kaspersky

Kaspersky Endpoint Agent

Содержание

Справка Kaspersky Endpoint Agent

Kaspersky Endpoint Agent - программа, которая устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации. Программа осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Kaspersky Endpoint Agent взаимодействует с другими решениями "Лаборатории Касперского" для обнаружения комплексных угроз (таких как таргетированные атаки).

Функционал программы Kaspersky Endpoint Agent зависит от программного решения, в составе которого используется программа.

В этой справке приведены инструкции по управлению и настройке Kaspersky Endpoint Agent без привязки к определенному решению. Часть описанного функционала может быть недоступна в рамках решения, которое вы используете.

Полную информацию о Kaspersky Endpoint Agent для Windows в составе программного решения, которое вы используете, а также полную информацию о самом решении смотрите в справке соответствующего решения:

- в *Справке Kaspersky Anti Targeted Attack Platform*;
- в *Справке Kaspersky Sandbox*;
- в *Справке Kaspersky Endpoint Detection and Response Optimum*;
- в *Справке Kaspersky Managed Detection and Response*.

Информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу:

- в *Справке Kaspersky Anti Targeted Attack Platform*;
- в *Справке Kaspersky Managed Detection and Response*.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent - программа, которая устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации. Программа осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Kaspersky Endpoint Agent взаимодействует с другими решениями "Лаборатории Касперского" для обнаружения комплексных угроз (таких как таргетированные атаки).

Комплект поставки Kaspersky Endpoint Agent

В комплект поставки программы Kaspersky Endpoint Agent входят следующие файлы:

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.ini	Конфигурационный файл, необходимый для создания инсталляционного пакета англоязычной версии Kaspersky Endpoint Agent с помощью Kaspersky Security Center.
agent\kpd.loc\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\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.
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.

Если Kaspersky Endpoint Agent устанавливается через Kaspersky Security Center при помощи инсталляционного пакета программы с веб-сервера "Лаборатории Касперского", в состав дистрибутива также входит конфигурационный файл install_props.json.

Аппаратные и программные требования

Аппаратные и программные требования

Минимальные аппаратные требования для рабочей станции:

- Процессор: 1.4 ГГц (одноядерный).
- Оперативная память: 1ГБ.
- Объем свободного места на диске: 500 МБ.

Минимальные аппаратные требования для сервера:

- Процессор: 1.4 ГГц (одноядерный).
- Оперативная память: 512МБ.
- Объем свободного места на диске: 500 МБ.

Поддерживаемые операционные системы для рабочих станций:

- Windows 7 SP1 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 19H1 (версия 1903) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 19H2 (версия 1909) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 20H1 (версия 2004) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 20H2 (версия 2009) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 21H1 Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.

Поддерживаемые серверные операционные системы:

- Windows Server 2008 SP2 Standard / Enterprise 64-разрядная.
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 64-разрядная.
- Windows Server 2012 Foundation / Standard / Enterprise / Datacenter 64-разрядная.
- Windows Server 2012 R2 Foundation / Standard / Enterprise / Datacenter 64-разрядная.
- Windows Server 2016 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 Essentials / Standard / Datacenter 64-разрядная.

Поддерживаемые встраиваемые операционные системы:

- Windows Embedded Standard 7 SP1 32-разрядная / 64-разрядная.

Следующие операционные системы поддерживаются только для сценариев интеграции с Kaspersky Industrial CyberSecurity for Networks:

- Windows XP SP2 Professional 32-разрядная.
- Windows Vista SP2 32-разрядная / 64-разрядная.
- Windows Server 2003 SP2 Standard / Enterprise 32-разрядная / 64-разрядная.
- Windows 7 SP1 Ultimate 32-разрядная / 64-разрядная.
- Windows XP Embedded (POS Ready) 32-разрядная.
- Windows Embedded 8.0 Standard 32-разрядная / 64-разрядная.
- Windows Embedded 8.1 Industry Pro 32-разрядная / 64-разрядная.
- Windows 10 IoT Enterprise 32-разрядная / 64-разрядная.

