно **Диаграмма по свойствам обнаружений**.

Выполните следующие действия:

a. В поле **Имя** введите имя диаграммы. Например, **Топ 5 обнаружений по технологии**. Вы также можете оставить поле пустым.

b. В списке **Источник данных** выберите свойство обнаружения, по которому вы хотите создать диаграмму. Например, **Технологии**.

c. В поле **Количество секторов** укажите максимальное количество секторов диаграммы. При создании отчета программа выберет наиболее часто встречающиеся данные. Например, если вы указали 5 секторов и хотите создать диаграмму по технологии, программа покажет диаграмму по 5 технологиям, выполнившим наибольшее количество обнаружений. Технологии, выполнившие наименьшее количество обнаружений, не отобразятся на диаграмме.

Нажмите на кнопку **Применить**.

9. Если вы выбрали добавление таблицы, откроется окно **Таблица обнаружений**. Выполните следующие действия:

a. В поле **Доступные столбцы** двойным щелчком мыши выберите свойства обнаружений, которые вы хотите добавить в таблицу отчета.

Выбранные свойства переместятся в поле **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.

Например, если в поле **Выбранные столбцы** вы переместили свойства **Технологии, Обнаружено** и **Время создания**, в таблице созданного отчета отобразятся технологии, выполнившие обнаружения, список обнаруженных объектов и время создания обнаружений.

b. Если вы хотите отфильтровать обнаружения по свойству **Состояние**, установите флажки рядом с теми состояниями обработки обнаружений пользователем, данные по которым вы хотите отображать в отчете.

c. Если вы хотите отфильтровать обнаружения по свойству **Технологии**, установите флажки рядом с теми названиями модулей и компонентов программы, данные по которым вы хотите отображать в отчете.

d. Если вы хотите отфильтровать обнаружения по свойству **Важность**, установите флажки рядом с теми степенями важности обнаружений, данные по которым вы хотите отображать в отчете.

e. Если вы хотите отфильтровать обнаружения по статусу **Статус VIP**, в списке выберите **VIP**. В отчете отобразятся только обнаружения со статусом VIP.

f. Нажмите на кнопку **Применить**.

10. Нажмите на кнопку **Сохранить** в правом верхнем углу окна.

Будет создан новый шаблон.

Создание отчета по шаблону

► *Чтобы создать отчет по шаблону, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

Откроется таблица отчетов.

2. Нажмите на кнопку **Добавить**.

Откроется окно **Новый отчет**.

3. Выполните следующие действия:
   a. В раскрывающемся списке **Шаблон** выберите один из шаблонов для создания отчета.
   b. В блоке параметров **Период** выберите один из следующих вариантов:
      - **Прошедший час**, если вы хотите, чтобы отчет содержал информацию о работе программы за предыдущий час.
      - **Прошедшие сутки**, если вы хотите, чтобы отчет содержал информацию о работе программы за предыдущий день.
      - **Прошедшие 7 дней**, если вы хотите, чтобы отчет содержал информацию о работе программы за предыдущую неделю.
      - **Прошедшие 30 дней**, если вы хотите, чтобы отчет содержал информацию о работе системы за предыдущий месяц.
      - **Пользовательский**, если вы хотите, чтобы отчет содержал информацию о работе системы за указанный вами период.
4. Если вы выбрали период отображения информации о работе программы **Пользовательский**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода, за который будет создан отчет.
   b. Нажмите на кнопку **Применить**.
5. Если вы используете режим распределенного решения и multitenacy, в блоке параметров **Серверы** установите флажки напротив тех организаций и серверов, данные по которым вы хотите отображать в отчете.
6. Нажмите на кнопку **Создать**.

Созданный отчет отобразится в таблице отчетов. Вы можете загрузить отчет для просмотра (см. раздел "Скачивание отчета на локальный компьютер" на стр. 361) на вашем компьютере.

Просмотр таблицы шаблонов и отчетов

Шаблоны и отчеты отображаются в разделе **Отчеты** окна веб-интерфейса программы.

В подразделе **Созданные отчеты** отображается таблица отчетов. Таблица содержит следующую информацию:

- **Время создания** – дата и время создания отчета.
- **Имя отчета** – имя отчета, созданного по шаблону.
- **Серверы** – имя сервера с компонентом Central Node, на котором создан отчет (если вы используете режим распределенного решения и multitenancy).
- **Период** – период, за который создан отчет.
- **Автор** – имя пользователя, создавшего отчет.

В подразделе **Шаблоны** отображается таблица шаблонов. Таблица содержит следующую информацию:

- **Время создания** – дата и время создания шаблона.
- **Время обновления** – дата и время последнего изменения шаблона.

- **Имя отчета** – имя шаблона.
- **Автор** – имя пользователя, создавшего шаблон.

Просмотр отчета

► *Чтобы просмотреть отчет, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. Выберите отчет, который вы хотите просмотреть.

Отчет откроется в новой вкладке вашего браузера.

Скачивание отчета на локальный компьютер

► *Чтобы скачать отчет на ваш компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. В строке с отчетом, который вы хотите просмотреть, нажмите на значок  .

   Отчет будет сохранен в формате HTML на ваш локальный компьютер в папку загрузки браузера.

   Для просмотра отчета вы можете использовать любую программу для просмотра HTML-файлов (например, браузер).

Изменение шаблона

► *Чтобы изменить шаблон, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.
2. Выберите шаблон, который вы хотите изменить.

   Откроется окно изменения шаблона.
3. Вы можете изменить следующие параметры:
   - **Имя шаблона** – имя отчета, которое отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов по этому шаблону.
   - **Заголовок отчета** – имя отчета, которое отобразится в отчете после создания отчета.

     Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
   - **Описание отчета** – описание отчета, которое отобразится в отчете после создания отчета.

     Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
   - **Изображение**. Вы можете загрузить или удалить изображение.

- **Диаграмма**. Вы можете изменить следующие параметры диаграммы:
  - **Имя**.
  - **Источник данных**.
  - **Количество секторов**.

  Нажмите на кнопку **Применить**.
- **Таблица**. Вы можете изменить следующие параметры таблицы:
  - **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.
  - **Состояние**.
  - **Технологии**.
  - **Важность**.
  - **Статус VIP**.

4. Выберите один из следующих способов сохранения шаблона:
   - Если вы хотите применить изменения к текущему шаблону, нажмите на кнопку **Сохранить**.

     Шаблон будет изменен.
   - Если вы хотите создать новый шаблон, введите имя и нажмите на кнопку **Сохранить как**.

     Имя нового шаблона не должно совпадать с именем уже существующего шаблона.

     Новый шаблон будет сохранен.

Фильтрация шаблонов по имени

► *Чтобы отфильтровать шаблоны по имени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.
2. По ссылке **Имя отчета** откройте меню фильтрации шаблонов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени шаблона.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по имени пользователя, создавшего шаблон

► *Чтобы отфильтровать шаблоны по имени пользователя, создавшего шаблон, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.
2. По ссылке **Автор** откройте меню фильтрации шаблонов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по времени создания

► *Чтобы отфильтровать шаблоны отчетов по времени создания, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.
2. По ссылке **Время создания** откройте меню фильтрации шаблонов.
3. Выберите один из следующих периодов отображения шаблонов:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все созданные шаблоны.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные за указанный вами период.
4. Если вы выбрали период отображения шаблонов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения шаблонов.
   b. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Сброс фильтра шаблонов

► *Чтобы сбросить фильтр шаблонов по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Нажмите на кнопку справа от того заголовка графы таблицы шаблонов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Удаление шаблона

► *Чтобы удалить шаблон, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Установите флажок в строке с шаблоном, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранный вами шаблон будет удален.

Фильтрация отчетов по времени создания

► *Чтобы отфильтровать отчеты по времени их создания, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. По ссылке **Время создания** откройте меню фильтрации отчетов.
3. Выберите один из следующих периодов отображения отчетов:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все созданные отчеты.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице отчеты, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице отчеты, созданные за предыдущий день.

- **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице отчеты, созданные за указанный вами период.

4. Если вы выбрали период отображения отчетов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения отчетов.
   b. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени

► *Чтобы отфильтровать отчеты по имени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Имя отчета** откройте меню фильтрации отчетов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени отчета.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени сервера с компонентом Central Node

► *Чтобы отфильтровать отчеты по имени сервера с компонентом Central Node, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Серверы** откройте меню фильтрации отчетов.
3. Установите флажки напротив тех серверов, по которым вы хотите отфильтровать отчеты.
4. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени пользователя, создавшего отчет

► *Чтобы отфильтровать отчеты по имени пользователя, создавшего отчет, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Автор** откройте меню фильтрации отчетов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Сброс фильтра отчетов

► *Чтобы сбросить фильтр отчетов по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. Нажмите на кнопку ⊠ справа от того заголовка графы таблицы отчетов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Удаление отчета

► *Чтобы удалить отчет о работе программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. Установите флажок в строке с отчетом, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранный отчет будет удален.

kaspersky

Отправка уведомлений

Вы можете настроить отправку уведомлений на один или несколько адресов электронной почты.

В программе доступны уведомления об обнаружениях и о проблемах в работе программы.

В этом разделе

Просмотр таблицы правил для отправки уведомлений

Правила для отправки уведомлений отображаются в разделе **Параметры**, подразделе **Отправка уведомлений** окна веб-интерфейса программы.

Таблица правил для отправки уведомлений содержит следующую информацию:

- – тип правила для отправки уведомлений.

  Возможны следующие типы правил:

  - – правило для отправки уведомления об обнаружениях;
  - – правило для отправки уведомления о работе компонентов программы.
- **Тема** – тема сообщения с уведомлением.
- **Кому** – адреса электронной почты, на которые отправляются уведомления.
- **Состояние** – состояние правила для отправки уведомления.

Создание правила для отправки уведомлений об обнаружениях

► *Чтобы создать правило для отправки уведомлений об обнаружениях, выполните*

следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило отправки уведомлений**.
3. В поле **Кому** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.

   Вы можете ввести несколько адресов электронной почты через запятую.
4. В поле **Тема** введите тему сообщения с уведомлением.
5. Если вы хотите, чтобы программа подставляла важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.
6. В поле **Тип уведомления** выберите **Обнаружения**.
7. В раскрывающемся списке **Важность обнаружения** выберите минимальное значение важности обнаружений, о которых вы хотите настроить отправку уведомлений.

   Например, вы можете настроить отправку уведомлений об обнаружениях только высокой степени важности или только средней и высокой степени важности.
8. В поле **Адрес источника или назначения** введите IP-адрес и маску сети, если вы хотите настроить отправку уведомлений об обнаружениях, связанных с определенным IP-адресом или адресом подсети источника или назначения.
9. В поле **Email** введите адрес электронной почты, если вы хотите настроить отправку уведомлений об обнаружениях, связанных с определенным адресом отправителя или получателя сообщений электронной почты.
10. В блоке параметров **Компоненты** установите флажки рядом с названиями одной или нескольких технологий, если вы хотите настроить отправку уведомлений об обнаружениях, выполненных определенными технологиями.
11. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений об обнаружениях будет добавлено в список правил.

Создание правила для отправки уведомлений о работе компонентов программы

► *Чтобы создать правило для отправки уведомлений о работе компонентов программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило отправки уведомлений**.
3. В поле **Кому** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.

   Вы можете ввести несколько адресов электронной почты через запятую.

4. В поле **Тема** введите тему сообщения с уведомлением.
5. Если вы хотите, чтобы программа подставляла важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.
6. В поле **Тип уведомления** выберите **Работа программы**.
7. В блоке параметров **Компоненты** установите флажки рядом с названиями тех функциональных областей программы, о которых вы хотите получать уведомления.
8. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений о работе компонентов программы будет добавлено в список правил.

Включение и отключение правила для отправки уведомлений

► *Чтобы включить или отключить правило для отправки уведомлений об обнаружениях, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. В строке с правилом для отправки уведомлений, которое вы хотите включить или отключить, в графе **Состояние** выполните одно из следующих действий:
   - Включите переключатель, если вы хотите включить правило.
   - Выключите переключатель, если вы хотите отключить правило.

Состояние правила для отправки уведомлений об обнаружениях будет изменено.

Изменение правила для отправки уведомлений

► *Чтобы изменить правило для отправки уведомлений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. В списке правил для отправки уведомлений выберите правило, которое вы хотите изменить.

   Откроется окно **Редактировать правило отправки уведомлений**.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Сохранить**.

Правило для отправки уведомлений будет изменено.

Удаление правила для отправки уведомлений

► *Чтобы удалить правило для отправки уведомлений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.

2. Установите флажок слева от названия каждого правила, которое вы хотите удалить.

   Если вы хотите удалить все правила, установите флажок над списком.

3. Нажмите на кнопку **Удалить** в нижней части окна.
4. В окне подтверждения нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Фильтрация и поиск правил отправки уведомлений по типу правила

► *Чтобы отфильтровать или найти правила отправки уведомлений по типу правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. В таблице правил для отправки уведомлений нажмите на значок  .

   Откроется окно настройки фильтрации.
3. Выберите один из следующих вариантов:
   - **Все**.
   - **Обнаружения**.
   - **Работа программы**.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по теме уведомлений

► *Чтобы отфильтровать или найти правила отправки уведомлений по теме уведомлений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. По ссылке **Тема** откройте окно настройки фильтрации.
3. Введите один или несколько символов темы уведомлений.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным

вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по адресу электронной почты

► *Чтобы отфильтровать или найти правила отправки уведомлений по адресу электронной почты, на который они отправляются, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. По ссылке **Кому** откройте окно настройки фильтрации.
3. Введите один или несколько символов адреса электронной почты.
4. Нажмите на кнопку **Применить**.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по их состоянию

► *Чтобы отфильтровать или найти правила отправки уведомлений по их состоянию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. По ссылке **Состояние** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом со значениями состояний:
   - **Включено**.
   - **Отключено**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил отправки уведомлений

► *Чтобы сбросить фильтр правил отправки уведомлений по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. Нажмите на кнопку справа от того заголовка графы таблицы правил отправки уведомлений, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

kaspersky

Работа с правилами присвоения обнаружениям статуса VIP

Вы можете создавать, импортировать и экспортировать список правил присвоения обнаружениям статуса VIP. Обнаружения со статусом VIP доступны только пользователям с ролью **Старший сотрудник службы безопасности**.

Вы можете создавать правила одного из следующих типов:

- **IP**. Новым обнаружениям, связанным с этим IP-адресом компьютера, будет присвоен статус VIP.
- **Имя хоста**. Новым обнаружениям, связанным с этим именем хоста, будет присвоен статус VIP.
- **Email**. Новым обнаружениям, связанным с этим адресом электронной почты, будет присвоен статус VIP.

В этом разделе

Добавление правила присвоения статуса VIP

► *Чтобы добавить правило присвоения обнаружениям статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Добавить**.

   Откроется окно добавления правила.
3. В раскрывающемся списке **Критерий** выберите один из следующих типов правила:
   - **IP**, если вы хотите добавить правило для IP-адреса компьютера.
   - **Хост**, если вы хотите добавить правило для имени хоста.
   - **Email**, если вы хотите добавить правило для адреса электронной почты.
4. В поле **Значение** введите нужное значение.

   Например, если в списке **Критерий** вы выбрали **Email**, в поле **Значение** введите адрес электронной

почты, для которого вы хотите добавить правило.

5. В поле **Описание** введите дополнительную информацию, если необходимо.
6. Нажмите на кнопку **Добавить**.

Правило будет добавлено. Новым обнаружениям, связанным с добавленным IP-адресом, именем хоста или адресом электронной почты, будет присвоен статус VIP.

Удаление правила присвоения статуса VIP

► *Чтобы удалить правило присвоения обнаружениям статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Установите флажок слева от каждого правила, которое вы хотите удалить из списка.
3. Если вы хотите удалить все правила, установите флажок над списком.
4. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Изменение правила присвоения статуса VIP

► *Чтобы изменить правило присвоения обнаружениям статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Выберите правило, которое вы хотите изменить.

   Откроется окно изменения правила.
3. Внесите необходимые изменения в поля **Критерий**, **Значение**, **Описание**.
4. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Импорт списка правил присвоения статуса VIP

► *Чтобы импортировать список правил присвоения обнаружениям статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Нажмите на кнопку **Импортировать**.

   Отобразится подтверждение импорта списка.

Импортированный список правил присвоения обнаружениям статуса VIP заменит текущий список правил присвоения обнаружениям статуса VIP.

3. Нажмите на кнопку **Да**.

   Откроется окно выбора файлов.

4. Выберите файл формата JSON со списком правил, которые вы хотите импортировать, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Список будет импортирован.

Экспорт списка правил присвоения статуса VIP

► *Чтобы экспортировать список правил присвоения статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Экспортировать**.

Список правил присвоения статуса VIP будет экспортирован в файл формата JSON.

Фильтрация и поиск по типу правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по типу правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Критерий** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом с типами правил:
   - **IP**.
   - **Хост**.
   - **Email**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по значению правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по значению правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Значение** откройте окно настройки фильтрации.
3. Введите один или несколько символов значения правила.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по описанию правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по описанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Описание** откройте окно настройки фильтрации.
3. Введите один или несколько символов описания.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил присвоения статуса VIP

► *Чтобы сбросить фильтр правил присвоения обнаружениям статуса VIP по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Нажмите на кнопку ⊠ справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

kaspersky

Работа с белым списком объектов

Вы можете создавать, импортировать и экспортировать *белый список* – список данных, которые Kaspersky Endpoint Detection and Response будет считать безопасными и не будет отображать в таблице обнаружений. Вы можете включать следующие данные в белый список:

- **MD5**.
- **Формат**.
- **Маска URL**.
- **Адрес или подсеть источника**.
- **Адрес или подсеть назначения**.
- **Агент пользователя**.

В этом разделе

Добавление записи в белый список

► *Чтобы добавить запись в белый список, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения ТАА**, закладку **Белый список**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Добавить**.

   Откроется окно **Новая запись**.
3. В раскрывающемся списке **Критерий** выберите один из следующих критериев добавления записи в белый список:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Адрес или подсеть источника**.
   - **Адрес или подсеть назначения**.

- **Агент пользователя**.

4. Если вы выбрали **Формат**, в раскрывающемся списке **Значение** выберите формат файла, который вы хотите добавить.

   Например, вы можете выбрать формат **MSOfficeDoc**.

5. Если вы выбрали **MD5**, **Маска URL**, **Адрес получателя электронной почты**, **Адрес отправителя электронной почты**, **Адрес или подсеть источника**, **Адрес или подсеть назначения** или **Агент пользователя**, в поле **Значение** введите значение соответствующего критерия, которое вы хотите добавить в белый список:

   - Если вы выбрали **MD5**, в поле **Значение** введите MD5-хеш файла.
   - Если вы выбрали **Маска URL**, в поле **Значение** введите маску URL-адреса.

     При формировании маски вы можете использовать следующие специальные символы:

     * – любая последовательность символов.

Пример:

Если вы введете маску `*abc*`, программа будет считать безопасным любой URL-адрес, содержащий последовательность `abc`. Например, `www.example.com/download_virusabc`

     ? – любой один символ.

Пример:

Если вы введете маску `example_123?.com`, программа будет считать безопасным любой URL-адрес, содержащий заданную последовательность символов и любой символ, следующий за `3`. Например, `example_1234.com`

     В случае, если символы `*` и `?` входят в состав полного URL-адреса, добавляемого в белый список, необходимо при вводе этого адреса использовать символ `\` – отмена одного из следующих за ним символов `*` или `?`, \.

Пример:

В качестве доверенного адреса необходимо добавить следующий URL-адрес:
`www.example.com/download_virus/virus.dll?virus_name=`

Чтобы программа не восприняла `?` как специальный символ формирования маски, нужно поставить перед `?` знак `\`.

URL-адрес, добавляемый в белый список, будет выглядеть следующим образом:
`www.example.com/download_virus/virus.dll\?virus_name=`

   - Если вы выбрали **Адрес получателя электронной почты** или **Адрес отправителя электронной почты**, в поле **Значение** введите адрес электронной почты.
   - Если вы выбрали **Агент пользователя**, в поле **Значение** введите заголовок User agent HTTP-запросов, содержащий информацию о браузере.
   - Если вы выбрали **Адрес или подсеть источника** или **Адрес или подсеть назначения**, в поле **Значение** введите адрес или подсеть. Например, 255.255.255.0

> В полях **Маска URL**, **Адрес получателя электронной почты**, **Адрес отправителя электронной почты** вы можете указывать доменные имена, содержащие символы кириллицы. В этом случае указанный адрес будет преобразован в Punycode и обработан в соответствии с параметрами программы.

6. Нажмите на кнопку **Добавить**.

Запись будет добавлена в белый список.

Удаление записи из белого списка

► *Чтобы удалить одну или несколько записей из белого списка, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения ТАА**, закладку **Белый список**.
2. Установите флажок слева от каждой записи, которую вы хотите удалить из белого списка.

   Если вы хотите удалить все записи, установите флажок над списком.
3. В правом верхнем углу окна нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранные записи будут удалены из белого списка.

Изменение записи в белом списке

► *Чтобы изменить запись в белом списке, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения ТАА**, закладку **Белый список**.
2. Выберите запись, которую вы хотите изменить.

   Откроется окно **Редактировать правило**.
3. Внесите необходимые изменения в поля **Критерий** и **Значение**.
4. Нажмите на кнопку **Сохранить**.

Запись будет изменена.

Экспорт белого списка

► *Чтобы экспортировать белый список, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения ТАА**, закладку **Белый список**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Экспортировать**.

Файл в формате JSON с экспортированным белым списком будет сохранен в папку загрузки браузера на вашем компьютере.