При создании инсталляционного пакета в Kaspersky Security Center версии 12 и выше для установки Kaspersky Endpoint Agent на устройства под управлением Windows XP необходимо использовать файл запуска установки (setup.exe) из инсталляционного пакета, созданного в Kaspersky Security Center версии 10.5.

Для управления программой Kaspersky Endpoint Agent с помощью Kaspersky Security Center Web Console требуется Google Chrome для Windows.

Совместимость программы Kaspersky Endpoint Agent версии 3.11 с предыдущими версиями Kaspersky Endpoint Agent

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

Доступна установка программы Kaspersky Endpoint Agent 3.11 на устройство с программой Endpoint Sensor версии 3.5 и ниже, установленной в составе Kaspersky Endpoint Security. Программы работают независимо и без конфликтов.

Обновление с предыдущей версии Kaspersky Endpoint Agent до версии 3.11 доступно только для Kaspersky Endpoint Agent версий 3.7 и выше. Обновление возможно для предыдущих версий программы, установленных как в составе программ Endpoint Protection Platform, так и отдельно.

Плагин управления Kaspersky Endpoint Agent версии 3.11 и Веб-плагин Kaspersky Endpoint Agent версии 3.11 совместимы с Kaspersky Endpoint Agent версий 3.7 и выше.

Интеграция программы Kaspersky Endpoint Agent 3.11 с программами Endpoint Protection Platform "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.11 поддерживает интеграцию со следующими программами Endpoint Protection Platform "Лаборатории Касперского" (далее также "EPP"):

- Kaspersky Endpoint Security для Windows: 11.2, 11.3, 11.4, 11.5, 11.6, 11.7.
- Kaspersky Security для Windows Server: 11, 11.0.1.
- Kaspersky Security для виртуальных сред 5.2 Легкий агент.

Информацию о доступных функциях Endpoint Detection and Response см. в справке соответствующей программы EPP.

Интеграция программы Kaspersky Endpoint Agent 3.11 с другими программами и решениями "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.11 поддерживает интеграцию со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center версий 10.5, 11 и 12.1.
- Kaspersky Security Center Cloud Console.
- Kaspersky Sandbox 1.0.
- Kaspersky Anti Targeted Attack Platform 3.7.1, 3.7.2.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Поддерживаемые интеграционные сценарии Kaspersky Endpoint Agent 3.11 и их ограничения

Поддерживаемые интеграционные сценарии и их ограничения

Программа EPP	Версия EPP	Версия программного решения "Лаборатории Касперского"			Ограничения
		Kaspersky Sandbox	Kaspersky Anti Targeted Attack Platform	Kaspersky Endpoint Detection and Response Optimum	
Kaspersky Endpoint Security для Windows	11.2, 11.3	1.0	3.7.1, 3.7.2	Не поддерживается	• Программа EPP не интегрируется с Kaspersky Anti Targeted Attack Platform (только совместимость) • Kaspersky Anti Targeted Attack Platform версии 3.7.1 принимает ограниченный объем данных от Kaspersky Endpoint Agent версии 3.11

	11.4	1.0	3.7.1, 3.7.2	1.0	• Kaspersky Endpoint Agent не передает Kaspersky Anti Targeted Attack Platform данные о событии **AMSI-проверка** • Kaspersky Anti Targeted Attack Platform версии 3.7.1 принимает ограниченный объем данных от Kaspersky Endpoint Agent версии 3.11
	11.5, 11.6	1.0	3.7.1, 3.7.2	1.0	Kaspersky Anti Targeted Attack Platform версии 3.7.1 принимает ограниченный объем данных от Kaspersky Endpoint Agent версии 3.11
Kaspersky Security для Windows Server	11, 11.0.1	1.0	3.7.1, 3.7.2	1.0	• Kaspersky Endpoint Agent не передает Kaspersky Anti Targeted Attack Platform данные о событии **AMSI-проверка** • Kaspersky Anti Targeted Attack Platform версии 3.7.1 принимает ограниченный объем данных от Kaspersky Endpoint Agent версии 3.11
Kaspersky Security для виртуальных сред Легкий агент	5.2	1.0	3.7.1, 3.7.2	1.0	• Kaspersky Endpoint Agent не передает Kaspersky Anti Targeted Attack Platform данные о событии **AMSI-проверка** • Kaspersky Anti Targeted Attack Platform версии 3.7.1 принимает ограниченный объем данных от Kaspersky Endpoint Agent версии 3.11

Совместимость Kaspersky Endpoint Agent с антивирусными программами других производителей

На устройствах, на которые вы хотите установить программу Kaspersky Endpoint Agent, может быть установлена антивирусная программа Bitdefender GravityZone Advanced Business Security.

Что нового

В Kaspersky Endpoint Agent 3.11 для Windows исправлены известные ошибки, в полном объеме сохранены возможности предыдущих версий, а также реализованы новые функции:

- Добавлена интеграция с сервером Kaspersky Industrial CyberSecurity for Networks, на который отправляется EDR-телеметрия, которую программа регистрирует на устройствах.
- Расширен список поддерживаемых старых версий операционных систем: Windows XP SP2, Windows Vista SP2, Windows Server 2003 SP2, Windows 7 SP1 Ultimate.
- Добавлена поддержка новых версий операционных систем: Windows 10 21H1, Windows Server 2012 x64 Datacenter.
- Добавлен режим ретроспективного сканирования IOC, а также расширен перечень поддерживаемых типов IOC-документов.
- Реализована возможность автоматического определения критичных системных объектов и исключения их удаления или блокировки в рамках ответных действий, вызываемых из карточки инцидента.
- Реализована возможность автоматического определения Kaspersky Endpoint Agent необходимости подключаться через прокси-сервер к компоненту KATA Central Node при настройке параметров через плагин управления или веб-плагин управления Kaspersky Endpoint Agent.
- Добавлена поддержка ротации файлов журналов трассировки при настройке параметров через плагин управления или веб-плагин управления Kaspersky Endpoint Agent.
- В плагине управления Kaspersky Endpoint Agent добавлена сортировка списка исключений для EDR-телеметрии.

Ограничения текущей версии программы Kaspersky Endpoint Agent

В Kaspersky Endpoint Agent версии 3.11 известны следующие ограничения:

1. Компонент запрета открытия документов не запрещает открытие документа, подпадающего под критерии применяющегося правила, если документ открыт с использованием OLE-автоматизации.
2. Перед отправкой событий телеметрии на KATA Central Node программа Kaspersky Endpoint Agent сохраняет данные в очередь событий. Если очередь событий превышает 10000 необработанных событий, часть событий будет удалена и не будет отправлена на компонент KATA Central Node.
3. При работе программы Kaspersky Endpoint Agent на устройствах с операционной системой Windows 7 программа исключает из телеметрии данные о сетевых соединениях, относящихся к процессам с идентификаторами PID=4 и PID=0.
4. Если программа Kaspersky Endpoint Agent используется на одном устройстве с программой Kaspersky Endpoint Security, и в программе Kaspersky Endpoint Security установлен компонент, обеспечивающий файловое шифрование (FLE), то программа Kaspersky Endpoint Agent не регистрирует события телеметрии о загрузке модулей (LoadImage) и не отправляет их компоненту KATA Central Node.
5. Если при настройке параметров исключения из сетевой изоляции для критерия "Приложение" указано больше одной программы, Kaspersky Endpoint Agent разрешит подключение только для первой программы из списка. Сетевые подключения для остальных указанных программ будут проигнорированы. Ограничение воспроизводится при изоляции устройств, работающих под управлением операционных систем Windows 7 и Windows Server 2008 R2.

6. При проверке индикаторов компрометации, поиск которых предполагает разбор текстовых строк, по условию "is" учитывается наличие пробелов, а также необходимость экранировать описание индикатора в IOC-файле символами CDATA. Например, чтобы обнаружить объект с копирайтом "Copyright (C) 1998-2017 Mark Russinovich " по условию "is", необходимо указать описание индикатора в следующем формате: <Content type="string"><![CDATA[Copyright (C) 1998-2017 Mark Russinovich]]></Content>. Для упрощения описания индикаторов можно также использовать условие "contains".

7. Kaspersky Endpoint Agent может дважды отображать данные о сработавшем объекте при выводе результатов задачи поиска IOC.