Фильтрация и поиск записей в белом списке по критерию

► *Чтобы отфильтровать или найти записи в белом списке по типу правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения ТАА**, закладку **Белый список**.
2. По ссылке **Критерий** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом с критериями, по которым вы хотите отфильтровать записи:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Адрес или подсеть источника**.
   - **Адрес или подсеть назначения**.
   - **Агент пользователя**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В белом списке отобразятся только записи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск записей в белом списке по значению

► *Чтобы отфильтровать или найти записи в белом списке по значению, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения ТАА**, закладку **Белый список**.
2. По ссылке **Значение** откройте окно настройки фильтрации.
3. Введите один или несколько символов значения.
4. Нажмите на кнопку **Применить**.

В белом списке отобразятся только записи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра записей в белом списке

► *Чтобы сбросить фильтр записей в белом списке по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения ТАА**, закладку **Белый список**.
2. Нажмите на кнопку справа от того заголовка графы таблицы записей в белом списке, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В белом списке отобразятся только записи, соответствующие заданным вами условиям.

kaspersky

Работа с ТАА-исключениями

Вы можете добавлять правила ТАА (IOA) в исключения.Kaspersky Endpoint Detection and Response не будет создавать обнаружения по этим правилам и не будет отображать события, в которых сработали эти правила ТАА (IOA).

В этом разделе

Просмотр списка правил ТАА (IOA), добавленных в исключения

► *Чтобы просмотреть список правил ТАА (IOA), добавленных в исключения,*

в окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белые списки** и закладку **Исключения ТАА (IOA)**.

Отобразится таблица правил ТАА (IOA), добавленных в исключения. Вы можете фильтровать правила по ссылкам в названии граф.

В таблице содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, выполненному по этому правилу ТАА (IOA).

   Степень важности может иметь одно из следующих значений:

   - – **Низкая**.
   - – **Средняя**.
   - – **Высокая**.

2. **Тип** – тип правила в зависимости от роли сервера, на котором оно создано, в режиме распределенного решения (см. раздел "Распределенное решение и режим multitenancy" на стр. 76):

   - **Глобальный** – правило создано на сервере PCN.
   - **Локальный** – правило создано на сервере SCN.

3. **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:

   - **Высокая**.
   - **Средняя**.
   - **Низкая**.

   Чем выше надежность, тем меньше вероятность ложных срабатываний

4. **Имя** – имя правила.

Просмотр правила TAA (IOA), добавленного в исключения

► *Чтобы просмотреть правило TAA (IOA), добавленного в исключения, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белые списки** и закладку **Исключения TAA (IOA)**.
2. Отобразится таблица правил TAA (IOA), добавленных в исключения.
3. Выберите правило, которое вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Правило TAA (IOA)**. По ссылке открывается окно с описанием техники MITRE, соответствующей этому правилу, рекомендациям по реагированию на событие и данными о вероятности ложных срабатываний.
- **ID** – идентификатор, присваиваемый программой каждому правилу.
- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, по оценке специалистов "Лаборатории Касперского".
- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, по оценке специалистов "Лаборатории Касперского".

Удаление правил TAA (IOA) из исключений

Вы можете удалить из исключений одно или несколько правил TAA (IOA), а также все правила сразу.

► *Чтобы удалить правило TAA (IOA) из исключений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белые списки** и закладку **Исключения TAA (IOA)**.
2. Отобразится таблица правил TAA (IOA), добавленных в исключения.
3. Выберите правило, которое вы хотите удалить из исключений.

   Откроется окно с информацией о правиле.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Правило будет удалено из исключений. Правило будет применяться при создании обнаружений и при проверке событий.

► *Чтобы удалить все или несколько правил TAA (IOA) из исключений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белые списки** и

закладку **Исключения ТАА (IOA)**.

2. Отобразится таблица правил ТАА (IOA), добавленных в исключения.
3. Установите флажки напротив правил, которые вы хотите удалить из исключений.

   Вы можете выбрать все правила, установив флажок в строке с заголовками граф.
4. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из исключений. Правила будут применяться при создании обнаружений и при проверке событий.

Добавление правила ТАА (IOA) в исключения

Вы можете добавить в исключения только правила ТАА (IOA) "Лаборатории Касперского". Если вы не хотите применять при проверке событий пользовательское правила ТАА (IOA), вы можете отключить это правило (см. раздел "Включение и отключение использования правил ТАА (IOA)" на стр. 332) или удалить его (см. раздел "Удаление пользовательских правил ТАА (IOA)" на стр. 333).

► *Чтобы добавить правило ТАА (IOA) в исключения из раздела **Обнаружения**, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке в графе **Технологии** откройте окно настройки фильтрации.
3. В левом раскрывающемся списке выберите **Содержит**.
4. В правом раскрывающемся списке выберите технологию **(TAA) Targeted Attack Analyzer**.
5. Нажмите на кнопку **Применить**.

   В таблице отобразятся обнаружения, выполненные технологией ТАА на основе правил ТАА (IOA).
6. Выберите обнаружение, для которого в графе **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об обнаружении.
7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.
8. Справа от названия параметра **Исключения ТАА** нажмите на кнопку **Добавить в исключения**.

   Откроется окно добавления правила ТАА (IOA) в исключения.
9. Нажмите на кнопку **Добавить**.

Правило ТАА (IOA) будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса программы, подразделе **Белые списки** на закладке **Исключения ТАА (IOA)**. Это правило не будет применяться при создании обнаружений.

► *Чтобы добавить правило ТАА (IOA) в исключения из раздела **Поиск угроз**, выполните*

следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Задайте условия поиска и нажмите на кнопку **Найти**. Например, вы можете выбрать критерии для поиска событий в группе **Свойства ТАА** в режиме конструктора (см. раздел "Поиск событий с помощью режима конструктора" на стр. 251).

   Отобразится таблица событий, удовлетворяющих условиям поиска.

3. Выберите событие.

4. Справа от названия параметра **Имя IOA** нажмите на имя правила.

   Откроется окно с информацией о правиле.

5. Справа от названия параметра **Исключения ТАА** нажмите на кнопку **Добавить в исключения**.

   Откроется окно добавления правила ТАА (IOA) в исключения.

6. Нажмите на кнопку **Добавить**.

Правило ТАА (IOA) будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса программы, подразделе **Белые списки** на закладке **Исключения ТАА (IOA)**. Это правило не будет применяться при проверке событий.

Создание списка паролей для архивов

Программа не проверяет архивы, защищенные паролем. Вы можете создать список наиболее часто встречающихся паролей для архивов, которые используются при обмене файлами в вашей организации. В этом случае при проверке архива программа будет проверять пароли из списка. Если какой-либо из паролей подойдет, архив будет разблокирован и проверен.

Список паролей, заданный в параметрах программы, также передается на сервер с компонентом Sandbox.

► *Чтобы создать список паролей для архивов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пароли к архивам**.

2. В поле **Пароли к архивам** введите пароли, которые программа будет использовать для архивов, защищенных паролем.

   Вводите каждый пароль с новой строки. Вы можете ввести до 50 паролей.

3. Нажмите на кнопку **Применить**.

Список паролей для архивов будет создан. При проверке файлов формата PDF, а также файлов программ Microsoft Word, Excel, PowerPoint, защищенных паролем, программа будет подбирать пароли из заданного списка.

kaspersky

Управление программой Kaspersky Endpoint Agent

Kaspersky Endpoint Agent устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Программа осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами.

Kaspersky Endpoint Agent обеспечивает взаимодействие защищаемого устройства с другими решениями "Лаборатории Касперского" для обнаружения комплексных угроз (таких как таргетированные атаки).

Kaspersky Endpoint Agent 3.8, входящий в состав решения Kaspersky Endpoint Detection and Response Expert, поддерживает взаимодействие с Kaspersky Anti Targeted Attack Platform (KATA) и Kaspersky Sandbox.

Взаимодействие выполняется с помощью компонента KATA Central Node. При настроенной интеграции Kaspersky Endpoint Agent с KATA Central Node (см. раздел "Настройка интеграции Kaspersky Endpoint Agent с KATA Central Node" на стр. 413), программа выполняет задачи и применяет настройки, поступающие от компонента KATA Central Node, а также отправляет на сервер с компонентом KATA Central Node данные телеметрии с защищаемого устройства.

При настроенной интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox, программа обеспечивает коммуникацию EPP и программы Kaspersky Sandbox, а также выполнение действий по автоматическому реагированию на обнаруженные угрозы (см. раздел "Настройка действий Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox" на стр. 407) (например, запуск проверки важных областей на устройстве или помещение подозрительного объекта на карантин).

В этом разделе

kaspersky

Установка и удаление Kaspersky Endpoint Agent

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Agent на устройство, как обновить предыдущую версию программы и как удалить программу с устройства.

В этом разделе

Подготовка к установке Kaspersky Endpoint Agent

Перед установкой Kaspersky Endpoint Agent на устройство или обновлением предыдущей версии программы проверьте следующие условия:

- выполнение аппаратных и программных требований;
- наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление.

Установка Kaspersky Endpoint Agent

Установка Kaspersky Endpoint Agent может быть выполнена:

- локально с помощью Мастера установки (см. раздел "Установка Kaspersky Endpoint Agent с помощью Мастера установки" на стр. 390);
- локально с помощью командной строки (см. раздел "Установка и удаление программы с помощью командной строки" на стр. 391);
- удаленно с помощью Kaspersky Security Center (подробнее см. в справке Kaspersky Security Center);
- удаленно с помощью редактора управления групповыми политиками Microsoft Windows (подробнее см. на сайте Службы технической поддержки Microsoft).

При удаленной установке параметры установки можно передать при помощи конфигурационного файла install_props.json. Для это необходимо предварительно разместить файл install_props.json в одной папке с файлом endpointagent.msi.

Настройка параметров установки с помощью конфигурационного файла install_props.json недоступна, если этот файл был изменен вручную. Для изменения параметров установки создайте пользовательский пакет установки программы в Kaspersky Security Center или установите программу удаленно средствами групповых политик Microsoft Windows. Если вам требуется указать пароль для установки новой версии программы поверх старой, рекомендуется отключить парольную защиту на время установки программы.

Установка Kaspersky Endpoint Agent с помощью Мастера установки

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы.

► *Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы,*

скопируйте файл endpointagent.msi, входящий в комплект поставки, на устройство пользователя и запустите его.

Запустится мастер установки программы.

После установки программы Kaspersky Endpoint Agent на устройство, мастер установки может быть запущен на этом устройстве в одном из следующих режимов:

- **Изменение** (изменить параметры установленной программы).
- **Восстановление** (восстановить поврежденные модули программы).
- **Удаление** (удалить программу с устройства).

Обновление предыдущей версии Kaspersky Endpoint Agent

В процессе установки Kaspersky Endpoint Agent 3.8 на устройство с установленной предыдущей версией Kaspersky Endpoint Agent все данные, которые можно перенести, сохраняются и используются при установке Kaspersky Endpoint Agent 3.8, а предыдущая версия программы автоматически удаляется.

Если на устройстве установлен и используется Endpoint Sensor версии 3.6.X в составе Kaspersky Endpoint Security, рекомендуется отключить Endpoint Sensor перед установкой Kaspersky Endpoint Agent во избежание возможных конфликтов между программами.

При обновлении предыдущей версии Kaspersky Endpoint Agent, защищенной паролем, необходимо передать установщику этот пароль одним из следующих способов:

- При установке локально через интерфейс Мастера установки или в интерактивном режиме через командную строку указать пароль на соответствующем шаге.
- При установке локально через командную строку в неинтерактивном режиме указать пароль в качестве значения ключа `UNLOCK_PASSWORD`.
- При установке удаленно через Kaspersky Security Center передать текущий пароль в параметрах

инсталляционного пакета.

Удаление Kaspersky Endpoint Agent с помощью Мастера установки и удаления

Вы можете удалить Kaspersky Endpoint Agent стандартными средствами установки и удаления программ Microsoft Windows. Для удаления программы запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы.

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов, удаляются с устройства при удалении программы.

Установка и удаление программы с помощью командной строки

Kaspersky Endpoint Agent можно установить и удалить при помощи msi-пакета, задавая при этом значения свойств MSI стандартным образом. Подробная информация об использовании стандартных команд и ключей установщика Windows содержится в документации, предоставляемой корпорацией Microsoft.

Установка Kaspersky Endpoint Agent

Ниже приведен пример установки программы в неинтерактивном режиме с параметрами по умолчанию. После запуска установки программы в неинтерактивном режиме ваше участие в процессе установки не требуется.

Установка Kaspersky Endpoint Agent в неинтерактивном режиме требует принятия Лицензионного соглашения и Политики конфиденциальности. Используйте параметры `EULA=1` и `PRIVACYPOLICY=1`, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

Пример:

```
msiexec /i endpointagent.msi EULA=1 PRIVACYPOLICY=1 /qn
```

Удаление Kaspersky Endpoint Agent

Ниже приведен пример удаления программы в неинтерактивном режиме. После запуска удаления программы в неинтерактивном режиме ваше участие в процессе удаления не требуется.

Пример:

```
msiexec /i {2B71B95B-A56B-4B7C-AFFD-EB731B288EDF} REMOVE=ALL /qn
```

Если программа защищена паролем:

```
msiexec /i {2B71B95B-A56B-4B7C-AFFD-EB731B288EDF} REMOVE=ALL
UNLOCK_PASSWORD=<пароль> /qn
```

Все данные, которые программа хранит локально на устройстве, кроме файлов трассировки и дампов, удаляются с устройства при удалении программы.

kaspersky

Активация Kaspersky Endpoint Agent

Этот раздел содержит информацию об активации Kaspersky Endpoint Agent.

В этом разделе

kaspersky

Управление активацией Kaspersky Endpoint Agent

Вы можете активировать Kaspersky Endpoint Agent с помощью Консоли администрирования Kaspersky Security Center (см. раздел "Управление задачами активации Kaspersky Endpoint Agent" на стр. 427), используя задачу активации программы или через командную строку (см. раздел "Управление активацией Kaspersky Endpoint Agent" на стр. 453) локально на устройстве.

Информацию о действующей лицензии можно просмотреть в Kaspersky Security Center в разделе **Лицензии Лаборатории Касперского**, в свойствах устройства (см. раздел "Просмотр информации о действующей лицензии" на стр. 395) или через командную строку (см. раздел "Управление активацией Kaspersky Endpoint Agent" на стр. 453).

Подробную информацию об управлении лицензиями с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

После окончания срока действия лицензии программа продолжит работу в режиме ограниченной функциональности (см. раздел "Функциональные ограничения после окончания срока действия лицензии" на стр. 394).

Функциональные ограничения после окончания срока действия лицензии

Когда заканчивается срок действия текущей лицензии, возникают следующие ограничения в работе функциональных компонентов Kaspersky Endpoint Agent:

- Прекращается выполнение заданий от компонента Central Node и отправка результатов компоненту Central Node.

  Программа отправляет компоненту Central Node сообщение об изменении статуса активации Kaspersky Endpoint Agent.

  При этом соединение с компонентом Central Node не разрывается. Kaspersky Endpoint Agent продолжает принимать от компонента Central Node задания на создание задач и изменение параметров, но не запускает эти задачи и не включает сетевую изоляцию и функцию Запрет запуска.
- Прекращается отправка телеметрии.
- Невозможно включить сетевую изоляцию.

  Если сетевая изоляция была включена на момент окончания срока действия лицензии, программа отключает сетевую изоляцию в соответствии с заданными параметрами автоматического отключения сетевой изоляции.
- Невозможно включить функцию Запрет запуска.

  Если функция Запрет запуска была включена на момент окончания срока действия лицензии, программа прекращает блокирование объектов, которые подпадают под заданные правила запрета.
- Останавливаются и становятся недоступными для запуска следующие задачи: Получить файл, Запустить процесс, Завершить процесс, Удалить файл.
- Останавливаются и становятся недоступными для запуска стандартные задачи поиска IOC.
- Прекращается использование KSN/KPSN.

При попытке использования перечисленных функциональных компонентов программы после окончания

срока действия лицензии программа записывает критическое событие `LicenseViolation` в журнал событий Windows и в журнал Сервера администрирования Kaspersky Security Center. При работе через командную строку, программа возвращает код `8` (`AccessDenied`).

Просмотр информации о действующей лицензии

Информацию о действующей лицензии можно посмотреть в Kaspersky Security Center в разделе **Лицензии "Лаборатории Касперского"** или в свойствах устройства в разделе **Ключи**. Подробную информацию об управлении лицензиями с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

► *Чтобы посмотреть информацию о действующей лицензии на определенном устройстве, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите устройство, для которого вы хотите настроить параметры Kaspersky Endpoint Agent.
5. В контекстном меню устройства выберите пункт **Свойства**.

   Откроется окно свойств устройства.
6. Выберите раздел **Программы**.

   В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
7. Выберите программу Kaspersky Endpoint Agent и откройте окно ее свойств одним из следующих способов:
   - Двойным щелчком мыши по названию программы.
   - В контекстном меню программы выберите пункт **Свойства**.
   - Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".
8. Выберите раздел **Ключи**.

Информация о действующей лицензии отобразится в рабочей области окна.

kaspersky

Управление Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center

Программа Kaspersky Security Center предназначена для централизованного решения основных задач управления и обслуживания системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Agent, настраивать параметры работы программы, запускать и останавливать задачи программы. В Kaspersky Security Center предусмотрено разграничение прав доступа к Kaspersky Endpoint Agent, реализованное на основе технологии управления доступом на основе ролей (Role Based Access Control, RBAC).

Подробную информацию о Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Пользовательский интерфейс для работы с Kaspersky Security Center предоставляется с помощью компонента *Консоль администрирования Kaspersky Security Center* (далее также *Консоль администрирования*). Консоль администрирования реализована в виде компонента расширения к Консоли управления (Microsoft Management Console, MMC).

Управление Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center осуществляется с помощью *плагина управления Kaspersky Endpoint Agent*.

Далее в разделе приведена основная информация об управлении Kaspersky Endpoint Agent с помощью Консоли администрирования Kaspersky Security Center.

В этом разделе

Управление политиками Kaspersky Endpoint Agent

В этом разделе приведены инструкции по созданию политики Kaspersky Endpoint Agent и включению параметров в политике.

kaspersky

В этом разделе

Создание политики Kaspersky Endpoint Agent

► *Чтобы создать политику Kaspersky Endpoint Agent в Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Нажмите на кнопку **Создать политику**.

   Запустится мастер создания политики.
4. В окне **Ввод названия групповой политики** выполните следующие действия:
   a. Введите имя, под которым создаваемая политика будет отображаться в списке политик.
   b. Если вы хотите импортировать параметры существующей политики Kaspersky Endpoint Agent в новую политику, выполните следующие действия:
      1. Установите флажок **Использовать параметры политики для предыдущей версии программы**.
      2. Нажмите на кнопку **Выбрать** и в открывшемся окне выберите политику, параметры которой требуется импортировать.
      3. Нажмите на кнопку **ОК**.
   c. Нажмите на кнопку **Далее**.
5. В окне **Создать политику** выберите один из следующих вариантов и нажмите на кнопку **Далее**:
   - **Создать новую политику и настроить параметры**.
   - **Создать новую политику с параметрами по умолчанию**.

   Если на предыдущем шаге вы установили флажок **Использовать параметры политики для предыдущей версии программы**, то по умолчанию выбран вариант **Создать новую политику и настроить параметры**, а в процессе создания политики отображаются параметры, заданные в импортируемой политике. В этом случае положение переключателя применения политики в правом верхнем углу каждого из разделов с параметрами зависит от положения переключателей в блоках параметров импортируемой политики.
6. В окне **Выбрать тип политики** выберите необходимый способ развертывания Kaspersky Endpoint Agent, установив соответствующие флажки, и нажмите на кнопку **Далее**.
7. Если вы выбрали вариант **Создать новую политику и настроить параметры**, выполните одно из следующих действий во всех последовательно отображающихся окнах с параметрами:
   - Чтобы настроить параметры программы из отображаемых разделов во время создания политики:

a. Нажмите на кнопку **Настроить** рядом с названием необходимого раздела.

b. В открывшемся окне настройте необходимые параметры и нажмите на кнопку **ОК.**

c. Нажмите на кнопку **Далее**.

- Чтобы настроить параметры программы из отображаемых разделов позднее, нажмите на кнопку **Далее**.

Настройка параметров программы состоит из следующих этапов:

> Состав этапов зависит от выбранного на предыдущем шаге типа политики и может отличаться от приведенного ниже.

- Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox.
- Настройка интеграции Kaspersky Endpoint Agent с компонентом KATA Central Node.
- Настройка параметров реагирования на угрозы.
- Настройка репозиториев программы.
- Настройка параметров безопасности программы.
- Настройка общих параметров программы.

8. В окне **Целевая группа** выберите группу администрирования Kaspersky Security Center, на которую должна распространяться создаваемая политика, выполнив следующие действия:

   a. Нажмите на кнопку **Обзор**.

      Откроется окно выбора группы администрирования.

   b. Выберите группу администрирования в списке.

      Например, вы можете выбрать группу **Управляемые устройства**.

   c. Если вы хотите создать подгруппу устройств в группе **Управляемые устройства**, выполните следующие действия:

      1. Нажмите на кнопку **Новая группа**.
      2. В открывшемся окне введите имя подгруппы устройств.
      3. Нажмите на кнопку **ОК**.

   d. Нажмите на кнопку **Далее**.

9. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:

   - **Активная политика**, чтобы политика начала действовать сразу после создания.
   - **Неактивная политика**, чтобы активировать политику позже.

10. Установите флажок **Открыть свойства политики сразу после создания**, если требуется выполнить дополнительную настройку политики сразу после ее создания.

11. Нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик.

Включение параметров в политике Kaspersky Endpoint Agent

При настройке параметров политики Kaspersky Endpoint Agent по умолчанию значения параметров сохраняются, но не применяются до тех пор, пока вы их не включите.