8. Установщик не может остановить службу soyuz до тех пор, пока не завершится инициализация службы. Например, установщик возвращает ошибку "Неверный пароль" при попытке удалить или изменить конфигурацию программы сразу после завершения установки, так как служба soyuz не завершила инициализацию и не может быть остановлена.

9. При проверке объектов по IOC-документу FileItem Kaspersky Endpoint Agent пропускает объекты, доступ к которым ограничен, например, файлы, с которыми на момент проверки работают другие программы. Для таких объектов Kaspersky Endpoint Agent возвращает ложно-отрицательный результат проверки.

10. При несовпадении локализации Kaspersky Endpoint Agent и плагина управления Kaspersky Endpoint Agent в Kaspersky Security Center некоторые параметры могут некорректно отображаться в выводах команд "show" в командную консоль.

11. При поиске индикаторов, включающих перебор модулей, загруженных в адресное пространство, Kaspersky Endpoint Agent пропускает случаи, в которых система загружает 64-разрядные модули в 32-разрядные процессы. Например, загрузка wowcpu64.dll в system32 или загрузка ntdll в system32 не будут обнаружены. Ограничение воспроизводится в операционных системах Windows Server 2008 R2 и Windows 7 x64.

12. При попытке запуска Установщика Kaspersky Endpoint Agent с правами учетной записи пользователя, в имени которого содержатся китайские иероглифы, работа Установщика завершается ошибкой. Рекомендуется выполнять установку программы с правами учетной записи Local System, например, запускать установку средствами Kaspersky Security Center.

13. Невозможно восстановить или удалить Kaspersky Endpoint Agent с устройства, если нарушена целостность модуля agent.exe (утилита командной строки Kaspersky Endpoint Agent).

14. В Kaspersky Endpoint Agent реализована функция запуска и исполнения службы Kaspersky Endpoint Agent (soyuz.exe) с признаком PPL. Эта функция обеспечивается драйвером klelaml.sys. Нарушение целостности драйвера klelaml.sys приводит к сбою при загрузке операционной системы. В этом случае рекомендуется использовать системные утилиты восстановления Windows. Отсутствие драйвера klelaml.sys при включенном признаке PPL для процесса soyuz.exe не приводит к сбою операционной системы, но вызывает аварийное завершение Kaspersky Endpoint Agent. В этом случае рекомендуется запустить Установщик программы для выполнения восстановления в тихом режиме с ключом REINSTALL=Drivers.klelam.

15. Невозможно запустить Установщик Kaspersky Endpoint Agent на устройстве с операционной системой, к которой применяется активная политика CodeIntegrity.

16. В свойствах программы Kaspersky Endpoint Agent в Консоли администрирования (в разделе "Общие") данные о статусе установки программы отображаются некорректно.

17. Для объектов, помещенных на карантин программой Kaspersky Endpoint Agent, не поддерживается отправка на анализ в "Лабораторию Касперского" из карантина Kaspersky Security Center.

18. В секциях параметров для управления доступом на основе ролей (RBAC) в Консоли администрирования, в разделе с правами управления плагином Kaspersky Endpoint Agent отображаются флажки, соответствующие правам "Чтение" и "Выполнение операций с выборками устройств", которые не

применяются к блокам параметров в Kaspersky Security Center. Если вы установите эти флажки, права "Чтение" и "Выполнение операций с выборками устройств" не будут ограничены для указанных пользователей.

19. К некоторым событиям Kaspersky Endpoint Agent, которые публикуются в Консоли администрирования Kaspersky Security Center, не применяются фильтры при построении выборок событий.

20. Не исправлены "косметические" ошибки в интерфейсе программы, например, урезание текста в интерфейсе элементов управления.

21. В результатах выполнения команды agent.exe --help не поддерживается вывод справки для одной указанной команды. В консоль выводится полный перечень всех поддерживаемых утилитой команд.

22. В свойствах объекта, помещенного на карантин в репозиторий Сервера администрирования, в поле "User" записывается имя рабочей группы, а не имя пользователя.