Включение параметров доступно для блоков, в которых находятся эти параметры. В рамках одной политики вы можете включить как часть блоков параметров, так и все блоки параметров.

► *Чтобы включить блок параметров в политике Kaspersky Endpoint Agent, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. Выберите политику, для которой вы хотите включить параметры.
5. В открывшемся окне выберите раздел и блок параметров, к которым относятся нужные параметры.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

Все параметры блока будут применяться в политике.

kaspersky

Настройка параметров Kaspersky Endpoint Agent

В этом разделе приведены инструкции по настройке параметров Kaspersky Endpoint Agent с помощью плагина управления.

► *Чтобы открыть окно параметров Kaspersky Endpoint Agent, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
3. Выберите группу администрирования, для которой требуется настроить параметры программы.
4. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** двойным щелчком мыши по названию политики или выбрав пункт **Свойства** в контекстном меню.
   - Чтобы настроить параметры программы для отдельного устройства, выберите закладку **Устройства** и выполните следующие действия:
     a. Откройте окно **Свойства: <Название устройства>** двойным щелчком мыши по названию устройства или выбрав пункт **Свойства** в контекстном меню.
     b. Выберите раздел **Программы**.
     c. Откройте окно **Параметры: <Название программы>** двойным щелчком мыши по названию программы в рабочей области окна или нажав на кнопку **Свойства** под списком программ.

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

В этом разделе

kaspersky

Настройка параметров безопасности Kaspersky Endpoint Agent

Для обеспечения максимального уровня безопасности IT-инфраструктуры организации вы можете настроить доступ пользователей и сторонних процессов к Kaspersky Endpoint Agent. Для этого предусмотрены следующие возможности:

- Ограничение прав пользователей на управление параметрами и службами программы.
- Защита действий в программе паролем.
- Механизм самозащиты программы.

В этом разделе

Настройка прав пользователей

Вы можете предоставить доступ к Kaspersky Endpoint Agent для отдельных пользователей или групп пользователей. В результате только заданные пользователи смогут управлять параметрами или службами программы.

► *Чтобы настроить права пользователей, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
5. В блоке параметров **Права пользователей** нажмите на кнопку **Настроить** рядом с названием нужного параметра.

   Откроется окно разрешений для группы Kaspersky Endpoint Agent.
6. В верхнем блоке параметров групп или пользователей выберите группу или пользователя, которому вы хотите предоставить права.
7. В нижнем блоке параметров разрешений для групп или пользователей установите флажки в строках с требуемыми правами.
8. Нажмите на кнопку **OK**.
9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
10. В окне свойств политики нажмите на кнопку **OK**.

Права пользователей на управление параметрами и службами программы будут настроены.

Включение защиты паролем

Неограниченный доступ пользователей к программе и ее параметрам может привести к снижению уровня безопасности устройства. Защита паролем позволяет ограничить доступ пользователей к программе.

► *Чтобы включить защиту паролем, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
5. В блоке параметров **Защита паролем** установите флажок **Применить защиту паролем**.
6. Задайте пароль и подтвердите его.

   Рекомендуется задать пароль, который удовлетворяет следующим условиям:
   - Длина пароля должна быть не менее 8 символов.
   - Пароль не должен содержать имени учетной записи пользователя.
   - Пароль не должен совпадать с именем устройства, на котором установлена программа Kaspersky Endpoint Agent.
   - Пароль должен содержать символы как минимум трех групп из следующего списка:
     - верхний регистр (A-Z);
     - нижний регистр (A-Z) (a-z);
     - цифры (0-9);
     - специальные символы (!$#%).
7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
8. Нажмите на кнопку **ОК**.

Защита паролем будет включена. При попытке пользователя выполнить действие, защищенное паролем, программа предложит пользователю ввести пароль.

Программа не проверяет надежность заданного пароля. Рекомендуется использовать сторонние средства для проверки надежности пароля. Пароль считается надежным, если по результатам проверки подтверждена невозможность подбора пароля минимум за 6 месяцев.

Программа не блокирует возможность ввода пароля после множества попыток ввода некорректного пароля.

Включение и отключение механизма самозащиты

Для защиты от вредоносных программ, которые пытаются заблокировать работу Kaspersky Endpoint Agent или удалить программу, в программе реализован механизм самозащиты. Этот механизм предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

► *Чтобы включить или отключить механизм самозащиты, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
5. В блоке параметров **Самозащита** выполните одно из следующих действий:
   - Установите флажок **Включить самозащиту модулей программы в памяти**, чтобы включить механизм самозащиты.
   - Снимите флажок **Включить самозащиту модулей программы в памяти**, чтобы отключить механизм самозащиты.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **ОК**.

Механизм самозащиты будет включен или отключен.

Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером

Параметры соединения с прокси-сервером используются для обновления баз, активации программы и работы внешних служб.

Если вы используете Nginx в качестве прокси-сервера, настройте параметр `client_max_body_size`: значение параметра `client_max_body_size` должно быть равно максимальному размеру объекта, отправляемого программой Kaspersky Endpoint Agent на обработку в программу Kaspersky Sandbox. Иначе Nginx не будет пропускать объекты, размер которых превышает установленное значение. Значение по умолчанию – 1 МБ.

► *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Параметры программы** выберите подраздел **Другие параметры**.
5. Выберите один из следующих вариантов использования прокси-сервера:
   - **Не использовать прокси-сервер**.
   - **Использовать прокси-сервер с указанными параметрами**.
6. Если вы выбрали вариант**Использовать прокси-сервер с указанными параметрами**, в полях **Имя или IP-адрес сервера** и **Порт** введите адрес и порт прокси-сервера, соединение с которым вы хотите установить.

   По умолчанию используется порт 8080.
7. Если вы хотите использовать NTLM-аутентификацию при подключении к прокси-серверу, выполните следующие действия:
   a. Установите флажок **Использовать NTLM-аутентификацию по имени пользователя и паролю**.
   b. В поле **Имя пользователя** введите имя пользователя, учетная запись которого будет использоваться для авторизации на прокси-сервере.
   c. В поле **Пароль** введите пароль подключения к прокси-серверу.

      Вы можете включить отображение символов пароля, нажав на кнопку **Показать** справа от поля **Пароль**.
8. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.
9. Нажмите на кнопку **Применить**.

   При этом вы вернетесь в окно свойств политики.
10. В правом верхнем углу блока параметров измените положение переключателя с с **Политика не применяется** на **Политика применяется**.
11. Нажмите на кнопку **OK**.

Параметры соединения с прокси-сервером будут настроены.

Настройка использования KSN и KMP в Kaspersky Endpoint Agent

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Agent использует данные, полученные от пользователей во всем мире. Сеть Kaspersky Security Network предназначена для получения этих данных.

Kaspersky Security Network (далее также KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Web Traffic Security на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, информация о которых еще не вошла в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы.

Во время участия в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Endpoint Agent, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Kaspersky Managed Protection (далее также KMP) – это операционный сервис активного поиска киберугроз, направленных на вашу организацию. В рамках оказания сервиса эксперты Центра мониторинга кибербезопасности «Лаборатории Касперского» осуществляют анализ расширенной телеметрии с установленных в сетях заказчика продуктов Kaspersky Security для бизнеса и Kaspersky Anti Targeted Attack, выступающих в качестве сенсоров. Полученная информация агрегируется с использованием Kaspersky Security Network и исследуется аналитиками на основе данных об угрозах (Threat intelligence), собранных «Лабораторией Касперского» за все время деятельности, что позволяет обнаружить актуальные тактики, техники и процедуры злоумышленников.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Endpoint Agent передает в Kaspersky Security Network и в Kaspersky Managed Protection, вы можете прочитать в Положении о KSN и в Положении о KMP.

Участие в Kaspersky Security Network и Kaspersky Managed Protection добровольное. По умолчанию использование KSN и KMP отключено. После включения использования KSN и KMP, вы можете отключить эту опцию в любой момент времени.

► *Чтобы включить использование KSN и KMP, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. Выберите раздел **Участие в KSN и KMP**.
5. Ознакомьтесь с Положением о KSN.
6. Если вы согласны с условиями Положения, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Положения о KSN**.

7. Установите флажок **Включить использование Kaspersky Security Network**.
8. Если вы хотите включить использование KMP, выполните следующие действия:
    a. Ознакомьтесь с Положением о KMP.
    b. Если вы согласны с условиями Положения, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Положения о KMP**.
    c. Установите флажок **Включить использование Kaspersky Managed Protection**.
9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
10. Нажмите на кнопку **OK**.

Использование KSN и KMP будет включено.

Настройка действий Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox

Kaspersky Endpoint Agent может выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox.

Вы можете настроить действия следующих типов:

- *Локальные* – действия, которые будут выполняться на каждом устройстве, на котором обнаружена угроза.
- *Групповые* – действия, которые будут выполняться на всех устройствах группы администрирования, для которой вы настраиваете политику.

Локальные действия:

- **Поместить на карантин и удалить**.

  При обнаружении угрозы на устройстве копия объекта, содержащего угрозу, будет помещена на карантин, а объект будет удален с устройства.

- **Уведомить пользователя устройства**.

  При обнаружении угрозы на устройстве пользователю устройства будет показано уведомление об обнаруженной угрозе.

  > Уведомление отображается, если устройство работает под учетной записью пользователя, под которой была обнаружена угроза.
  > Если устройство выключено или выполнен вход под другой учетной записью, уведомление не отображается.

- **Дать команду Endpoint Protection Platform (EPP) на проверку важных областей**.

  При обнаружении угрозы на устройстве Kaspersky Endpoint Agent отправляет команду программе EPP на выполнение проверки важных областей этого устройства. К важным областям относится память ядра, объекты, загружаемые при запуске операционной системы, и загрузочные секторы жесткого диска. Подробнее о настройке параметров проверки см. в документации к используемой EPP.

Групповые действия:

- **Запустить поиск IOC по управляемой группе устройств**.

  При обнаружении угрозы на любом из устройств группы администрирования, для которой вы настраиваете политику, Kaspersky Endpoint Agent проверяет все устройства этой группы администрирования на наличие объекта, содержащего обнаруженную угрозу.

- **Поместить на карантин и удалить при обнаружении IOC**.

  При обнаружении угрозы на любом из устройств группы администрирования, для которой вы настраиваете политику, Kaspersky Endpoint Agent проверяет все устройства этой группы администрирования на наличие объекта, содержащего обнаруженную угрозу. При обнаружении объекта, содержащего угрозу, на каких-либо устройствах этой группы администрирования копия этого объекта будет помещена на карантин, а объект будет удален с устройств.

- **Дать команду Endpoint Protection Platform (EPP) на проверку важных областей при обнаружении IOC**.

  При обнаружении угрозы на любом из устройств группы администрирования, для которой вы

настраиваете политику, Kaspersky Endpoint Agent отправляет команду программе EPP на выполнение проверки важных областей на всех устройствах этой группы администрирования, на которых обнаружен объект, содержащий угрозу. Подробнее о настройке параметров проверки см. в документации к используемой EPP.

Для настройки групповых действий по реагированию на угрозы необходимо настроить права пользователей Kaspersky Security Center, под учетными записями которых вы хотите управлять задачами поиска IOC.

При настройке действий по реагированию на угрозы учитывайте, что в результате выполнения некоторых из настроенных действий объект, содержащий угрозу, может быть удален с рабочей станции, на которой он был обнаружен.

В этом разделе

Включение и отключение выполнения действий по реагированию на угрозы

► *Чтобы включить или отключить выполнение программой Kaspersky Endpoint Agent действий по реагированию на угрозы, обнаруженные Kaspersky Sandbox, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Действия**:
   - Установите флажок **Выполнять действия по реагированию на угрозы, обнаруженные**

Kaspersky Sandbox, чтобы включить выполнения действий по реагированию на угрозы.

- Снимите флажок **Выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox**, чтобы отключить выполнения действий по реагированию на угрозы.

6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопки **Применить** и **ОК**.

Добавление действий по реагированию на угрозы в список действий текущей политики

► *Чтобы добавить действия по реагированию на угрозы в список действий текущей политики, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Действия** установите флажок **Выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox**, если он не установлен.
6. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите одно из следующих действий:
   - **Поместить на карантин и удалить**. Локальное действие. Выполняется на устройстве, на котором обнаружена угроза.
   - **Уведомить пользователя устройства**. Локальное действие. Выполняется на устройстве, на котором обнаружена угроза.
   - **Дать команду Endpoint Protection Platform (EPP) на проверку важных областей**. Локальное действие. Выполняется на устройстве, на котором обнаружена угроза.
   - **Запустить поиск IOC по управляемой группе устройств**. Групповое действие. Выполняется на всех устройствах группы администрирования.
   - **Поместить на карантин и удалить при обнаружении IOC**. Групповое действие. Выполняется на всех устройствах группы администрирования.
   - **Дать команду Endpoint Protection Platform (EPP) на проверку важных областей при обнаружении IOC**. Групповое действие. Выполняется на всех устройствах группы администрирования.

   Действие будет добавлено в список **Текущие действия**.

   При настройке действий по реагированию на угрозы учитывайте, что в результате выполнения некоторых из настроенных действий объект, содержащий угрозу, может быть удален с рабочей станции, на которой он был обнаружен.

7. Если вы хотите удалить действие, выберите его в таблице и нажмите на кнопку **Удалить**.
8. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
9. Нажмите на кнопки **Применить** и **ОК**.

Аутентификация на Сервере администрирования для групповых задач по реагированию на угрозы

Если вы хотите, чтобы программа Kaspersky Endpoint Agent создавала групповые задачи по реагированию на угрозы, необходимо выполнить аутентификацию на Сервере администрирования: указать имя пользователя и пароль подключения к Kaspersky Security Center.

Вы можете выполнить аутентификацию с правами учетной записи внутреннего пользователя Kaspersky Security Center, созданной в Kaspersky Security Center, или использовать аутентификацию Windows.

Подробная информация о создании учетных записей Kaspersky Security Center и аутентификации Windows приведена в *Справке Kaspersky Security Center*.

Имя учетной записи не должно совпадать с доменным именем пользователя и не должно быть указано в формате `<имя домена>\<имя пользователя>`.

► *Чтобы пройти аутентификацию на Сервере администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Аутентификация на Сервере администрирования** в поле **Имя пользователя Сервера администрирования** введите имя учетной записи пользователя Kaspersky Security Center.
6. В блоке параметров **Аутентификация на Сервере администрирования** в поле **Пароль для Сервера администрирования** введите пароль доступа к Kaspersky Security Center.
7. В правом верхнем углу блока параметров измените положение переключателя с с **Политика не применяется** на **Политика применяется**.
8. Нажмите на кнопку **ОК**.

Защита устройств от легальных программ, которые могут быть использованы злоумышленниками

Вы можете включить обнаружение легальных программ, которые могут быть использованы

злоумышленниками для нанесения вреда локальной сети вашей организации. Kaspersky Endpoint Agent будет расценивать такие программы как представляющие угрозу и выполнять над ними действия по реагированию на угрозы.

Легальные программы – программы, разрешенные к установке и использованию на устройствах и предназначенные для выполнения пользовательских задач. Однако легальные программы некоторых типов при использовании злоумышленниками могут нанести вред устройству или локальной сети организации. Если злоумышленники получат доступ к таким программам или внедрят их на устройстве, они могут использовать отдельные функции этих программ для нарушения безопасности устройства или локальной сети организации.

К таким программам относятся: IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

► *Чтобы включить обнаружение потенциально опасных легальных программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Дополнительные параметры** установите флажок **Включить обнаружение легальных программ, которые могут быть использованы злоумышленниками**.
6. В правом верхнем углу блока параметров измените положение переключателя с с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопки **Применить** и **ОК**.

Обнаружение легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда локальной сети вашей организации, будет включено.

Настройка запуска автономных задач поиска IOC

Когда программа Kaspersky Sandbox обнаруживает угрозу, в Kaspersky Endpoint Agent автоматически создаются задачи поиска IOC (MD5-хешей объектов, в которых была обнаружена угроза) по всем устройствам.

► *Чтобы настроить запуск автономных задач поиска IOC, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.

- В контекстном меню политики выберите пункт **Свойства**.
- В правой части окна выберите пункт **Настроить параметры политики**.

4. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
5. В блоке параметров **Дополнительные параметры** нажмите на кнопку **Настроить**.

   Откроется окно **Параметры поиска IOC**.
6. В блоке параметров **Области поиска** выберите одну из следующих областей, в которых Kaspersky Endpoint Agent будет выполнять поиск IOC:
   - **Файловые области, содержащие системные диски**.
   - **Критические файловые области**.
7. В блоке параметров **Запуск поиска** выберите один из следующих вариантов запуска задач поиска IOC:
   - **Вручную**. Задачи поиска IOC будут создаваться автоматически, но не будут запускаться. Вы сможете запускать вручную отдельную задачу или все задачи.
   - **Сразу по факту обнаружения Kaspersky Sandbox**. Задачи поиска IOC будут автоматически создаваться и запускаться.
   - **В заданный период**. Задачи поиска IOC будут создаваться автоматически, а запускаться в заданный период. Например, в нерабочее время с 20:00 до 7:00.

     Если вы выбрали вариант **В заданный период**, в полях **Начало периода (чч:мм)** и **Конец периода (чч:мм)** укажите начало и конец периода.

     Все задачи поиска IOC, автоматически созданные *до начала* указанного периода, запустятся в произвольное время *в рамках* указанного периода.
     Все задачи поиска IOC, автоматически созданные *в рамках* указанного периода, запустятся *сразу после* создания.
     Все задачи поиска IOC, автоматически созданные *после окончания* указанного периода, запустятся *при следующем наступлении* указанного периода.

Пример:

Если вы настроили запуск задач в период с 20:00 до 7:00:

Задачи, автоматически созданные в 19:00, запустятся в произвольное время с 20:00 до 7:00.

Задачи, автоматически созданные в 21:00, запустятся в 21:00.

Задачи, автоматически созданные в 8:00, запустятся при следующем наступлении периода, с 20:00 до 7:00.

8. Нажмите на кнопку **OK**.

   Окно **Параметры поиска IOC** закроется.
9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
10. Нажмите на кнопки **Применить** и **OK**.

Запуск автономных задач поиска IOC будет настроен.

kaspersky

Настройка интеграции Kaspersky Endpoint Agent с KATA Central Node

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с компонентом KATA Central Node с помощью Консоли администрирования Kaspersky Security Center.

В этом разделе

Настройка общих параметров передачи телеметрии

► *Чтобы настроить общие параметры телеметрии, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Интеграция с сервером сбора данных и реагирования** выберите подраздел **Общие**.
5. В блоке параметров **Общие параметры передачи телеметрии** выполните одно из следующих действий:
   - Укажите значения в поле **Период передачи события (сек.)**.
   - Укажите значения в поле **Лимит событий в одном пакете**.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **OK**.

Включение и отключение интеграции с KATA Central Node

► *Чтобы включить или отключить интеграцию с компонентом KATA Central Node, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.

- В контекстном меню политики выберите пункт **Свойства**.
- В правой части окна выберите пункт **Настроить параметры политики**.

4. В разделе **Интеграция с KATA** выберите подраздел **KATA Central Node**.
5. В блоке параметров **Параметры подключения** выполните одно из следующих действий:
   - Чтобы включить интеграцию с KATA Central Node, выполните следующие действия:
     a. Установите флажок **Включить интеграцию с KATA**.
     b. Укажите IP-адрес или полное доменное имя сервера KATA, а также порт подключения к серверу.
   - Чтобы отключить интеграцию с KATA Central Node, снимите флажок **Включить интеграцию с KATA**.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **OK**.

Интеграция с KATA Central Node будет включена или отключена.

Настройка доверенного соединения с KATA Central Node

► *Чтобы настроить доверенное соединение Kaspersky Endpoint Agent с KATA Central Node, выполните следующие действия на стороне Kaspersky Endpoint Agent:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Интеграция с KATA** выберите подраздел **KATA Central Node**.
5. В блоке параметров **Параметры подключения** установите флажок **Использовать доверенное соединение**.
6. Нажмите на кнопку **Добавить TLS-сертификат**.

   Откроется окно **Добавление TLS-сертификата**.
7. Выполните одно из следующих действий по добавлению TLS-сертификата:
   - Добавьте файл сертификата. Для этого нажмите на кнопку **Обзор**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Открыть**.
   - Скопируйте содержимое файла сертификата в поле **Вставьте данные TLS-сертификата**.

В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера KATA. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

8. Нажмите на кнопку **Добавить**.

   Информация о добавленном TLS-сертификате отобразится в блоке параметров **Данные TLS-сертификата**.

9. Если вы хотите настроить дополнительную защиту подключения с использованием пользовательского сертификата, нажмите на кнопку **Дополнительная защита подключения**.
10. В открывшемся окне **Дополнительная защита подключения** выполните следующие действия:
    a. Установите флажок **Защита подключения с помощью клиентского сертификата**.
    b. Нажмите на кнопку **Загрузить**, в открывшемся окне выберите архив формата PFX и нажмите на кнопку **Открыть**.
    c. Введите пароль к архиву формата PFX.
    d. Нажмите на кнопку **ОК**.
11. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
12. Нажмите на кнопку **ОК**.

Доверенное соединение с сервером KATA будет настроено.

Настройка параметров синхронизации Kaspersky Endpoint Agent с KATA Central Node

► *Чтобы настроить параметры синхронизации Kaspersky Endpoint Agent с KATA Central Node, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Интеграция с KATA** выберите подраздел **KATA Central Node**.
5. В блоке параметров **Параметры подключения** настройте следующие параметры:
   - **Время ожидания (сек.)**. Укажите максимальное время ожидания ответа от сервера KATA.
   - **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)**. Укажите период отправки запросов на синхронизацию параметров и задач Kaspersky Endpoint Agent с KATA Central Node. Можно указать значение в пределе от 1 до 60 минут.
6. Установите или снимите флажок **Использовать кеш события**.
7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не**

применяется на **Политика применяется**.

8. Нажмите на кнопку **OK**.

Настройка параметров карантина в Kaspersky Endpoint Agent

В этом разделе приведены инструкции по настройке параметров карантина с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

О карантине Kaspersky Endpoint Agent

Карантин – это специальное локальное хранилище на устройстве с программой Kaspersky Endpoint Agent, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

По умолчанию локальное хранилище карантина расположено в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Quarantine`. По умолчанию объекты, восстановленные из карантина, хранятся в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Restored`.

Kaspersky Security Center формирует общий список объектов, помещенных на карантин на устройствах с программой Kaspersky Endpoint Agent. Агенты администрирования устройств передают информацию о файлах на карантине на Сервер администрирования.

Kaspersky Security Center не копирует файлы из карантина на Сервер администрирования. Все объекты находятся на защищаемых устройствах с программой Kaspersky Endpoint Agent. Восстановление объектов из карантина также выполняется на защищаемых устройствах.

Об управлении карантином в Kaspersky Endpoint Agent

Через Kaspersky Security Center можно настраивать параметры карантина (см. раздел "Настройка параметров карантина в Kaspersky Endpoint Agent" на стр. 416), просматривать свойства объектов, находящихся на карантине на защищаемых устройствах, запускать проверку этих объектов, удалять объекты, находящиеся на карантине, а также восстанавливать объекты из карантина. Подробную информацию об управлении объектами, находящимися на карантине, через Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Для того чтобы Kaspersky Endpoint Agent отправлял данные об объектах, помещенных на карантин, на Сервер администрирования Kaspersky Security Center, необходимо включить эту опцию (см. раздел "Настройка синхронизации данных с Сервером администрирования" на стр. 418) в параметрах карантина в политике Kaspersky Endpoint Agent. По умолчанию опция включена.

Через интерфейс командной строки на устройстве можно просматривать информацию о параметрах карантина и свойствах объектов, находящихся на карантине (см. раздел "Просмотр информации о параметрах карантина и объектах на карантине" на стр. 456).

Объект помещается на карантин под системной учетной записью (SYSTEM).

Удаление объектов, помещенных на карантин, через командную строку доступно только под локальной учетной записью пользователя защищаемого устройства.

Настройка параметров карантина и восстановления объектов из карантина

► *Чтобы настроить параметры карантина, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Репозитории** выберите подраздел **Карантин**.
5. В разделе **Параметры карантина** настройте параметры карантина:
   a. В поле **Папка карантина** укажите путь, по которому будет создана папка карантина на устройствах, или нажмите на кнопку **Обзор** и выберите путь.

      По умолчанию используется путь `%SOYUZAPPDATA%\Quarantine\`. Папка Quarantine будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

      Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent.

Пример:

Если на устройстве установлена операционная система Windows 7 и программа Kaspersky Endpoint Agent установлена на диске C, путь к папке карантина будет следующим:

```
C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Quarantine
```

   b. Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер**

Карантина (МБ) и укажите или выберите в списке максимальный размер карантина в МБ.

Например, вы можете задать максимальный размер карантина 200 МБ.

При достижении максимального размера карантина Kaspersky Endpoint Agent публикует соответствующе событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

c. Чтобы задать пороговое значение карантина (место в карантине, оставшееся до достижения максимального размера карантина), установите флажок **Пороговое значение места на диске (МБ)**.

Например, вы можете задать пороговое значение карантина 50 МБ.

При достижении порогового значения карантина, Kaspersky Endpoint Agent публикует соответствующе событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

6. В разделе **Восстановление объектов из Карантина** в поле **Папка для восстановленных объектов** укажите путь, по которому будет создана папка для объектов, восстановленных из карантина.

По умолчанию используется путь `%SOYUZAPPDATA%\Restored\`. Папка Restored будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent.

Пример:

Если на устройстве установлена операционная система Windows 7 и программа Kaspersky Endpoint Agent установлена на диске C, путь к папке восстановленных из карантина объектов будет следующим:

`C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored`

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
8. Нажмите на кнопки **Применить** и **ОК**.

Параметры карантина и папка для восстановления объектов из карантина будут настроены.

Настройка синхронизации данных с Сервером администрирования

Вы можете настроить синхронизацию данных об объектах, помещенных на карантин на управляемых устройствах, с Сервером администрирования Kaspersky Security Center.

► *Чтобы настроить синхронизацию данных с Сервером администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.

- В контекстном меню политики выберите пункт **Свойства**.
- В правой части окна выберите пункт **Настроить параметры политики**.

4. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.
5. В разделе **Параметры**, в подразделе **Отправить следующие данные на Сервер администрирования** установите флажок **Данные об объектах в Карантине на управляемых устройствах**.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопки **Применить** и **ОК**.

Синхронизация данных с Сервером администрирования будет настроена.

Настройка параметров сетевой изоляции

В этом разделе приведены инструкции по настройке параметров сетевой изоляции с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

О сетевой изоляции в Kaspersky Endpoint Agent

Kaspersky Endpoint Agent предоставляет возможность изолировать устройства от сети по требованию (вручную) или автоматически, в результате ответных действий на обнаружения.

После включения сетевой изоляции программа разрывает все активные и блокирует все новые сетевые соединения TCP/IP на устройствах, кроме следующих соединений:

- соединения, указанные в исключениях из сетевой изоляции;
- соединения, инициированные службами совместимого EPP;
- соединения, инициированные службами Kaspersky Endpoint Agent;
- соединения, инициированные Агентом администрирования Kaspersky Security Center.

Включение и отключение сетевой изоляции

Сетевая изоляция устройства может быть включена вручную или автоматически, в результате ответных действий на обнаружения (см. раздел «Настройка параметров стандартной задачи поиска IOC» на стр.

444).

Сетевая изоляция может быть отключена автоматически по истечении заданного периода времени или вручную.

Если в параметрах сетевой изоляции не установлен флажок **Автоматически прекращать изоляцию устройства по истечении** и не указан период времени, сетевая изоляция будет отключена автоматически через пять часов с момента включения.

После отключения сетевой изоляции устройство может работать в сети без ограничений, наложенных Kaspersky Endpoint Agent при сетевой изоляции.

Исключения из сетевой изоляции

Вы можете задать исключения из сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на устройствах после включения сетевой изоляции.

Для упрощения настройки исключений из сетевой изоляции в программе доступен список сетевых профилей (наборы стандартных правил исключения). Редактирование списка и содержания сетевых профилей не предусмотрено.

Исключения можно задать как в составе сетевых профилей, так и отдельно. Исключения, заданные отдельно от сетевых профилей, называются *пользовательскими*.

По умолчанию в исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент.

При изменении параметров исключения, заданного при помощи сетевого профиля, это исключение становится пользовательским.

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена программой автоматически, в результате реагирования на обнаружение. Исключения, заданные в свойствах устройства, применятся, только если сетевая изоляция включена вручную.
Активная политика не блокирует применение исключений из сетевой изоляции, заданных в свойствах устройства, так как сценарии применения этих параметров разные.

Об управлении сетевой изоляцией в Kaspersky Endpoint Agent

Вы можете управлять сетевой изоляцией с помощью Сервера администрирования Kaspersky Security Center, через интерфейс компонента Central Node или через интерфейс командной строки на защищаемом устройстве. Информация о возможностях управления сетевой изоляцией каждым из перечисленных способов приведена в следующей таблице.

Таблица 18. Управление сетевой изоляцией

Интерфейс управления	Возможности	Примечания

Интерфейс управления	Возможности	Примечания
Консоль администрирования Kaspersky Security Center	• Включение и отключение сетевой изоляции (на стр. 421). • Настройка автоматического отключения сетевой изоляции (на стр. 422). • Настройка уведомления пользователя устройства о сетевой изоляции (см. раздел "Включение и отключение уведомления пользователя о сетевой изоляции" на стр. 422). • Настройка исключений из сетевой изоляции (на стр. 423).	В свойствах политики настраиваются параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную). Включение и отключение сетевой изоляции вручную для группы устройств через политику недоступно.
Командная строка	• Получение информации о текущем состоянии и параметрах сетевой изоляции устройства (см. раздел "Управление сетевой изоляцией" на стр. 467).	Включение и отключение сетевой изоляции, а также настройка ее параметров недоступны через интерфейс командной строки.
Компонент Central Node	Управление сетевой изоляцией через компонент Central Node описано отдельно.	Kaspersky Endpoint Agent сохраняет параметры сетевой изоляции, полученные от компонента Central Node, в свойствах устройства в Kaspersky Security Center.

Включение и отключение сетевой изоляции

► *Чтобы включить или отключить сетевую изоляцию устройства, выполните следующие действия:*

1. Откройте окно свойств программы для отдельного устройства.
2. В разделе **Сетевая изоляция** выберите **Общие**.
3. В блоке параметров **Изолировать устройство** установите или снимите флажок **Изолировать выбранное устройство от сети**.
4. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Включение и отключение сетевой изоляции вручную для группы устройств через политику недоступно.

Включение и отключение уведомления пользователя о сетевой изоляции

В свойствах политики настраиваются параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

► *Чтобы включить или отключить уведомление пользователя о сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. В разделе **Сетевая изоляция** выберите **Общие**.
3. В блоке параметров **Уведомление** установите или снимите флажок **Уведомить пользователя, когда устройство будет изолировано]**.
4. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Настройка автоматического отключения сетевой изоляции

В свойствах политики настраиваются параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

► *Чтобы настроить параметры автоматического отключения сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. В разделе **Сетевая изоляция** выберите **Общие**.
3. В блоке параметров **Условия изоляции устройства** выполните одно их следующих действий:
   - Снимите флажок **Автоматически прекращать изоляцию устройства по истечении**, чтобы выключить функцию автоматического отключения сетевой изоляции по истечении заданного периода времени.

     По умолчанию функция включена.
   - Установите флажок **Автоматически прекращать изоляцию устройства по истечении**, чтобы включить функцию автоматического отключения сетевой изоляции по истечении заданного периода.
4. Задайте период, по истечении которого сетевая изоляция должна быть отключена.

   По умолчанию задан период в 30 минут.
5. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Если в параметрах сетевой изоляции не установлен флажок **Автоматически прекращать изоляцию устройства по истечении** и не указан период времени, сетевая изоляция будет отключена автоматически через пять часов с момента включения.

Настройка исключений из сетевой изоляции

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена программой автоматически, в результате реагирования на обнаружение. Исключения, заданные в свойствах устройства, применятся, только если сетевая изоляция включена вручную.
Активная политика не блокирует применение исключений из сетевой изоляции, заданных в свойствах устройства, так как сценарии применения этих параметров разные.

► *Чтобы настроить параметры исключения из сетевой изоляции:*

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
   - Откройте окно свойств политики программы.
2. Если вы открыли окно свойств программы для отдельного устройства, то в разделе **Сетевая изоляция** выберите **Правила исключения**.
3. Если вы открыли окно свойств политики программы, то в разделе **Сетевая изоляция** выберите **Изоляция при обнаружении**.
4. Вы можете выполнить следующие действия:
   - Добавить пользовательское исключение
   - Добавить исключения из списка стандартных сетевых профилей
   - Изменить параметры добавленного исключения
   - Включить или отключить использование исключения
   - Удалить исключение из списка
5. Чтобы сохранить изменения, нажмите на кнопку **Применить**.

kaspersky

Управление задачами Kaspersky Endpoint Agent

В этом разделе приведены инструкции по управлению задачами Kaspersky Endpoint Agent.

В этом разделе

Создание локальной задачи

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Управляемые устройства**.
3. В папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входит требуемое устройство.
4. В рабочей области выберите закладку **Устройства**.
5. Выберите устройство, для которого вы хотите создать локальную задачу.
6. Выполните одно из следующих действий:
   - В контекстном меню устройства выберите пункт **Все задачи** → **Создать задачу**.
   - В контекстном меню устройства выберите пункт **Свойства** и в открывшемся окне **Свойства: <Название устройства>** на закладке **Задачи** нажмите на кнопку **Добавить**.
   - В раскрывающемся списке **Выполнить действие** выберите элемент **Создать задачу**.

   Запустится мастер создания задачи.
7. Выберите нужную задачу и нажмите **Далее**.
8. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать групповую задачу для всех устройств, управляемых с помощью программы

Kaspersky Security Center.

- В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят требуемые устройства.

3. В рабочей области выберите закладку **Задачи**.
4. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
5. Выберите нужную задачу и нажмите **Далее**.
6. Следуйте указаниям мастера создания задачи.

Просмотр списка задач

► *Чтобы просмотреть список задач на сервере Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

Отобразится список задач.

Удаление задач из списка

► *Чтобы удалить задачи из списка задач на сервере Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.
3. В списке задач выберите задачи, которые вы хотите удалить, и правой клавишей мыши откройте контекстное меню.

   Отобразится список действий, которые можно выполнить над задачами.
4. Выберите действие **Удалить**.

   Откроется окно подтверждения действия.
5. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены из списка.

Запуск задач вручную

► *Чтобы вручную запустить одну задачу, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В контекстном меню нужной задачи выберите действие **Запустить**.

Задача запустится.

Просмотр результатов выполнения задач

Вы можете просмотреть результаты выполнения задач в течение срока их хранения. Можно изменить срок хранения результатов выполнения задач.

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

► *Чтобы просмотреть результат выполнения задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. В меню выберите пункт **Результаты**.

Откроется окно **Результат выполнения задачи**.

Изменение срока хранения результатов выполнения задач на Сервере администрирования

По умолчанию результаты выполнения задач хранятся на Сервере администрирования в течение семи дней.

► *Чтобы изменить срок хранения результатов выполнения задач на Сервере администрирования, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел **Уведомление**.
6. Убедитесь, что в разделе **Сохранять информацию о результатах** установлен флажок **На Сервере администрирования в течение (сут)** и укажите, в течение какого времени (в сутках) требуется хранить результат выполнения задачи.
7. Нажмите на кнопки **Применить** и **ОК**.

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

kaspersky

Управление задачами активации Kaspersky Endpoint Agent

Вы можете активировать Kaspersky Endpoint Agent с помощью ключа или кода активации.

При активации с помощью кода активации данные отправляются на сервер активации для проверки введенного кода.

Для активации программы с помощью кода активации защищаемое устройство должно быть подключено к интернету.

► *Чтобы создать задачу активации Kaspersky Endpoint Agent, выполните следующие действия:*

1. Запустите мастер создания задачи **Активация программы** для нужной области действия одним из следующих способов:
   - Запустите мастер создания локальной задачи.
   - Запустите мастер создания групповой задачи.
2. Если вы хотите активировать программу с помощью кода активации, выполните следующие действия в окне **Параметры активации**:
   a. Выберите **Активировать при помощи кода активации** и нажмите на кнопку **Выбрать**.
   b. В открывшемся окне введите код активации и нажмите **ОК**.
3. Если вы хотите активировать программу с помощью файла ключа или ключа из хранилища ключей Kaspersky Security Center, выполните следующие действия в окне **Параметры активации**:
   a. Выберите **Активировать при помощи файла ключа или ключа** и нажмите на кнопку **Выбрать**.
   b. В раскрывающемся списке выберите нужный способ распространения ключа.
   c. Если вы выбрали **Файл ключа из папки**, в открывшемся окне укажите расположение файла ключа и нажмите на кнопку **Открыть**.
   d. Если вы выбрали **Файл ключа из хранилища Kaspersky Security Center**, в открывшемся окне выберите нужный ключ и нажмите **ОК**.

   Подробная информация о хранилище ключей Kaspersky Security Center приведена в *справке Kaspersky Security Center*.
4. Если вы хотите добавить дополнительный ключ для автоматического продления срока действия лицензии, установите флажок **Использовать в качестве дополнительного ключа**.
5. Нажмите на кнопку **Далее**.
6. В окне **Расписание** настройте параметры расписания запуска задачи и нажмите на кнопку **Далее**.

   Подробная информация о настройке параметров в этом окне приведена в Справке Kaspersky Security Center.
7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой будет выполняться задача, и нажмите на кнопку **Далее**.

   Подробная информация о настройке параметров в этом окне приведена в Справке Kaspersky Security Center.

8. В окне **Определение названия задачи** задайте имя задачи и нажмите на кнопку **Далее**.
9. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.
10. Нажмите на кнопку **Завершить**.

Будет создана новая задача активации программы для выбранного устройства или группы устройств.

Управление задачами обновления баз Kaspersky Endpoint Agent

Вы можете создавать и настраивать параметры задач обновления баз и модулей программы.

В этом разделе

Создание задачи обновления баз и модулей программы программы

► *Чтобы создать задачу обновления баз и модулей программы Kaspersky Endpoint Agent в Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Выберите программу, для которой будет создана задача – **Kaspersky Endpoint Agent**, и тип задачи **Обновление баз и модулей программы**.
5. Нажмите на кнопку **Далее**.

   Запустится мастер создания задачи обновления баз.

Мастер создания задачи обновления баз состоит из следующих шагов:

1. Выбор источника обновления баз

Выполните следующие действия:

1. В блоке **Источник обновлений** выберите один из следующих источников обновления баз:
   - **Сервер администрирования Kaspersky Security Center**.
   - **Серверы обновлений "Лаборатории Касперского"**.
   - **Другие HTTP-, FTP-серверы или сетевые папки**.
2. Если вы хотите включить параметр **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**, установите флажок слева от названия параметра.
3. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые папки**,

выполните следующие действия:

a. Нажмите на ссылку **Другие HTTP-, FTP-серверы или сетевые папки**.

b. Добавьте серверы обновлений в список:

1. Нажмите на кнопку **Серверы обновлений**.
2. В добавленной строке введите IP-адрес сервера обновлений.
3. Если вы хотите использовать этот сервер для обновления баз, установите флажок рядом с его IP-адресом. Вы также можете добавить в список серверы и снять флажки рядом с IP-адресами серверов, которые вы не хотите использовать сейчас, а планируете использовать в будущем.

> Выполняйте аналогичные действия по добавлению каждого сервера.

4. Нажмите на кнопку **OK**.
5. Окно **Серверы обновлений** закроется.

4. Настройка параметров обновления модулей программы

Выполните следующие действия:

1. В блоке **Параметры обновления** выберите, при каких условиях программа будет проверять доступность обновлений модулей программы:
   - **Не проверять доступность обновлений**. Kaspersky Endpoint Agent не будет проверять доступность обновлений модулей программы.
   - **Проверять доступность только важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.
   - **Загружать и устанавливать критические обновления модулей программы**. Kaspersky Endpoint Agent будет проверять доступность обновлений модулей программы и будет загружать и устанавливать критические обновления модулей программы.
2. Если вы хотите, чтобы программа отображала уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений, установите флажок **Получать информацию о доступных запланированных обновлениях модулей программы**.
3. Настройка расписания обновления баз

Выполните следующие действия:

1. В блоке **Расписание запуска задач** установите флажок **Запускать по расписанию**.
2. В списке **Периодичность** выберите один из следующих вариантов запуска задачи по расписанию: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю**, **При запуске программы** или **После обновления баз программы**.
3. Если вы выбрали запуск задачи обновления баз **В указанное время**, в блоке **Запускать по расписанию** укажите время и дату запуска задачи.
4. Если вы выбрали запуск задачи обновления баз **Каждый час**, **Каждый день** или **Каждую неделю**, в блоке **Запускать по расписанию** настройте параметры запуска задачи:

a. В списке **Каждый**выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.

b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

5. Если вы хотите выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:
   a. Если вы хотите задать максимальное время ожидания выполнения задачи обновления баз, установите флажок **Завершать задачу, выполняющуюся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.
   b. Если вы хотите, чтобы расписание запуска задачи обновления баз действовало до определенной даты, установите флажок **Отменить расписание с** и укажите дату окончания действия расписания.
   c. Если вы хотите, чтобы программа при первой возможности запускала задачи обновления баз, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.
   d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Запускать задачу каждые** и задайте интервал запуска в минутах.
   e. Нажмите на кнопку **OK**.
6. Нажмите на кнопку **Далее**

7. Выбор устройств, на которых будет выполняться задача

В открывшемся окне выбора устройств выберите устройства, на который вы хотите назначить задачу и нажмите на кнопку **Далее**.

Например, вы можете выбрать вариант **Назначить задачу группе администрирования** и выбрать группу администрирования из списка.

1. Выбор учетной записи пользователя Kaspersky Security Center, с правами которой будет выполняться задача

В окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:

- Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.
- Введите имя и пароль пользователя, под учетной записью которого вы хотите выполнять задачу и нажмите на кнопку **Далее**.

1. Указание названия задачи

В окне **Определение название задачи** в поле **Имя** введите название задачи и нажмите на кнопку **Далее**.

1. Запуск задачи сразу после создания

Настройка параметров задачи обновления баз и модулей программы

Вы можете настроить параметры задачи обновления баз и модулей программы после ее создания.

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

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.

3. В разделе **Обновление баз и модулей программы** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел параметров, которые вы хотите настроить.
6. В правой части окна внесите необходимые изменения и нажмите на кнопки **Применить** и **ОК**.

Вы можете настроить следующие параметры задачи:

1. Название задачи

Выполните следующие действия:

1. Выберите раздел **Общие**.
2. Измените имя задачи в верхней строке.

3. Устройства, на которых будет выполняться задача

В правой части окна отображаются текущие устройства, на которые назначена задача. Если вы хотите добавить устройства, выполните следующие действия:

1. Нажмите на кнопку **Добавить**.

   Откроется окно со списком управляемых устройств.
2. Установите флажки рядом с теми устройствами, которые вы хотите добавить.
3. Если вы хотите добавить устройства, которых нет в списке, нажмите на кнопку **Добавить** в правой части окна и выполните действия по добавлению устройств.

   Например, вы можете задать адреса устройств вручную или импортировать их из списка

   Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым вы хотите назначить задачу.

Подробнее о работе с управляемыми устройствами см. в *Справке Kaspersky Security Center*.

1. Источник обновления баз

Выполните следующие действия:

1. В блоке **Источник обновлений** выберите один из следующих источников обновления баз:
   - **Сервер администрирования Kaspersky Security Center**.
   - **Серверы обновлений "Лаборатории Касперского"**.
   - **Другие HTTP-, FTP-серверы или сетевые папки**.
2. Если вы хотите включить параметр **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**, установите флажок слева от названия параметра.
3. Если вы выбрали источник обновления баз **Серверы обновлений "Лаборатории Касперского"** и хотите использовать прокси-сервер для обновления баз, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.
4. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые папки**, выполните следующие действия:

a. Нажмите на ссылку **Другие HTTP-, FTP-серверы или сетевые папки**.

b. Добавьте серверы обновлений в список:

1. Нажмите на кнопку **Серверы обновлений**.
2. В добавленной строке введите IP-адрес сервера обновлений.
3. Если вы хотите использовать этот сервер для обновления баз, установите флажок рядом с его IP-адресом. Вы также можете добавить в список серверы и снять флажки рядом с IP-адресами серверов, которые вы не хотите использовать сейчас, а планируете использовать в будущем.

> Выполняйте аналогичные действия по добавлению каждого сервера.

4. Нажмите на кнопку **OK**.
5. Окно **Серверы обновлений** закроется.

c. Если вы хотите использовать прокси-сервер для соединения с серверами обновлений, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

5. Настройка дополнительных парамаметров обновления баз

Выполните следующие действия:

1. В блоке **Параметры обновления** выберите, при каких условиях программа будет проверять доступность обновлений модулей программы:
   - **Не проверять доступность обновлений**. Kaspersky Endpoint Agent не будет проверять доступность обновлений модулей программы.
   - **Проверять доступность только важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.
   - **Загружать и устанавливать критические обновления модулей программы**. Kaspersky Endpoint Agent будет проверять доступность обновлений модулей программы и будет загружать и устанавливать критические обновления модулей программы.
2. Если вы хотите, чтобы программа отображала уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений, установите флажок **Получать информацию о доступных запланированных обновлениях модулей программы**.
3. Расписание обновления баз

Выполните следующие действия:

1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.
2. В списке **Периодичность** выберите один из следующих вариантов запуска задачи по расписанию: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю**, **При запуске программы** или **После обновления баз программы**.
3. Если вы выбрали запуск задачи обновления баз **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.
4. Если вы выбрали запуск задачи обновления баз **Каждый час**, **Каждый день** или **Каждую неделю**, в разделе **Запускать по расписанию** настройте параметры запуска задачи:

a. В списке **Каждый** выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в

неделю по вторникам и четвергам.

b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

5. Чтобы выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:

   a. Если вы хотите задать максимальное время ожидания выполнения задачи обновления баз, установите флажок **Завершать задачу, выполняющуюся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.

   b. Если вы хотите, чтобы расписание запуска задачи обновления баз действовало до определенной даты, установите флажок **Отменить расписание с** и укажите дату окончания действия расписания.

   c. Если вы хотите, чтобы программа при первой возможности запускала задачи обновления баз, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.

   d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Запускать задачу каждые** и задайте интервал запуска в минутах.

   e. Нажмите на кнопку **OK**.

6. Учетную запись пользователя Kaspersky Security Center, с правами которой будет выполняться задача

В окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:

- Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.
- Введите имя и пароль пользователя, под учетной записью которого вы хотите выполнять задачу.

1. Срок хранения результатов выполнения задачи на Сервере администрирования

Выполните следующие действия:

1. Выберите раздел **Уведомление**.
2. В блоке **Сохранять информацию о результатах** убедитесь, что флажок **На Сервере администрирования в течение (сут)** установлен и укажите, сколько суток вы хотите хранить результат выполнения задачи.

   По умолчанию результат выполнения задачи хранится на Сервере администрирования 7 дней.

kaspersky

Управление задачами поиска IOC в Kaspersky Endpoint Agent

В этом разделе приведены инструкции по управлению задачами поиска IOC в Kaspersky Endpoint Agent с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

О задачах поиска IOC в Kaspersky Endpoint Agent

Задачи поиска IOC – это задачи, в ходе выполнения которых Kaspersky Endpoint Agent использует IOC-файлы (файлы индикаторов компрометации открытого стандарта описания OpenIOC) для поиска этих индикаторов на устройствах.

Kaspersky Endpoint Agent поддерживает три типа задач поиска IOC:

- *Стандартные задачи поиска IOC* – задачи, которые создаются вручную в Kaspersky Security Center или через интерфейс командной строки.
- *Автономные задачи поиска IOC* – задачи, которые создаются автоматически, при реагировании на угрозы, обнаруженные программой.
- *Поиск IOC по IOC-файлам, загружаемым вручную через веб-интерфейс программы* – пользователи программы могут использовать IOC-файлы для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и обнаружений, а также для проверки компьютеров с установленным компонентом Kaspersky Endpoint Agent.

Задачи отличаются возможностями управления, доступными для настройки параметрами, а также областью действия. Описание каждого типа задач поиска IOC приведено в следующей таблице.

Таблица 19. Типы задач поиска IOC

Тип задач	Описание задач	Область действия задач
Стандартные задачи поиска IOC	Задачи создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки, без интеграции со сторонними системами. Для запуска задач используются IOC-файлы, подготовленные пользователем. Параметры задач не зависят от политик. Вы можете задать следующие действия по реагированию на найденные IOC (недоступно при запуске задач из командной строки): • Запуск на устройстве задач проверки по требованию при помощи EPP. • Включение сетевой изоляции устройства. Просмотр отчетов доступен как в результатах выполнения задач в виде сводной таблицы, так и в карточке обнаруженных IOC.	*Карточка обнаруженных IOC* содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла. Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации. Локальные или групповые

Тип задач	Описание задач	Область действия задач
Автономные задачи поиска IOC	Задачи создаются автоматически, если в политике Kaspersky Endpoint Agent задано действие (см. раздел "Настройка действий Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox" на стр. 407) **Запустить поиск IOC на управляемой группе устройств** по реагированию на угрозы, обнаруженные Kaspersky Sandbox. Kaspersky Endpoint Agent автоматически формирует IOC-файл. Работа с пользовательскими IOC-файлами не предусмотрена. Пользователю доступно ограниченное управление задачами в Kaspersky Security Center. В политике можно задать расписание запуска задач и области поиска. Задачи автоматически удаляются через семь дней после последнего запуска или с момента создания, если задачи не запускались. Вы можете задать следующие действия по реагированию на найденные IOC: • Запуск на устройстве задач проверки по требованию при помощи EPP. • Помещение объекта на карантин и удаление с устройства. Просмотр отчетов доступен как в результатах выполнения задач в виде сводной таблицы, так и в карточке обнаруженных IOC.	*Карточка обнаруженных IOC* содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла. Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации. Групповые
Поиск IOC по IOC-файлам, загружаемым вручную через веб-интерфейс программы	IOC-файлы загружаются вручную через веб-интерфейс программы. Также есть возможность настроить расписание IOC-проверки компьютеров с программой Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Endpoint Detection and Response. Управление задачами с помощью Kaspersky Security Center или через командную строку не предусмотрено. Автоматических действий при обнаружении IOC не предусмотрено. Параметры задач не зависят от политик Kaspersky Endpoint Agent.	Не применимо

Результаты выполнения групповых задач поиска IOC доступны для просмотра в Kaspersky Security Center в течение семи дней с момента выполнения задачи или до момента удаления задачи.

Управление задачами поиска IOC в Kaspersky Endpoint Agent

Вы можете управлять задачами поиска IOC через Kaspersky Security Center или через интерфейс командной строки Kaspersky Endpoint Agent, а также загружать IOC-файлы и настраивать расписание IOC-проверки через веб-интерфейс Kaspersky Endpoint Detection and Response. Описание каждого типа задач поиска IOC и информация о доступных возможностях управления задачами поиска IOC приведены в таблице ниже.

Таблица 20. Управление задачами поиска IOC.

Тип задачи	С помощью Kaspersky Security Center	С помощью компонента Central Node	Через интерфейс командной строки
Стандартная задача поиска IOC	• Создание (см. раздел "Создание и настройка стандартной задачи поиска IOC" на стр. 443), удаление (см. раздел "Удаление задач из списка" на стр. 425) и запуск (см. раздел "Запуск задач вручную" на стр. 425) задачи вручную. • Просмотр детальных отчетов в результатах выполнения задачи (см. раздел "Просмотр результатов выполнения задачи поиска IOC" на стр. 445) в виде сводной таблицы и в карточке обнаруженных IOC. *Карточка обнаруженных IOC* содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла. Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации. • Экспорт IOC-коллекции (на стр. 445). • Настройка следующих параметров в мастере создания задачи (см. раздел "Создание и настройка стандартной задачи поиска IOC" на стр. 443) или в свойствах задачи (см. раздел "Настройка параметров стандартной задачи поиска IOC" на стр. 444) после ее создания:	Управление не предусмотрено.	• Создание и запуск задачи с требуемыми параметрами (см. раздел "Управление стандартными задачами поиска IOC" на стр. 467). • Просмотр данных о выполнении задачи (см. раздел "Управление стандартными задачами поиска IOC" на стр. 467).

Тип задачи	С помощью Kaspersky Security Center	С помощью компонента Central Node	Через интерфейс командной строки
	• Параметры IOC-коллекции. • Параметры поиска IOC. • Действия программы при обнаружении IOC (сетевая изоляция устройства и запуск проверки на устройстве с помощью EPP). • Параметры расписания запуска задачи. • Срок хранения результатов выполнения задачи на Сервере администрирования (недоступно в мастере создания задачи).		
Автономная задача поиска IOC	• Настройка запуска задач (см. раздел "Настройка запуска автономных задач поиска IOC" на стр. 411). • Запуск (см. раздел "Запуск задач вручную" на стр. 425) и удаление (см. раздел "Удаление задач из списка" на стр. 425) задачи вручную. • Включение выполнения действий по реагированию на угрозы, обнаруженные Kaspersky Sandbox (см. раздел "Включение и отключение выполнения действий по реагированию на угрозы" на стр. 408). • Добавление действия автоматического создания Автономной задачи поиска IOC (см. раздел "Добавление действий по реагированию на угрозы в список действий текущей политики" на стр. 409). • Просмотр детальных отчетов в результатах выполнения задачи (см. раздел "Просмотр результатов выполнения задачи поиска IOC" на стр. 445) в виде сводной таблицы и в карточке обнаруженных IOC. *Карточка обнаруженных IOC* содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а	Управление не предусмотрено.	Управление не предусмотрено.

Тип задачи	С помощью Kaspersky Security Center	С помощью компонента Central Node	Через интерфейс командной строки

	также текст совпавших веток или отдельных условий из этого IOC-файла.
	
	Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации.
	
	• Экспорт IOC-коллекции. (см. раздел "Экспорт IOC-коллекции" на стр. 445)
	• Настройка следующих параметров в свойствах задачи (см. раздел "Настройка параметров автономной задачи поиска IOC" на стр. 448):
	  • Действия программы при обнаружении IOC (помещение объекта на карантин и удаление с устройства; запуск проверки на устройстве с помощью EPP).
	  • Параметры расписания запуска задачи.
	  • Срок хранения результатов выполнения задачи на Сервере администрирования.		

Задача поиска IOC, созданная в Central Node	Управление не предусмотрено.	Загрузка IOC-файлов (см. раздел "Загрузка IOC-файла" на стр. 338), настройка расписания IOC-проверки (на стр. 340).	Управление не предусмотрено.

kaspersky

Управление стандартными задачами поиска IOC

Стандартные задачи поиска IOC – задачи, которые создаются вручную в Kaspersky Security Center или через интерфейс командной строки.

В этом разделе приведены инструкции по управлению стандартными задачами поиска IOC с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

Требования к IOC-файлам

Kaspersky Endpoint Agent поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.

Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.

Если при создании задачи Поиск IOC все загруженные вами IOC-файлы не поддерживаются Kaspersky Endpoint Agent, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации.

Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.

Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.

Особенности и ограничения поддержки стандарта OpenIOC программой приведены в следующей таблице.

Таблица 21. 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). Программа 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 Программа поддерживает интерпретацию типов данных date и duration, если индикаторы заданы в формате ISO 8601, Zulu time zone, UTC.
Поддерживаемые IOC-термины	Поддерживаемые программой IOC-термины приведены в таблице "Поддерживаемые IOC термины".

Создание и настройка стандартной задачи поиска IOC

► *Чтобы создать и настроить стандартную задачу поиска IOC,*

в зависимости от требуемой области действия задачи выполните одно из следующих действий:

- Запустите мастер создания локальной задачи.
- Запустите мастер создания групповой задачи.

Мастер создания задачи позволяет настроить следующие параметры:

- IOC-коллекция
- Типы данных (IOC-документы) для анализа во время поиска IOC
- Действия программы при обнаружении IOC
- Расписание запуска задачи
- Учетная запись пользователя Kaspersky Security Center для запуска задачи
- Название задачи

Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.

Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.

Настройка параметров стандартной задачи поиска IOC

► *Чтобы настроить параметры стандартной задачи поиска IOC выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   В рабочей области отобразится список задач.
3. Откройте параметры требуемой задачи одним из следующих способов:
   - Двойным щелчком мыши по названию задачи.
   - Откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Выберите задачу и нажмите на ссылку **Настроить параметры задачи** в правой части окна.

   Откроется окно **Свойства: <Название задачи>**.
4. В левой части окна выберите раздел параметров, которые вы хотите настроить.
5. В правой части окна внесите необходимые изменения и нажмите на кнопки **Применить** и **ОК**.

Вы можете настроить следующие параметры задачи:

- Название задачи

Выполните следующие действия:

1. Выберите раздел **Общие**.
2. Измените имя задачи в верхней строке.

- Срок хранения результатов выполнения задачи на Сервере администрирования

Выполните следующие действия:

1. Выберите раздел **Уведомление**.
2. В блоке **Сохранять информацию о результатах** убедитесь, что флажок **На Сервере администрирования в течение (сут)** установлен и укажите, сколько суток вы хотите хранить результат выполнения задачи.

По умолчанию результат выполнения задачи хранится на Сервере администрирования 7 дней.

- IOC-коллекция
- Действия программы при обнаружении IOC
- Типы данных (IOC-документы) для анализа во время поиска IOC
- Расписание запуска задачи поиска IOC
- Учетная запись пользователя Kaspersky Security Center для запуска задачи

Исключение групп устройств из области действия задачиЕсли вы хотите исключить группы хостов из области действия задачи, в разделе **Исключения из области действия задачи** выберите группы устройств, к которым не будет применяться задача.

Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

Экспорт IOC-коллекции

► *Чтобы экспортировать IOC-коллекцию, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В разделе **Запустить поиск IOC** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. Выберите раздел **Параметры поиска IOC**.
6. В разделе **IOC-коллекция** нажмите на кнопку **Экспортировать**.
7. В открывшемся окне задайте имя файла, а также выберите папку, в которую вы хотите его сохранить.
8. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной вами папке.

Просмотр результатов выполнения задачи поиска IOC

► *Чтобы просмотреть результаты выполнения задачи Поиск IOC, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   В рабочей области отобразится список задач.
3. Откройте параметры нужной задачи одним из следующих способов:

- Двойным щелчком мыши по названию задачи.
- Откройте контекстное меню задачи и выберите пункт **Свойства**.
- Выберите задачу и нажмите на ссылку **Настроить параметры задачи** в правой части окна.

Откроется окно **Свойства: <Имя задачи>**.

4. Выберите раздел **Результаты**.
5. В списке **Показать результаты по устройству** выберите, по каким устройствам вы хотите просмотреть результаты выполнения задач поиска IOC.
6. Чтобы просмотреть подробную информацию об определенной задаче, раскройте ее двойным щелчком мыши.
7. Чтобы просмотреть подробную информацию об обнаруженном индикаторе компрометации, нажмите на кнопку **Показать карточку инцидента**.

   Карточка обнаруженных IOC содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.

   Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации.

kaspersky

Управление автономными задачами поиска IOC

Автономные задачи поиска IOC – задачи, которые создаются автоматически, при реагировании на угрозы, обнаруженные Kaspersky Endpoint Detection and Response.

В этом разделе приведены инструкции по настройке параметров автономных задач поиска IOC с помощью плагина управления Kaspersky Endpoint Agent.

В этом разделе

Об Автономных задачах поиска IOC

Автономные задачи поиска IOC создаются автоматически на сервере Kaspersky Security Center, если в политиках Kaspersky Endpoint Agent настроено действие по реагированию на угрозу **Запустить поиск IOC на управляемой группе устройств**.

Создание Автономных задач поиска IOC вручную недоступно.

Вы можете просматривать список задач, удалять неиспользуемые задачи из списка, просматривать результаты выполнения задач, запускать задачи вручную, настраивать срок хранения результатов выполнения задач, а также настраивать параметры запуска задач поиска IOC.

Автоматически созданные задачи хранятся на сервере Kaspersky Security Center. Администратору Kaspersky Endpoint Agent рекомендуется следить, чтобы количество задач в списке не превышало 1000 и периодически удалять задачи из списка (см. раздел "Удаление задач из списка" на стр. 425) вручную.

Автономные задачи поиска IOC по умолчанию хранятся на сервере Kaspersky Security Center семь дней с момента последнего запуска.

Kaspersky Endpoint Agent удаляет Автономные задачи поиска IOC, если хотя бы на одном устройстве программа работала без перерыва не менее семи дней и выполнено одно из следующих условий:

- задача в последний раз запускалась не менее семи дней назад;
- задача не запускалась ни разу, и с момента создания задачи прошло не менее семи дней.

Kaspersky Endpoint Agent удаляет Автономную задачу поиска IOC независимо от того, на каком устройстве впервые был обнаружен объект и было выполнено действие по реагированию на угрозы. Удаленная задача будет недоступна для всех устройств, входящих в группу администрирования.

Удаление неиспользуемых Автономных задач поиска IOC происходит автоматически. Настройка

параметров автоматического удаления Автономных задач поиска IOC не предусмотрена программой.

Если удаление Автономных задач поиска IOC выполняется некорректно или вы хотите изменить поведение программы, обратитесь в Службу технической поддержки "Лаборатории Касперского".

По умолчанию в Автономной задаче поиска IOC настроено хранение всех типов событий, возникающих при выполнении групповых задач. По умолчанию результаты выполнения Автономных задач поиска IOC хранятся семь дней. Вы можете изменить срок хранения результатов выполнения задач.

Не рекомендуется менять заданные по умолчанию значения параметров хранения результатов выполнения задач или сокращать срок хранения результатов выполнения Автономных задач поиска IOC.

Настройка прав пользователей для управления задачами поиска IOC

Необходимо настроить права пользователя Kaspersky Security Center, учетная запись которого используется для управления задачами поиска IOC.

► *Чтобы настроить права пользователя Kaspersky Security Center для управления задачами поиска IOC, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите **Сервер администрирования**.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.
4. В левой части окна выберите раздел **Безопасность**.
5. Выберите пользователя Kaspersky Security Center, учетную запись которого вы хотите использовать для управления задачами поиска IOC.

   В нижней части окна отобразится список прав выбранного пользователя, сгруппированных по программам, которыми пользователь может управлять в Kaspersky Security Center.
6. В группе прав **Kaspersky Endpoint Agent** раскройте блок **Предотвращение вторжений**.
7. Для типов прав **Изменение**, **Выполнение** и **Выполнение действий над выборками устройств** установите флажки в столбце **Разрешить**.
8. Нажмите на кнопки **Применить** и **ОК**.

Настройка параметров автономной задачи поиска IOC

► *Чтобы настроить параметры автононономной задачи поиска IOC, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

Отобразится список задач.

3. В разделе **Запустить поиск IOC** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел параметров, которые вы хотите изменить.
6. В правой части окна внесите необходимые изменения и нажмите на кнопки **Применить** и **OK**.

Вы можете настроить следующие параметры задачи:

- Название задачи

Выполните следующие действия:

1. Выберите раздел **Общие**.
2. Измените имя задачи в верхней строке.

- Срок хранения результатов выполнения задачи на Сервере администрирования

Выполните следующие действия:

1. Выберите раздел **Уведомление**.
2. В блоке **Сохранять информацию о результатах** убедитесь, что флажок **На Сервере администрирования в течение (сут)** установлен и укажите, сколько суток вы хотите хранить результат выполнения задачи.

   По умолчанию результат выполнения задачи хранится на Сервере администрирования 7 дней.

- Действия программы, при обнаружении IOC
- Расписание запуска задач поиска IOC
- Учетная запись пользователя Kaspersky Security Center для запуска задачи
- Исключение групп устройств из области действия задачи

Если вы хотите исключить группы хостов из области действия задачи, в разделе **Исключения из области действия задачи** выберите группы устройств, к которым не будет применяться задача.

Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

Экспорт IOC-коллекции

► *Чтобы экспортировать IOC-коллекцию, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В разделе **Запустить поиск IOC** выберите задачу в списке и правой клавишей мыши раскройте

меню действий над задачами.

4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.

5. Выберите раздел **Параметры поиска IOC**.
6. В разделе **IOC-коллекция** нажмите на кнопку **Экспортировать**.
7. В открывшемся окне задайте имя файла, а также выберите папку, в которую вы хотите его сохранить.
8. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной вами папке.

Просмотр результатов выполнения задачи поиска IOC

► *Чтобы просмотреть результаты выполнения задачи Поиск IOC, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   В рабочей области отобразится список задач.

3. Откройте параметры нужной задачи одним из следующих способов:
   - Двойным щелчком мыши по названию задачи.
   - Откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Выберите задачу и нажмите на ссылку **Настроить параметры задачи** в правой части окна.

   Откроется окно **Свойства: <Имя задачи>**.

4. Выберите раздел **Результаты**.
5. В списке **Показать результаты по устройству** выберите, по каким устройствам вы хотите просмотреть результаты выполнения задач поиска IOC.
6. Чтобы просмотреть подробную информацию об определенной задаче, раскройте ее двойным щелчком мыши.
7. Чтобы просмотреть подробную информацию об обнаруженном индикаторе компрометации, нажмите на кнопку **Показать карточку инцидента**.

   Карточка обнаруженных IOC содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.

   Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации.

kaspersky

Управление Kaspersky Endpoint Agent через интерфейс командной строки

Программой Kaspersky Endpoint Agent можно управлять через интерфейс командной строки. Функциональность интерфейса командной строки обеспечивает утилита agent.exe. Утилита agent.exe входит в комплект поставки программы Kaspersky Endpoint Agent и устанавливается на каждое устройство вместе с Kaspersky Endpoint Agent в папку `%ProgramFiles%\Kaspersky Lab\Endpoint Agent` (если на устройстве установлена 32-разрядная операционная система) или `%ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent` (если на устройстве установлена 64-разрядная операционная система).

Пример:

Если на устройстве установлена 64-разрядная операционная система Windows и для установки программы Kaspersky Endpoint Agent вы выбрали установку на диск C, то при установке утилита agent.exe будет размещена в следующую папку:

`C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\`

► *Чтобы управлять программой Kaspersky Endpoint Agent через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Введите команду: `agent.exe --<параметр программы, который вы хотите настроить>=<действие над параметром, которое вы хотите выполнить>` и нажмите на клавишу **ENTER**.

   Отобразится результат выполнения команды (код возврата).

Можно управлять следующими параметрами Kaspersky Endpoint Agent:

- `help`

  Отображает справочную информацию по всем параметрам программы и их возможным значениям.
- `trace`

  Позволяет настроить трассировку в программе Kaspersky Endpoint Agent.

  Доступные действия: `enable`, `disable`, `show`.
- `dump`

  Позволяет настроить создание дампов в программе Kaspersky Endpoint Agent.

  Доступные действия: `enable`, `disable`, `show`.
- `quarantine`

  Позволяет работать с карантином Kaspersky Endpoint Agent.

Доступные действия: `add`, `delete`, `restore`, `show`, `limits`.

- `sandbox`

  Позволяет управлять интеграцией программы Kaspersky Endpoint Agent с программой Kaspersky Sandbox.

  Доступные действия: `enable`, `disable`, `show`.

- `update`

  Позволяет управлять обновлением баз программы Kaspersky Endpoint Agent.

  Доступные действия: `bases`, `modules`.

- `ppl`

  Позволяет управлять процессами программы Kaspersky Endpoint Agent, запускающимися с признаком PPL (процессы защищены технологией Protected Process Light).

  Процессы, запускающиеся с признаком PPL, не могут быть остановлены или изменены другими процессами без признака PPL.

  Использование признака PPL для служб программы позволяет надежно защитить службы от вредоносных воздействий извне и попыток компрометации программы.

  Доступные действия: `enable`, `disable`, `show`.

- `password`

  Позволяет управлять защитой программы Kaspersky Endpoint Agent с помощью пароля.

  Доступные действия: `set`, `reset`, `state`.

- `product`

  Позволяет управлять программой Kaspersky Endpoint Agent.

  Доступные действия: `start`, `stop`, `state`.

Пример:

Для вызова справки по всем параметрам программы и их возможным значениям выполните команду:

```
agent.exe --help
```

Для включения интеграции с Kaspersky Sandbox выполните команду:

```
agent.exe --sandbox=enable
```

kaspersky

В этом разделе

Управление активацией Kaspersky Endpoint Agent

► *Чтобы управлять активацией программы через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:
   - Чтобы активировать программу с помощью кода активации или файла ключа:

     `agent.exe --license=add <код активации или путь к файлу ключа>`

     > Для активации программы с помощью кода активации защищаемое устройство должно быть подключено к интернету.

   - Чтобы указать дополнительный ключ для автоматического продления срока действия лицензии:

     `agent.exe --license=reserve <код активации или путь к файлу ключа>`

   - Чтобы удалить добавленный основной или дополнительный ключ:

```
agent.exe --license=delete <серийный номер ключа>
```

- Чтобы просмотреть статус добавленных ключей:

  ```
  agent.exe --license=show
  ```

Коды возврата команды `--license`:

- `E_EXPIRED` – срок действия добавляемого ключа истек.
- `E_FAIL` – неопределенная программная ошибка.
- `E_KEY_IN_BLST` – добавляемый ключ находится в черном списке.
- `E_KEY_NOT_MATCH` – добавляемый ключ не подходит для активации Kaspersky Endpoint Agent.
- `E_GENERAL_ERROR` – общая ошибка (например, файл ключа поврежден).
- `E_INVALID_SYNTAX` – синтаксические ошибки.
- `E_INVALID_PATH` – указан некорректный путь к файлу ключа.

Настройка трассировки

► *Чтобы настроить трассировку в программе Kaspersky Endpoint Agent через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:

   - `agent.exe --trace=enable --folder <путь к папке, в которой вы хотите создавать файлы трассировки>`, чтобы включить трассировку.

   Трассировка будет включена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы трассировки будут создаваться в папке, которую вы указали.

   - `agent.exe --trace=disable`, чтобы выключить трассировку.

   Трассировка будет отключена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент.

   - `agent.exe --trace=show`, чтобы просмотреть текущее состояние трассировки и путь к папке для сохранения файлов трассировки.

   Отобразятся значения параметров `trace.enable` (`true`, если трассировка включена или `false`, если трассировка отключена) и `trace.folder` (путь к папке).

Коды возврата команды `--trace`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.

- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 5 – объект не найден (не найден путь, указанный в качестве пути к папке с файлами журнала трассировки).
- 9 – неверная операция (например, попытка выполнения команды `--trace=disable`, если трассировка уже отключена).

Настройка создания дампа

► *Чтобы настроить создание дампа в программе Kaspersky Endpoint Agent через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:

   - `agent.exe --dump=enable --folder <путь к папке, в которой вы хотите создавать дамп>`, чтобы включить создание дампа.

   Создание дампа будет включено для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы дампа будут создаваться в папке, которую вы указали.

   - `agent.exe --dump=disable`, чтобы отключить создание дампа.

   Создание дампа будет отключено для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент.

   - `agent.exe --dump=show`, чтобы просмотреть текущее состояние создания дампа и путь к папке с файлами дампа.

   Отобразятся значения параметров `dump.enable` (`true`, если создание дампа включено или `false`, если создание дампа отключено) и `dump.folder` (путь к папке).

Коды возврата команды `--dump`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 5 – объект не найден (не найден путь, указанный в качестве пути к папке с файлами дампа).
- 9 – неверная операция (например, попытка выполнения команды `--dump=disable`, если создание дампа уже отключено).

Просмотр информации о параметрах карантина и объектах на карантине

► *Чтобы просмотреть информацию о параметрах карантина и объектах, находящихся на карантине, через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --quarantine=show [--pwd=<текущий пароль пользователя>]`, чтобы просмотреть список объектов, помещенных на карантин.

   Отобразится следующая информация обо всех объектах, находящихся в папке карантина, указанной при настройке параметров карантина:
   - Идентификаторы объектов, помещенных на карантин к текущему моменту (параметр `ouid`).
   - Имена объектов, помещенных на карантин (имя + расширение).
   - Дата и время помещения объекта на карантин (UTC).
   - Исходный путь к файлу, помещенному на карантин, и путь восстановления файла из карантина, заданный по умолчанию (без имени файла).
   - Размер файла, помещенного на карантин (в байтах).
   - Учетная запись пользователя, с правами которой выполнялась задача помещения файла на карантин.
   - Статус объекта:
     - `DETECT`, если файл был помещен на карантин программой EPP или в рамках действий по реагированию на угрозу, обнаруженную Kaspersky Sandbox. Например, в результате локального действия **Поместить на карантин и удалить** или глобального действия **Поместить на карантин и удалить при обнаружении IOC**.
     - `CUSTOM`, если файл был помещен на карантин вручную, в результате выполнения команды `--quarantine=add`.
   - Способ, которым файл был помещен на карантин:
     - `AUTOMATIC_<название программы, обнаружившей угрозу в файле, помещенном на карантин>`, если файл был помещен на карантин программой EPP или в рамках действий по реагированию на угрозу, обнаруженную Kaspersky Sandbox. Например, в результате локального действия **Поместить на карантин и удалить** или глобального действия **Поместить на карантин и удалить при обнаружении IOC**.
     - `BY USER`, если файл был помещен на карантин вручную, в результате выполнения команды `--quarantine=add`.
   - `agent.exe --quarantine=limits`, чтобы просмотреть текущие значения параметров **Максимальный размер Карантина (МБ)** и **Пороговое значение места на диске (МБ)**, а также статусы применения этих параметров (статусы флажков), заданные при настройке параметров

карантина (см. раздел "Настройка параметров карантина и восстановления объектов из карантина" на стр. 417).

Коды возврата команды `--quarantine`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Действия над объектами на карантине

► *Чтобы выполнить действия над объектами, находящимися на карантине программы Kaspersky Endpoint Agent через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Выполните следующие действия и нажмите на клавишу **ENTER**:
   - Если вы хотите безвозвратно удалить объекты, находящиеся на карантине, выполните команду:

     `agent.exe --quarantine=delete --ouid=<`идентификаторы объектов на карантине через запятую. Обязательный параметр`> [--pwd=<`текущий пароль пользователя`>]`.

     Объекты с указанными идентификаторами будут удалены из папки карантина устройствах, указанной при настройке параметров карантина.
   - Если вы хотите восстановить объекты из карантина, выполните команду:

     `agent.exe --quarantine=restore --ouid=<`идентификаторы объектов на карантине через запятую. Обязательный параметр`> [--path-type=<`один из вариантов выбора папки назначения при восстановлении объекта из карантина: `original|custom|settings`. Необязательный параметр`> --path=<`путь к папке назначения для восстановленных объектов. Обязательный параметр, если передан параметр `--path-type` и указано значение `original>] [--action=<`одно из действий над объектом: `replace|rename`. Необязательный параметр`>] [--pwd=<`текущий пароль пользователя`>]`.
   - Если вы хотите поместить объект на карантин, выполните одну из следующих команд:
     - `agent.exe --quarantine=add [--file=<`полный путь к объекту, который вы хотите поместить на карантин`>] [--pwd=<`текущий пароль пользователя`>]`
     - `agent.exe --quarantine=add [--hash=<`хеш объекта, который вы хотите поместить на карантин. Обязательный параметр, если вы не указываете полный путь к объекту и передаете параметр `--hashalg >]--hashalg=<`один из типов хеша: `md5|sha256`. Обязательный параметр, если вы не указываете полный путь к объекту`> [--file=<`путь к

папке с объектом, который вы хотите поместить на карантин>] [--pwd=<текущий пароль пользователя>].

Таблица 22. Параметры команд при выполнении действий над объектами на карантине

Параметр	Описание
--ouid	Обязательный параметр. В параметре передается уникальный числовой (int64) идентификатор объекта на карантине. Отображается при просмотре информации об объектах на карантине (команда --quarantine=show).
--path-type=<original|custom|settings>	Параметр описывает логику выбора папки назначения при восстановлении объекта из карантина. • Если параметр не передан, объект будет восстановлен в исходную папку – папку, в которой находился объект до помещения его на карантин. Если исходная папка недоступна, объект будет восстановлен в папку, указанную при настройке параметров карантина. • Если параметр передан со значением <original>, объект будет восстановлен в исходную папку – папку, в которой находился объект до помещения его на карантин. Если исходная папка недоступна, объект будет восстановлен в папку, указанную при настройке параметров карантина. • Если параметр передан со значением <settings>, объект будет восстановлен в папку, указанную при настройке параметров карантина. Если папка недоступна, задача завершается с ошибкой. • Если параметр передан со значением <custom>, объект будет восстановлен в папку, путь к которой вы укажете для параметра --path. Если папка недоступна, задача завершается с ошибкой.
--path=<путь к папке назначения для восстановленных объектов>	Обязательный параметр, если передан параметр --path-type со значением <custom>. Параметр определяет путь, по которому вы хотите создать папку для объектов, восстановленных из карантина, если вы не хотите использовать папку, в которой находился объект до помещения его на карантин и папку, указанную при настройке параметров карантина.

`--action=<replace|rename>`	Параметр определяет действие над объектом, которое вы хотите выполнить, если при восстановлении объекта из карантина папка назначения для восстановленных объектов содержит файл с таким же именем. • Если параметр не передан, восстановленный объект будет переименован: к первоначальному имени объекта будет добавлен суффикс `_restored`. • Если параметр передан со значением `<rename>`, восстановленный объект будет переименован: к первоначальному имени объекта будет добавлен суффикс `_restored`. • Если параметр передан со значением `<replace>`, первоначальный объект будет заменен на восстановленный объект.
`--file=<`полный путь к объекту, который вы хотите поместить на карантин`>`	Обязательный параметр, если не передан параметр `-hashalg`. Параметр задает полный путь к объекту, который вы хотите поместить на карантин.
`--hashalg=<md5|sha256>`	Обязательный параметр, если не передан параметр `-file` и не указан полный путь к объекту, который вы хотите поместить на карантин. Параметр задает алгоритм хеширования, по которому будет рассчитана контрольная сумма объекта, который вы хотите поместить на карантин. Параметр может быть передан с одним из двух значений: `<md5>` или `<sha256>`.
`--hash=<target file checksum>`	Обязательный параметр, если передан параметр `-hashalg`. Параметр задает контрольную сумму объекта, который вы хотите поместить на карантин.
`--file=<target file folder>`	Обязательный параметр, если передан параметр –hashalg. Параметр задает путь к папке с объектом, который вы хотите поместить на карантин и хеш которого вы указали в параметре `-hash`.
`--pwd=<`текущий пароль пользователя`>`	Позволяет ввести пароль пользователя, под учетной записью которого выполняется команда.

Коды возврата команды `--quarantine`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.

- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Управление параметрами интеграции с компонентом KATA Central Node

► *Чтобы управлять параметрами интеграции программы Kaspersky Endpoint Agent с компонентом KATA Central Node через интерфейс командной строки Kaspersky Endpoint Agent, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   `agent.exe --message-broker=<enable|disable|show> --type=<kata> --compression=<yes|no> --partitioning-strategy=<automatic|user> [--message-key=<ключ сообщения> --topic=<тема> --partition=<user specific partition>] --tls=<yes|no> --servers=<адрес>:<порт> [--timeout=<максимальное время ожидания ответа сервера KATA] [--pinned-certificate=<полный путь к файлу TLS-сертификата>] [--client-certificate=<полный путь к файлу сертификата>] --client-password=<пароль к архиву формата PFX> --sync-period=<период отправки запросов на синхронизацию>`

Таблица 23. Параметры команды `--message-broker` при управлении параметрами интеграции Kaspersky Endpoint Agent с компонентом KATA Central Node

Параметр	Описание
► *`--message-broker=<enable|disable|show>`*	Обязательный параметр. Позволяет включить, отключить и просмотреть состояние программы Kaspersky Endpoint Agent с компонентом KATA Central Node. • `--message-broker=<enable>` включает интеграцию. • `--message-broker=<disable>` отключает интеграцию. • `--message-broker=<show>` отображает состояние интеграции Kaspersky Endpoint Agent с компонентом KATA Central Node.

► `--type=<kata>`	• Обязательный параметр. • Позволяет указать компонент KATA Central Node для управления параметрами интеграции программы Kaspersky Endpoint Agent с этим компонентом.
`---tls=<yes|no>`	Необязательный параметр. Позволяет включить и отключить использование доверенного соединения Kaspersky Endpoint Agent с компонентом KATA Central Node. • `--tls=<yes>` включает использование доверенного соединения. • `--tls=<no>` отключает использование доверенного соединения.
`--servers=<`адрес`>:<`порт`>`	Обязательный параметр. Позволяет добавить сервер KATA.
`--timeout=<`максимальное время ожидания ответа сервера Kaspersky Anti Targeted Attack Platform`>`	Необязательный параметр. Позволяет задать максимальное время ожидания ответа сервера KATA в миллисекундах.
`--pinned-certificate=<`полный путь к файлу TLS-сертификата`>`	Обязательный параметр, если передан параметр `--tls` со значением `<yes>`. Позволяет добавить TLS-сертификат соединения Kaspersky Endpoint Agent с сервером KATA.
`--client-certificate=<`полный путь к файлу сертификата`>`	Позволяет добавить пользовательский сертификат соединения Kaspersky Endpoint Agent с сервером KATA.
`--pwd=<`текущий пароль пользователя`>`	Позволяет ввести пароль к архиву формата PFX, содержащему пользовательский сертификат соединения Kaspersky Endpoint Agent с сервером KATA.
`--sync-period=<`период отправки запросов на синхронизацию`>`	Позволяет задать период отправки запросов на синхронизацию параметров и задач Kaspersky Endpoint Agent с KATA Central Node.

Запуск обновления баз или модулей Kaspersky Endpoint Agent

► *Чтобы запустить обновление баз или модулей программы Kaspersky Endpoint Agent через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с

правами учетной записи локального администратора.

2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.

3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   ```
   agent.exe --update=bases|modules [--source=<адреса пользовательских источников обновлений баз, разделенные точкой с запятой без пробела>|kl|ksc]
   ```

Таблица 24. Параметры команд при запуске обновления баз Kaspersky Endpoint Agent

Параметр	Описание
`--update=bases|modules`	Обязательный параметр. Позволяет указать тип обновления: • `--update=bases` позволяет запустить обновление баз программы. • `--update=modules` позволяет запустить обновление модулей программы.
`--source=<адреса пользовательских источников обновления баз>|kl|ksc]`	Необязательный параметр. Позволяет выбрать источник обновления баз. • `--source=<адреса пользовательских источников обновлений баз>` позволяет указать источник обновлений баз **Другие HTTP-, FTP-серверы или сетевые папки** и задать путь к сетевой папке или IP-адрес, FTP или HTTP-адрес сервера, с которого программа будет загружать обновления баз. Вы можете указать несколько адресов пользовательских источников обновлений баз, разделенных точкой с запятой без пробела (";"). Программа будет загружать обновления с первого доступного источника обновлений баз. Если все адреса будут недоступны, задача завершится с ошибкой. • `--source=kl` позволяет указать источник обновления баз **Серверы обновлений "Лаборатории Касперского"**. Если серверы будут недоступны, задача завершится с ошибкой. • `--source=ksc` позволяет указать источник обновления баз **Сервер администрирования Kaspersky Security Center**. Если Сервер администрирования будет недоступен, задача завершится с ошибкой.

Коды возврата команды `--update=bases`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

- 8 – ошибка прав доступа.
- 200 – все объекты актуальны.
- -206 – файлы обновлений отсутствуют в указанном источнике обновлений баз или имеют неизвестный формат.
- -209 – ошибка подключения к источнику обновлений баз.
- -232 – ошибка подключения к прокси-серверу.
- -234 – ошибка подключения к Kaspersky Security Center.
- -236 – базы программы повреждены.

Запуск, остановка и просмотр текущего состояния программы

► *Чтобы запустить, остановить или просмотреть текущее состояние программы Kaspersky Endpoint Agent через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   ```
   agent.exe --product=<start|stop|state> [--pwd=<текущий пароль пользователя>]
   ```

Таблица 25. Параметры команд при запуске, остановке и просмотре текущего состояния Kaspersky Endpoint Agent

Параметр	Описание
`--product=<start|stop|state>`	Позволяет запустить, остановить или просмотреть текущее состояние программы. • `--product=<start>` запускает программу. • `--product=<stop>` останавливает программу. Если в программе настроена защита паролем, для выполнения команды `--product=<stop>` требуется ввести пароль. • `--product=<state>` отображает текущее состояние программы: запущена или остановлена.
`--pwd=<текущий пароль пользователя>`	Позволяет ввести пароль пользователя, с правами учетной записи которого выполняется команда.

Коды возврата команды `--product=<start|stop|state>`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.

- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 8 – ошибка прав доступа.
- 9 – неверная операция (например, попытка выполнения команды `--product=start`, если программа уже запущена).

Защита программы паролем

Чтобы ограничить выполнение действий с программой Kaspersky Endpoint Agent, которые могут привести к снижению уровня защиты компьютера пользователя и данных, обрабатываемых на этом компьютере, а также к снижению уровня самозащиты программы, требуется защитить программу паролем.

Ввод пароля требуется для выполнения следующих команд в интерфейсе командной строки Kaspersky Endpoint Agent:

- `--sandbox=disable`
- `--sandbox=show`
- `--sandbox=enable --tls=no`
- `--sandbox=enable --pinned-certificate=<полный путь к файлу TLS-сертификата соединения Kaspersky Endpoint Agent с Kaspersky Sandbox>`
- `--quarantine=delete –ouid`
- `--quarantine=show`
- `--quarantine=restore`
- `--quarantine=add`
- `--product=stop`
- `--password=reset`
- `--isolation=disable`
- `--prevention=disable`
- `--selfdefence`
- `--license=delete`
- `--message-broker --type=kata <параметры>`
- `--event --action=enable`
- `--event --action=disable`

Для ввода пароля используйте параметр `--pwd=<текущий пароль пользователя>`.

Также требуется вводить пароль при выполнении следующих действий над программой:

- удаление программы и удаленная деинсталляция программы с помощью Kaspersky Security Center;

- изменение состава компонентов программы (`modify`);
- обновление программы (`upgrade`);
- восстановление программы (`repair`);
- работа в мастере установки программы;
- работа в интерфейсе командной строки.

После включения защиты паролем и применения политики Kaspersky Security Center, на всех устройствах управляемой группы Kaspersky Endpoint Agent применяется единый пароль.

Изменение параметров защиты паролем (отключение защиты паролем или изменение пароля) на локальных устройствах недоступно.

После отключения защиты паролем в политике параметры защиты паролем сохраняются для локального устройства с возможностью редактирования.

Пароль хранится в параметрах программы в зашифрованном виде (как контрольная сумма).

Для ввода пароля используйте параметр `--pwd=<текущий пароль пользователя>`.

► *Чтобы настроить защиту паролем программы Kaspersky Endpoint Agent через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Выполните одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --password=stat`, чтобы просмотреть текущий статус защиты программы паролем.
   - `agent.exe --password=set --pwd=<текущий пароль пользователя> --new=<новый пароль пользователя>`, чтобы установить новый пароль пользователя.
   - `agent.exe --password=reset --pwd=<текущий пароль пользователя>`, чтобы сбросить пароль пользователя.

Защита служб программы технологией PPL

В программе Kaspersky Endpoint Agent реализована защита служб (например, службы soyuz.exe) с помощью технологии *Protected Process Light (PPL)*.

Процессы, исполняющиеся с признаком PPL, не могут быть остановлены или изменены другими процессами без признака PPL.

Использование признака PPL для служб программы позволяет защитить службы от вредоносных воздействий извне и попыток компрометации.

► *Чтобы настроить защиту служб программы технологией PPL через интерфейс командной*

строки, выполните следующие действия:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Выполните одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --ppl=show [--pwd=<текущий пароль пользователя>]`, чтобы просмотреть текущий статус защиты служб программы технологией PPL.
   - `agent.exe --ppl=disable [--pwd=<текущий пароль пользователя>]`, чтобы отключить защиту служб программы технологией PPL.

Коды возврата команды `--ppl`:

- 0 – команда выполнена успешно.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 8 – ошибка прав доступа.

Управление параметрами самозащиты

► *Чтобы управлять параметрами самозащиты через интерфейс командной строки Kaspersky Endpoint Agent, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   `agent.exe --selfdefence=<enable|disable>`

Управление фильтрацией событий

► *Чтобы управлять фильтрацией событий через интерфейс командной строки Kaspersky Endpoint Agent, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.

3. Выполните следующую команду и нажмите на клавишу **ENTER**:

```
agent.exe --event
=<createprocess|loadimage|registry|network|eventlog|filechange|accountl
oggon|codeinjection> --action=<enable|disable|show>
```

Управление сетевой изоляцией

► *Чтобы получить информацию о текущем состоянии сетевой изоляции через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.
3. Введите команду `agent.exe --isolation=show` и нажмите на клавишу **ENTER.**

   Команда выводит в консоль текущие параметры сетевой изоляции на устройстве, включая список заданных сетевых профилей исключений, а также список правил, заданных в сетевых профилях.

Коды возврата команды `--isolation`:

- -1 – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 9 – неверная операция (например, попытка отключения сетевой изоляции, если сетевая изоляция не включена).

Управление стандартными задачами поиска IOC

Стандартные задачи поиска IOC – задачи, которые создаются вручную в Kaspersky Security Center или через интерфейс командной строки.

► *Чтобы создать и настроить стандартную задачу поиска IOC через интерфейс командной строки, выполните следующие действия:*

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **ENTER**.

3. Выполните следующую команду и нажмите на клавишу **ENTER**:

```
agent.exe --scan-ioc {[--path=<путь к папке с IOC-файлами>] | [<полный путь к IOC-файлу>]} [--process=no] [--hint=<полный путь к исполняемому файлу процесса|полный путь к файлу>] [--registry=no] [--dnsentry=no] [--arpentry=no] [--ports=no] [-services=no] [--system=no] [--users=no] [--volumes=no] [--eventlog=no] [--datetime=<дата публикации события>] [--channels=<список каналов>] [--files=no] [--drives=<all|system|critical|custom>] [--excludes=<список исключений>][--scope=<настраиваемый список папок>]
```

Если команда `--scan-ioc` передана только с обязательными параметрами, Kaspersky Endpoint Agent выполняет проверку с параметрами по умолчанию.

Если команда `--scan-ioc` передана с двумя обязательными параметрами одновременно (`--path=<путь к папке с IOC-файлами>` и `<полный путь к IOC-файлу>`), Kaspersky Endpoint Agent выполняет проверку всех переданных IOC-файлов.

Таблица 26. Параметры команд при запуске и настройке стандартных задач поиска IOC

Параметры	Описание
`--scan-ioc`	Обязательный параметр. Запускает стандартную задачу поиска IOC на устройстве.
`--path=<путь к папке с IOC-файлами>`	Путь к папке с IOC-файлами, по которым требуется выполнять поиск. Обязательный параметр, если не задан параметр `<полный путь к IOC-файлу>`.
`<полный путь к IOC-файлу>`	Полный путь к IOC-файлу с расширением ioc или xml, по которому требуется выполнять поиск. Обязательный параметр, если не задан параметр `--path=<путь к папке с IOC-файлами>`. Передается без аргумента `--path`.

`--process=<no>`	Необязательный параметр. Параметр выключает анализ данных о процессах при проверке. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не учитывает запущенные на устройстве процессы при выполнении проверки. Если в IOC-файле указаны IOC-термины IOC-документа ProcessItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет данные о процессах, только если IOC-документ ProcessItem описан в переданном на проверку IOC-файле.
`--hint=<полный путь к исполняемому файлу процесса|полный путь к файлу>`	Необязательный параметр. Параметр позволяет сузить область анализируемых данных для проверки IOC-документов ProcessItem и FileItem, путем указания конкретного файла. В качестве значения параметра может быть задан: • `<полный путь к исполняемому файлу процесса (ProcessItem)>` – ProcessItem • `<полный путь к файлу>` – FileItem Параметр может быть передан только совместно с аргументами `--process=yes` и `--files=yes`.
`--dnsentry=no`	Необязательный параметр. Параметр выключает анализ данных о записях в локальном кеше DNS (IOC-документ DnsEntryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет локальный кеш DNS. Если в IOC-файле указаны термины IOC-документа DnsEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет локальный кеш DNS, только если IOC-документ DnsEntryItem описан в переданном на проверку IOC-файле.

`--arpentry=no`	Необязательный параметр. Параметр выключает анализ данных о записях в ARP-таблице (документ ArpEntryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет таблицу ARP. Если в IOC-файле указаны термины IOC-документа ArpEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет ARP-таблицу, только если IOC-документ ArpEntryItem описан в переданном на проверку IOC-файле.
`--ports=no`	Необязательный параметр. Параметр выключает анализ данных о портах, открытых на прослушивание (документ PortItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет таблицу активных соединений на устройстве. Если в IOC-файле указаны термины IOC-документа PortItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет таблицу активных соединений, только если IOC-документ PortItem описан в переданном на проверку IOC-файле.
`--services=no`	Необязательный параметр. Параметр выключает анализ данных о службах, установленных на устройстве (документ ServiceItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет данные о службах, установленных на устройстве. Если в IOC-файле указаны термины IOC-документа ServiceItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет данные о службах, только если IOC-документ ServiceItem описан в переданном на проверку IOC-файле.

`--volumes=no`	Необязательный параметр. Параметр выключает анализ данных о томах (документ VolumeItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет данные о томах на устройстве. Если в IOC-файле указаны термины IOC-документа VolumeItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет данные о томах, только если IOC-документ VolumeItem описан в переданном на проверку IOC-файле.
`--eventlog=no`	Необязательный параметр. Параметр выключает анализ данных о записях в журнале событий Windows (документ EventLogItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет записи в журнале событий Windows. Если в IOC-файле указаны термины IOC-документа EventLogItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет записи в журнале событий Windows, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.

`--datetime=<дата публикации события>`	Необязательный параметр. Параметр позволяет включать и выключать учет даты публикации события в журнале событий Windows при определении области поиска IOC для соответствующего IOC-документа. При поиске IOC Kaspersky Endpoint Agent будет обрабатывать только события, опубликованные в период с указанного времени и даты и до момента выполнения задачи. В качестве значения параметра Kaspersky Endpoint Agent позволяет задать дату публикации события. Проверка будет выполняться только для событий, опубликованных в журнале событий Windows после указанной даты и до момента выполнения проверки. Если параметр не передан, Kaspersky Endpoint Agent проверяет события с любой датой публикации. Параметр TaskSettings::BaseSettings::EventLogItem::datetime недоступен для редактирования. Параметр используется, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.
`--channel=<список каналов>`	Необязательный параметр. Параметр позволяет передать список имен каналов (журналов), для которых требуется выполнить поиск IOC. Если этот параметр передан, при выполнении задачи поиска IOC Kaspersky Endpoint Agent будет учитывать только события, опубликованные в указанных журналах. Имя журнала задается в формате строки, в соответствии с именем журнала (канала), указанного в свойствах этого журнала (параметр Full Name) или в свойствах события (параметр <Channel></Channel> в xml-схеме события). По умолчанию (в том числе, если параметр не передан) поиск IOC выполняется для каналов Application, System, Security. Параметру может быть передано несколько значений (через пробел). Параметр используется только в том случае, если IOC-документ EventLogItem описан в переданном на проверку IOC.

`--system=no`	Необязательный параметр. Параметр выключает анализ данных об окружении (IOC-документ SystemInfoItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не анализирует данные об окружении. Если в IOC-файле указаны термины IOC-документа SystemInfoItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent анализирует данные об окружении, только если IOC-документ SystemInfoItem описан в переданном на проверку IOC-файле.
`--users=no`	Необязательный параметр. Параметр выключает анализ данных о пользователях (IOC-документ UserItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не анализирует данные о пользователях, созданных в системе. Если в IOC-файле указаны термины IOC-документа UserItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent анализирует данные о пользователях, созданных в системе, только если IOC-документ UserItem описан в переданном на проверку IOC-файле.
`--files=no`	Необязательный параметр. Параметр выключает анализ данных о файлах (IOC-документ FileItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не анализирует данные о файлах. Если в IOC-файле указаны термины IOC-документа FileItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent анализирует данные о файлах, только если IOC-документ FileItem описан в переданном на проверку IOC-файле.

`--drives=<all|system|critical|custom>`	Необязательный параметр. Параметр позволяет задать область поиска IOC при анализе данных для IOC-документа FileItem. Можно задать одно из следующих значений параметра: • `<all>` – программа проверяет все доступные файловые области. • `<system>` – программа проверяет только файлы, расположенные в папках, в которых установлена ОС. • `<critical>` – программа проверяет только временные файлы в пользовательских и системных папках. • `<custom>` – программа проверяет только файлы в указанных пользователем областях. Если параметр не передан, проверка выполняется в критических областях.
`--excludes=<список исключений>`	Необязательный параметр. Параметр позволяет задать области исключений при анализе данных для IOC-документа FileItem. В параметре можно передать несколько путей через пробел. Если параметр не передан, проверка выполняется без исключений.
`--scope=<настраиваемый список папок>`	Необязательный параметр. Параметр становится обязательным, если передан параметр `--drives=custom`. Параметр позволяет задать список областей проверки. В параметре можно передать несколько путей через пробел.

Коды возврата команды `--scan-ioc`:

- `-1` – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Agent выводит в командную строку следующие данные о результатах

выполнения задачи:

Таблица 27. Данные, которые программа выводит в командную строку при обнаружении IOC.

`Uuid`	Идентификатор IOC-файла из заголовка структуры IOC-файла (тег `<ioc id="">`)
`Name`	Описание IOC-файла из заголовка структуры IOC-файла (тег `<description></description>`)
`Matched Indicator Items`	Перечень идентификаторов всех сработавших индикаторов.
`Matched objects`	Данные по каждому документу IOC, по которому было найдено совпадение.

Настройка сертифицированной конфигурации программы Kaspersky Endpoint Agent.

Программа Kaspersky Endpoint Agent находится в сертифицированной (безопасной) конфигурации, если параметры программы находятся в рамках указанных далее значений:

- При установке программы выбран компонент Интеграция с KATA.
- Активация программы выполнена с помощью файла ключа EDR Expert.
- Отключено использование Kaspersky Security Network, или в свойствах Сервера администрирования настроен Локальный KSN (подробнее см. в *Справке Kaspersky Security Center*).
- Включена интеграция с KATA Central Node.
- В параметрах интеграции с KATA Central Node задано использование одновременно TLS-сертификата и клиентского сертификата.
- Отключено применение политики для раздела параметров сетевой изоляции.
- Создана задача обновления баз и модулей программы с расписанием запуска каждый день.
- В параметрах задачи обновления баз и модулей программы задано значение отличное от **Загружать и устанавливать критические обновления модулей программы**.

Если вы меняете какие-либо из перечисленных выше значений параметров в сертифицированной конфигурации программы на другие значения, вы выводите программу из сертифицированной конфигурации.

Следующие действия также выводят программу из сертифицированной конфигурации:

- Удаление компонента Интеграция с KATA.
- Активация программы с помощью кода активации.

kaspersky

Создание резервной копии и восстановление программы

Вы можете создать резервную копию Kaspersky Endpoint Detection and Response, а затем восстановить программу из резервной копии.

Если вы не используете режим распределенного решения и multitenancy и используете отдельный сервер Central Node, вы можете создать резервную копию данных этого сервера Central Node.

Если вы используете режим распределенного решения и multitenancy, вы можете:

1. Создать резервную копию данных PCN.
2. Создать резервную копию данных SCN. При восстановлении данных из резервной копии SCN роль сервера изменится с SCN на отдельный сервер Central Node.

Выполняйте действия по созданию резервной копии программы на том сервере, резервную копию данных которого вы хотите создать.

В Kaspersky Endpoint Detection and Response могут содержаться данные пользователей и другая конфиденциальная информация. Администратору Kaspersky Endpoint Detection and Response необходимо обеспечить безопасность этих данных самостоятельно при создании резервной копии программы, замене оборудования, на которое установлена программа, и в прочих случаях, когда может потребоваться удаление данных без возможности восстановления. Администратор Kaspersky Endpoint Detection and Response несет ответственность за доступ к данным, хранящимся на серверах программы.

Вы можете создать резервную копию следующих данных:

- Базы данных программы.
- Объектов в Хранилище.
- Файлов из обнаружений, выполненных при повторной проверке (rescan).
- Артефактов Sandbox.
- Конфигурационных файлов.
- Данных о лицензии KEDR.
- Параметров Central Node или PCN:
  - Если вы используете отдельный сервер Central Node, создается резервная копия параметров Central Node.
  - Если вы используете режим распределенного решения и multitenancy и работаете на сервере PCN, создается резервная копия параметров PCN.
  - Если вы используете режим распределенного решения и multitenancy и работаете на сервере SCN, вы можете создать резервную копию SCN, но при восстановлении данных из резервной копии роль сервера изменится с SCN на отдельный сервер Central Node.

Вы можете очистить директорию перед созданием резервной копии программы.

Перед восстановлением программы из резервной копии на сервере Central Node или PCN, на котором вы выполняете восстановление программы, происходит очистка:

- Базы данных программы.
- Объектов в Хранилище.
- Файлов из обнаружений, выполненных при повторной проверке (rescan).
- Артефактов Sandbox.
- Конфигурационных файлов.
- Данных о лицензии KEDR.
- Параметров Central Node или PCN.

Таблица 28. Состав и объем данных, экспортируемых для создания резервной копии программы

Максимальный объем данных	Тип данных	Экспортируемые данные	Режим работы с программой
4 ГБ	Параметры Central Node Базы данных программы на Central Node: • обнаружения и наличие у обнаружений статуса VIP; • результаты выполнения задач; • политики; • пользовательские правила TAA (IOA) и исключения; • IOC-файлы; • белые списки объектов; • информация о файлах в Хранилище; • информация об объектах на карантине; • список компьютеров с Endpoint Agent; • отчеты и шаблоны отчетов; • уведомления.	Параметры Central Node – по выбору. Базы данных программы – по умолчанию.	Отдельный сервер Central Node.
4 ГБ	Параметры PCN.	По выбору.	Режим распределенного решения и multitenancy.
4 ГБ	Параметры SCN.	По выбору. Как для отдельного сервера Central Node.	Режим распределенного решения и multitenancy.

Максимальный объем данных	Тип данных	Экспортируемые данные	Режим работы с программой
4 ГБ	Базы данных программы на PCN: • обнаружения и наличие у обнаружений статуса VIP; • результаты выполнения задач; • политики; • пользовательские правила TAA (IOA) и исключения; • IOC-файлы; • белые списки объектов; • информация о файлах в Хранилище; • информация об объектах на карантине; • список компьютеров с Endpoint Agent; • отчеты и шаблоны отчетов; • уведомления.	По умолчанию.	Режим распределенного решения и multitenancy.
Нет	Конфигурационные файлы.	Да	Все режимы.
Нет	Лицензии KEDR.	Да	Все режимы.
300 ГБ	Хранилище.	По выбору.	Все режимы.
300 ГБ	Артефакты Sandbox.	По выбору.	Все режимы.
300 ГБ	Файлы из обнаружений, выполненных при повторной проверке (rescan).	По выбору.	Все режимы.
Нет	База событий.	Нет.	Все режимы.

Файлы, которые в момент создания резервной копии программы находились в очереди на проверку, не экспортируются.

kaspersky

В этом разделе

Создание резервной копии программы из меню администратора программы

► *Чтобы создать резервную копию программы, выполните следующие действия в меню администратора (см. раздел "Начало работы в меню администратора программы" на стр. 142) сервера:*

1. В списке разделов меню администратора программы выберите раздел **System administration**.
2. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
3. В списке действий выберите **Backup/Restore settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup/Restore settings**.
5. В списке действий выберите **New**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup settings**.
7. Нажмите на кнопку **Back up**.

Резервная копия программы будет создана на сервере.

Загрузка файла с резервной копией программы с сервера Central Node или PCN на жесткий диск компьютера

Рекомендуется сохранять файлы с резервной копией программы на жесткий диск вашего компьютера.

► *Чтобы загрузить файл с резервной копией программы на жесткий диск вашего компьютера, выполните команду в интерфейсе командной строки операционной системы*

Linux на вашем компьютере:

```
scp <имя учетной записи для работы в меню администратора и в консоли управления сервером (см. раздел "Шаг 4. Создание учетной записи для работы в меню администратора и в консоли управления сервером")>@<IP-адрес сервера>:<имя файла с резервной копией программы вида settings-<дата и время создания резервной копии>.tar.gz>
```

Пример:

Команда для загрузки на жесткий диск вашего компьютера архива с резервной копией программы, созданной на сервере Central Node с IP-адресом 10.0.0.10 под учетной записью admin 10 апреля 2020 года в 10 часов 00 минут 00 секунд:

```
scp admin@10.0.0.10:settings-20200410-100000.tar.gz
```

Файл с резервной копией программы будет сохранен на жесткий диск вашего компьютера в текущую директорию.

Загрузка файла с резервной копией программы с вашего компьютера на сервер Central Node

► *Чтобы загрузить файл с резервной копией программы с жесткого диска вашего компьютера на сервер, выполните следующую команду в режиме Technical Support Mode:*

```
scp <имя файла с резервной копией программы вида settings-<дата и время создания резервной копии>.tar.gz> <имя учетной записи для работы в меню администратора и в консоли управления сервером (см. раздел "Шаг 4. Создание учетной записи для работы в меню администратора и в консоли управления сервером")>@<IP-адрес сервера>:
```

Пример:

Команда для загрузки архива с резервной копией программы, созданной 10 апреля 2020 года в 10 часов 00 минут 00 секунд, на сервер Central Node с IP-адресом 10.0.0.10 под учетной записью admin:

```
scp settings-20200410-100000.tar.gz admin@10.0.0.10:
```

Файл с резервной копией программы будет загружен на сервер Central Node в текущую директорию.

kaspersky

Восстановление программы из резервной копии через меню администратора программы

Для восстановления программы из резервной копии необходимо предварительно создать резервную копию текущего состояния программы (см. раздел "Создание резервной копии программы из меню администратора программы" на стр. 480) и загрузить ее на жесткий диск вашего компьютера. В случае сбоя при восстановлении программы или необходимости переустановить программу вы сможете воспользоваться сохраненной копией программы.

► *Чтобы восстановить программу из уже созданной ранее резервной копии, выполните следующие действия в меню администратора (см. раздел "Начало работы в меню администратора программы" на стр. 142) сервера:*

1. В списке разделов меню администратора программы выберите раздел **System administration**.
2. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
3. В списке действий выберите **Backup/Restore settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup/Restore settings**.
5. В списке файлов с резервными копиями программы выберите файл, из которого вы хотите восстановить программу.

   Если нужного файла нет в списке, вам необходимо загрузить файл с резервной копией программы на сервер.
6. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
7. В списке действий выберите **Restore <имя файла с резервной копией программы>**.
8. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения действия.
9. Нажмите на кнопку **Restore**.

Программа будет восстановлена из файла с резервной копией программы.

Создание резервной копии программы в режиме Technical Support Mode

► *Чтобы создать резервную копию программы, выполните следующую команду в режиме Technical Support Mode (см. раздел "Начало работы с программой в режиме Technical Support Mode" на стр. 142) сервера:*

```
/opt/kaspersky/apt-base/bin/ie_kata.sh
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Таблица 29. Параметры команды для создания резервной копии

Обязательный параметр	Параметр	Описание
Да	`-b <path>`	Создать файл с резервной копией программы по указанному пути, где <path> – абсолютный или относительный путь к директории, в которой создается файл с резервной копией программы.
Нет	`-q`	Сохранить файлы на карантине.
Нет	`-a`	Сохранить файлы, ожидающие повторной проверки (rescan).
Нет	`-s`	Сохранить артефакты Sandbox.
Нет	`-n`	Сохранить параметры Central Node или PCN.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Если дополнительные параметры не указаны, резервная копия программы будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, белые списки, уведомления).

Все файлы с резервной копией программы сохраняются в один TAR-архив. Имя файла архива: data_kata_ddmmyyyyhhMM, где ddmmyyyy – дата, hhMM – часы и минуты создания резервной копии программы. Имя базы данных резервной копии программы – KATA3.7.sql для резервной копии программы версии 3.7.

Пример:

Команда для создания резервной копии программы со всеми параметрами:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh -b <path> -q -a -s -n -l <filepath>
```

Восстановление программы из резервной копии в режиме Technical Support Mode

► *Чтобы восстановить программу из резервной копии, выполните следующую команду в режиме Technical Support Mode (см. раздел "Начало работы с программой в режиме Technical*

Support Mode" на стр. 142) сервера:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Таблица 30. Параметры команды для восстановления из резервной копии

Обязательный параметр	Параметр	Описание команды
Да	`-r <path>`	Восстановить данные из файла с резервной копией программы, где <path> – абсолютный или относительный путь к директории, в которой находится файл.
Нет	`-c <path>`	Очистить директорию до начала восстановления программы по указанному пути, где <path> – абсолютный или относительный путь к директории, в которой создается файл для обновления программы. Также после выполнения этой команды программа проверяет наличие свободного места на диске.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Пример:

Команда для восстановления программы из резервной копии со всеми параметрами:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh -r <path> - c <path> -l <filepath>
```

kaspersky

Обновление Kaspersky Endpoint Detection and Response

Вы можете обновить Kaspersky Endpoint Detection and Response с версии 3.6 до версии 3.7.

Вы также можете устанавливать пакеты обновлений программы, выпускаемые "Лабораторией Касперского".

Если вы не используете режим распределенного решения и multitenancy и используете отдельный сервер Central Node, вы можете обновить программу на сервере Central Node.

Если вы используете режим распределенного решения и multitenancy:

1. Вы можете обновить программу на сервере PCN. После обновления программы сервер PCN будет относиться к той же организации, к которой он относился до обновления.
2. Если вы хотите обновить программу на сервере SCN, перед обновлением измените роль сервера с SCN на отдельный сервер Central Node.

   Программа обновится на отдельном сервере Central Node.

   После обновления программы вы сможете назначить серверам роль SCN и выбрать организацию, к которой относится сервер SCN (см. раздел "Назначение серверу роли SCN" на стр. 82).
3. После обновления программы всем пользователям с ролью Администратор по умолчанию предоставляется доступ к веб-интерфейсу сервера PCN и всех серверов SCN.

   Если до обновления программы вы настраивали доступ каждого пользователя к веб-интерфейсам SCN индивидуально, вы можете настроить его повторно (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148).

   После обновления всем пользователям с ролью Старший сотрудник службы безопасности и Сотрудник службы безопасности по умолчанию предоставляется доступ к веб-интерфейсу сервера PCN и всех серверов SCN.

   Если до обновления программы вы настраивали доступ каждого пользователя к веб-интерфейсам SCN индивидуально, вы можете настроить его повторно (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148). Для этого выполните следующие действия в веб-интерфейсе сервера PCN:

   1. Добавьте необходимые организации. (см. раздел "Добавление организации на сервере PCN" на стр. 84)
   2. Настройте доступ учетных записей пользователей с ролью Старший сотрудник службы безопасности и Сотрудник службы безопасности к этим организациям и серверам. (см. раздел "Изменение прав доступа учетной записи пользователя веб-интерфейса программы" на стр. 148)
   3. Удалите все SCN, временно отключенные от PCN него при обновлении (см. раздел "Отключение SCN от PCN" на стр. 85).
   4. Повторно подключите к PCN все необходимые SCN (см. раздел "Обработка запросов на подключение SCN к PCN" на стр. 82).

      При этом программа предложит вам выбрать организацию для каждого сервера SCN.

   Доступ пользователей к веб-интерфейсам SCN будет настроен.

Выполняйте действия по обновлению программы на том сервере, на котором вы хотите обновить данные.

В Kaspersky Endpoint Detection and Response могут содержаться данные пользователей и другая конфиденциальная информация. Администратору Kaspersky Endpoint Detection and Response необходимо обеспечить безопасность этих данных самостоятельно при обновлении программы и в прочих случаях, когда может потребоваться удаление данных без возможности восстановления. Администратор Kaspersky Endpoint Detection and Response несет ответственность за доступ к данным, хранящимся на серверах программы.

Обновление программы с версии 3.6 до версии 3.7

Перед обновлением программы с версии 3.6 до версии 3.7 рекомендуется предварительно создать резервную копию текущего состояния программы (см. раздел "Создание резервной копии программы из меню администратора программы" на стр. 480) и загрузить ее на жесткий диск вашего компьютера из меню администратора программы. В случае сбоя при обновлении программы или необходимости переустановить программу вы сможете воспользоваться сохраненной копией программы.

► *Чтобы обновить программу с версии 3.6 до версии 3.7, выполните следующие действия на сервере Central Node:*

1. Запустите образ диска с компонентом Central Node и Sensor Kaspersky Endpoint Detection and Response версии 3.7. Образ диска входит в комплект поставки программы.

   Запустится мастер установки.

2. Выберите установку с диска программы.

   Откроется окно начала установки программы.

3. Нажмите на кнопку **OK**.

   Откроется окно выбора языка для просмотра Лицензионного соглашения и Политики конфиденциальности.

   Для продолжения установки вам нужно просмотреть Лицензионное соглашение и Политику конфиденциальности и принять их условия. Если условия Лицензионного соглашения и Политики конфиденциальности не приняты, установка не выполняется.

4. Выберите язык для просмотра Лицензионного соглашения и Политики конфиденциальности в списке и нажмите на клавишу **ENTER**.

   Например, если вы хотите просмотреть Лицензионное соглашение и Политику конфиденциальности на английском языке, выберите English и нажмите на клавишу **ENTER**..

   Откроется окно с текстом Лицензионного соглашения.

5. Ознакомьтесь с Лицензионным соглашением.

6. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept the terms**.

   Откроется окно с текстом Политики конфиденциальности.

7. Ознакомьтесь с Политикой конфиденциальности.
8. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **I accept the terms**.

   Откроется окно **Select device**.

9. В окне **Select device** в списке дисков выберите диск, на котором установлена программа версии 3.6 и нажмите на клавишу **ENTER**.

   Откроется окно **Select action**.

10. В списке действий выберите **Upgrade**.
11. Нажмите на клавишу **ENTER**.

    Откроется окно с предупреждением о том, что на диске уже установлена программа версии 3.6 и что вы можете обновить программу до новой версии.

12. Нажмите на кнопку **Upgrade**.

    Программа версии 3.7 будет установлена на сервер Central Node. Сервер перезагрузится. Параметры программы, доступные для обновления программы с версии 3.6 до версии 3.7, будут применены.

    После обновления программы вам будет предложено задать минимальную длину пароля администратора и пользователей программы.

13. В поле **Minimal length** введите количество символов. Рекомендуется использовать пароли длиной 12 и более символов.
14. Нажмите на кнопку **Ok**.

После обновления программы необходимо заново добавить лицензионные ключи (см. раздел "Добавление ключа" на стр. 70).

Установка пакетов обновления программы из меню администратора и в режиме Technical Support Mode

Когда "Лаборатория Касперского" выпускает обновления программы, вы можете устанавливать пакеты обновлений программы.

Перед установкой пакетов обновления программы рекомендуется предварительно создать резервную копию текущего состояния программы (см. раздел "Создание резервной копии программы из меню администратора программы" на стр. 480) и загрузить ее на жесткий диск вашего компьютера из меню администратора программы. В случае сбоя при установке пакета обновления программы или необходимости переустановить Kaspersky Endpoint Detection and Response вы сможете воспользоваться сохраненной копией программы.

► *Чтобы загрузить архив с пакетом обновления программы на сервер с компонентом Central Node, выполните следующие действия:*

1. Войдите в консоль управления сервера с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

   Отобразится меню администратора программы.
3. В меню администратора программы выберите режим Technical Support Mode.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Выберите **Yes** и нажмите на клавишу **ENTER**.
6. Выполните команду

   `scp <имя пакета обновления программы>.ktgz <имя пользователя с правами администратора сервера Central Node>@<IP-адрес сервера с компонентом Central Node>:`

   Например, вы можете выполнить команду `scp apt-system-3.7.0-tr-patch-122.ktgz admin@10.10.10.1:`

Вы можете перейти к установке пакета обновления программы.

► *Чтобы установить пакет обновления программы, выполните следующие действия:*

1. Войдите в консоль управления сервера с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

   Отобразится меню администратора программы.
3. В меню администратора программы выберите пункт **System administration**.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно выбора действия.
5. Выберите **Install patch** и нажмите на клавишу **ENTER**.

   Отобразится окно со списком пакетов обновлений программы, доступных к установке.
6. Выберите пакет обновления программы, который вы хотите установить, и нажмите на клавишу **ENTER**.

   Отобразится окно выбора действия.
7. Выберите действие **Validate and install <имя пакета обновления программы>.ktgz** и нажмите на клавишу **ENTER**.

   Пакет обновления программы будет установлен. Потребуется перезагрузка сервера.
8. Выберите **Go back** и нажмите на клавишу **ENTER**.

Отобразится меню администратора программы.

9. В меню администратора программы выберите пункт **Reboot the machine** и нажмите на клавишу **ENTER**.

   Сервер с компонентом Central Node перезагрузится.

Установка пакета обновления программы будет завершена.

kaspersky

Устранение уязвимостей и установка критических обновлений системы Kaspersky Endpoint Detection and Response

"Лаборатория Касперского" может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (http://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (http://www.bdu.fstec.ru, https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).

По адресу электронной почты vulnerability@kaspersky.com.

На форуме "Лаборатории Касперского" (http://forum.kaspersky.com).

► *Чтобы загрузить архив с пакетом обновления программы на сервер с компонентом Central Node, выполните следующие действия:*

1. Войдите в консоль управления сервера с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы. Отобразится меню администратора программы.
3. В меню администратора программы выберите режим Technical Support Mode.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Выберите **Yes** и нажмите на клавишу **ENTER**.
6. Выполните команду

   ```
   scp <имя пакета обновления программы>.ktgz <имя пользователя с правами администратора сервера Central Node>@<IP-адрес сервера с компонентом Central Node>:
   ```

   Например, вы можете выполнить команду `scp apt-system-3.7.0-tr-patch-122.ktgz admin@10.10.10.1:`

Вы можете перейти к установке пакета обновления программы.

► *Чтобы установить пакет обновления программы, выполните следующие действия:*

1. Войдите в консоль управления сервера с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

   Отобразится меню администратора программы.
3. В меню администратора программы выберите пункт **System administration**.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно выбора действия.
5. Выберите **Install patch** и нажмите на клавишу **ENTER**.

   Отобразится окно со списком пакетов обновлений программы, доступных к установке.
6. Выберите пакет обновления программы, который вы хотите установить, и нажмите на клавишу **ENTER**.

   Отобразится окно выбора действия.
7. Выберите действие **Validate and install <имя пакета обновления программы>.ktgz** и нажмите на клавишу **ENTER**.

   Пакет обновления программы будет установлен. Потребуется перезагрузка сервера.
8. Выберите **Go back** и нажмите на клавишу **ENTER**.

   Отобразится меню администратора программы.
9. В меню администратора программы выберите пункт **Reboot the machine** и нажмите на клавишу **ENTER**.

   Сервер с компонентом Central Node перезагрузится.

Установка пакета обновления программы будет завершена.

В Kaspersky Endpoint Detection and Response могут содержаться данные пользователей и другая конфиденциальная информация.
Администратору Kaspersky Endpoint Detection and Response необходимо обеспечить безопасность этих данных самостоятельно при создании резервной копии программы, обновлении программы, замене оборудования, на которое установлена программа и в прочих случаях, когда может потребоваться удаление данных без возможности восстановления. Администратор Kaspersky Endpoint Detection and Response несет ответственность за доступ к данным, хранящимся на серверах Kaspersky Endpoint Detection and Response.

В случае сбоя программы рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" или переустановить Kaspersky Endpoint Detection and Response.

kaspersky

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе (см. раздел "Источники информации о программе" на стр. 493), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

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

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

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

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2b).

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

Техническая поддержка через Kaspersky CompanyAccount

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

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

Портал Kaspersky CompanyAccount доступен на следующих языках:

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

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

kaspersky

Глоссарий

A

Advanced persistent threat (APT)

Сложная целевая атака на IT-инфраструктуру организации с одновременным использованием различных методов проникновения в сеть, закрепления в сети и получения регулярного доступа к конфиденциальным данным.

Anti-Malware Engine

Ядро программы. Выполняет проверку файлов и объектов на вирусы и другие программы, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.

B

Backdoor-программа

Программа, которую злоумышленники устанавливают на взломанном компьютере для того, чтобы повторно получать доступ к этому компьютеру.

C

Central Node

Компонент программы. Выполняет проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс программы.

CSRF-атака

Cross-Site Request Forgery (также "XSRF-атака"). Атака на пользователей веб-сайтов, использующая уязвимости HTTP-протокола. Атака позволяет производить действия от имени авторизованного пользователя уязвимого веб-сайта. Например, от имени авторизованного пользователя уязвимого веб-сайта злоумышленник может тайно отправлять запрос на сервер сторонней платежной системы для перевода денег на счет злоумышленника.

E

End User License Agreement

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

Endpoint Agent

Компонент программы. Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми

соединениями и изменяемыми файлами.

I

ICAP-данные

Данные, полученные по протоколу ICAP (Internet Content Adaptation Protocol). Протокол позволяет фильтровать и изменять данные HTTP-запросов и HTTP-ответов. Например, производить антивирусную проверку данных, блокировать спам, запрещать доступ к персональным ресурсам. В качестве ICAP-клиента обычно выступает прокси-сервер, который взаимодействует с ICAP-сервером, используя протокол ICAP. Kaspersky Endpoint Detection and Response получает данные с прокси-сервера вашей организации после их обработки на ICAP-сервере.

IOA

Indicator of Attack (индикатор атаки). Описание подозрительного поведения объектов в IT-инфраструктуре организации, которое может являться признаком целевой атаки на эту организацию.

IOA-правило

Один признак подозрительного поведения объекта в IT-инфраструктуре организации, при совпадении с которым Kaspersky Endpoint Detection and Response считает событие обнаружением. IOA-правило содержит описание признака атаки и рекомендации по противодействию.

IOC

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

Файл, содержащий набор индикаторов IOC, при совпадении с которыми программа считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

K

Kaspersky Anti Targeted Attack Platform

Решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "*APT*"). Решение включает функциональные блоки KEDR и KATA.

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Kaspersky Threat Intelligence Portal

Информационная система "Лаборатории Касперского". Содержит и отображает информацию о репутации файлов и URL-адресов.

KATA

Kaspersky Anti Targeted Attack. Функциональный блок программы Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту периметра IT-инфраструктуры предприятия.

KEDR

Kaspersky Endpoint Detection and Response. Функциональный блок программы Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту компьютеров локальной сети организации.

M

MITM-атака

Man in The Middle (человек посередине). Атака на IT-инфраструктуру организации, при которой злоумышленник перехватывает канал связи между двумя точками доступа, ретранслирует и при необходимости изменяет связь между этими точками доступа.

Multitenancy

Режим работы, при котором программа может использоваться для защиты инфраструктуры нескольких организаций одновременно.

N

NTP-сервер

Сервер точного времени, использующий протокол Network Time Protocol.

O

Open IOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

kaspersky

S

Sandbox

Компонент программы. Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации.

Sensor

Компонент программы. Выполняет прием данных.

SIEM-система

Система Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

Syslog

Стандарт отправки и записи сообщений о происходящих в системе событиях, используемый на платформах UNIX™ и GNU/Linux.

T

Targeted Attack Analyzer

Модуль программы. Выполняет статистический анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации. Выполняет поиск признаков сетевой активности, на которую пользователю программы рекомендуется обратить внимание, а также признаков целевых атак на IT-инфраструктуру организации.

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

Y

YARA

Модуль программы. Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями программы.

YARA-правила

Общедоступная классификация вредоносных программ, содержащая сигнатуры признаков целевых атак и вторжений в IT-инфраструктуру организации, по которым программа производит проверку файлов и объектов.

kaspersky

А

Альтернативный поток данных

Потоки данных файловой системы NTFS (alternate data streams), предназначенные для размещения дополнительных атрибутов или информации к файлу.

Каждый файл в файловой системе NTFS представляет собой набор потоков (streams). В основном потоке находится содержимое файла. Остальные (альтернативные) потоки предназначены для размещения метаинформации. Потоки можно создавать, удалять, сохранять отдельно, переименовывать и даже запускать как процесс.

Альтернативные потоки могут использоваться злоумышленниками для скрытой передачи или получения данных с компьютера.

Атака "нулевого дня"

Атака на IT-инфраструктуру организации, использующая уязвимости "нулевого дня" в программном обеспечении, которые становятся известны злоумышленникам до момента выпуска производителем программного обеспечения обновления, содержащего исправления.

В

Вредоносные веб-адреса

Веб-адреса ресурсов, распространяющих вредоносное программное обеспечение.

Д

Дамп

Содержимое рабочей памяти процесса или всей оперативной памяти системы в определенный момент времени.

Л

Локальная репутационная база KPSN

База данных репутаций объектов (файлов или URL-адресов), которая хранится на сервере Kaspersky Private Security Network, а не на серверах Kaspersky Security Network. Управление локальными репутационными базами осуществляется администратором KPSN.

П

Пропускная способность канала связи

Наибольшая возможная в данном канале связи скорость передачи информации.

kaspersky

Р

Распределенное решение

Двухуровневая иерархия серверов с установленными компонентами Central Node, в которой выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*.

С

Сигнатура

Код в базах систем защиты информации, содержащий описание известных угроз.

Статус VIP

Статус обнаружений с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователям с ролью **Сотрудник службы безопасности**.

Т

Техника MITRE

База знаний MITRE ATT&CK https://attack.mitre.org/ (Adversarial Tactics, Techniques & Common Knowledge – Тактики, техники и общеизвестные знания о злоумышленниках) содержит описание поведения злоумышленников, основанное на анализе реальных атак. Представляет собой структурированный список известных техник злоумышленников в виде таблицы.

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

У

Угрозы нового поколения

Угрозы IT-инфраструктуре организации, способные перезаписывать, изменять, зашифровывать или искажать свои коды так, чтобы невозможно было обнаружить совпадение с сигнатурой в системе защиты информации.

Уязвимость "нулевого дня"

Уязвимость в программном обеспечении, обнаруженная злоумышленниками до момента выпуска производителем программного обеспечения обновления, содержащего исправленный код программы.

kaspersky

Ф

Фишинговые URL-адреса

URL-адреса ресурсов, занимающихся получением неправомерного доступа к конфиденциальным данным пользователей. Как правило, целью фишинга является кража различных финансовых данных.

Ц

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apple, Macintosh и Safari – товарные знаки Apple Inc.

Snort – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

Citrix, Citrix Hypervisor и XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

ESET и ESET NOD32 – товарные знаки или зарегистрированные товарные знаки ESET, spol. s r.o.

Google, Google Chrome – товарные знаки Google, Inc.

Intel, Xeon и 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.

McAfee – товарный знак или зарегистрированный в США и других странах товарный знак McAfee, Inc.

Microsoft, Active Directory, Excel, Hyper-V, PowerPoint, Win32, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

CentOS – товарный знак компании Red Hat, Inc.

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

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

VMware ESXi и 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.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации.

Таблица 31. Таблица соответствия терминов

Термин в документации	Термин в требованиях
Программа	Продукт, объект оценки, программное изделие
Вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
Администратор веб-интерфейса	Администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

Приложение. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на сертифицированную конфигурацию программы. В таблице ниже приведены значения этих параметров в сертифицированной конфигурации программы.

Если вы меняете какие-либо из перечисленных значений параметров (диапазон значений) в сертифицированной конфигурации программы на другие значения, вы выводите программу из сертифицированной конфигурации.

Таблица 32. Параметры и их значения при работе программы в сертифицированной конфигурации

Раздел / подраздел, к которому относится параметр	Название параметра	Значение параметра в сертифицированной конфигурации
Параметры – Отправка уведомлений	**Добавить** (Добавить правило отправки уведомлений)	Администратор должен создать и включить правило отправки уведомлений о событиях обнаружения вторжений и нарушения безопасности.
Параметры – Отправка уведомлений	**Отключить** (Отключить правило отправки уведомлений)	Отключение правил отправки уведомлений может привести к выходу из сертифицированной конфигурации.
Параметры – Отправка уведомлений	**Удалить** (Отключить правило отправки уведомлений)	Удаление правил отправки уведомлений может привести к выходу из сертифицированной конфигурации.
Параметры – Endpoint Sensors	**Предупреждение** Количество дней бездействия Endpoint Sensors, при котором программа отображает предупреждение.	Установка значений, превышающих значение по умолчанию, может привести к выходу из сертифицированной конфигурации.
Параметры – Endpoint Sensors	**Критическая (активность Endpoint Sensors)** Количество дней бездействия Endpoint Sensors, которое программа отображает как критическое.	Установка значений, превышающих значение по умолчанию, может привести к выходу из сертифицированной конфигурации.

Раздел / подраздел, к которому относится параметр	Название параметра	Значение параметра в сертифицированной конфигурации
Параметры – YARA-правила	**Удалить**	Удаление файла YARA-правил может привести к выходу из сертифицированной конфигурации.