23. Утилита командной строки agent.exe не поддерживает работу с кириллическими символами. Например, если в списке узлов Kaspersky Sandbox в параметрах Kaspersky Endpoint Agent указан узел, адрес которого содержит кириллические символы, вывод команды --sandbox=show может содержать ошибки.

24. Установщик Kaspersky Endpoint Agent и плагина управления Kaspersky Endpoint Agent автоматически выбирает локализацию программы на основе региональных параметров операционной системы на устройстве, где выполняется установка программы или плагина управления:

    - если в операционной системе используется локаль RU-RU, устанавливается русская версия Kaspersky Endpoint Agent или плагина управления Kaspersky Endpoint Agent;

    - если в операционной системе используется любая локаль, отличная от RU-RU, устанавливается английская версия Kaspersky Endpoint Agent или плагина управления Kaspersky Endpoint Agent.

    Локализация программы влияет на язык текстов, используемых при описании модулей программы в системе и при публикации событий работы программы в журнал событий Windows, и на отчеты Kaspersky Security Center. Локализация плагина управления Kaspersky Endpoint Agent влияет на язык текстов, используемых в интерфейсе программы в Консоли администрирования (интерфейс политик, групповых задач и свойств программы). Локализацию программы нельзя настроить вручную.

    Обратите внимание, что при несовпадении региональных параметров на управляемых устройствах и на устройстве с установленным плагином управления Kaspersky Endpoint Agent, локализация интерфейса Kaspersky Endpoint Agent в Консоли администрирования и локализация событий, публикуемых программой в отчеты Kaspersky Security Center, могут не совпадать. Также локализация интерфейса программы в Консоли администрирования и локализация событий, публикуемых программой в отчеты Kaspersky Security Center, могут отличаться от локализации интерфейса Консоли администрирования и интерфейса совместимых EPP в Консоли администрирования.

25. После установки, восстановления, изменения набора компонентов или удаления Kaspersky Endpoint Agent, рекомендуется выполнить перезагрузку ОС в ближайшее доступное время. Это необходимо, потому что часть настроек программы может быть завершена только в момент запуска операционной системы.

26. При создании инсталляционного пакета в Kaspersky Security Center версии 12 и выше для установки Kaspersky Endpoint Agent на устройства под управлением Windows XP необходимо использовать файл запуска установки (setup.exe) из инсталляционного пакета, созданного в Kaspersky Security Center версии 10.5.

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.

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;
- локально с помощью командной строки;
- удаленно с помощью 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.

Локальная установка и удаление Kaspersky Endpoint Agent

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Agent локально на устройстве.

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).

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, восстановление 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
```

Восстановление Kaspersky Endpoint Agent

Ниже приведен пример восстановления программы в неинтерактивном режиме. После запуска восстановления программы в неинтерактивном режиме ваше участие в процессе восстановления не требуется.

Пример:
```
msiexec /i endpointagent.msi REINSTALL=ALL /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 {2948C53C-650C-4F06-89CB-A80BA858F02A} REMOVE=ALL /qn
```
Если программа защищена паролем:
```
msiexec /i {2948C53C-650C-4F06-89CB-A80BA858F02A} 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.

Установка Kaspersky Endpoint Agent с помощью Kaspersky Security Center

Kaspersky Endpoint Agent можно установить с помощью задачи удаленной установки в Kaspersky Security Center. Установка состоит из следующих этапов:

1. Создание инсталляционного пакета.
2. Создание задачи удаленной установки.

Kaspersky Security Center также поддерживает и другие способы установки программ на группы управляемых устройств. Подробнее об установке с помощью задачи удаленной установки и о других способах установки см. в *Справке Kaspersky Security Center*.

При создании инсталляционного пакета в Kaspersky Security Center версии 12 и выше для установки Kaspersky Endpoint Agent на устройства под управлением Windows XP необходимо использовать файл запуска установки (setup.exe) из инсталляционного пакета, созданного в Kaspersky Security Center версии 10.5.

Создание инсталляционного пакета Kaspersky Endpoint Agent

Инсталляционный пакет – набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы.

Создание инсталляционного пакета в Консоли администрирования.

Чтобы создать инсталляционный пакет, выполните следующие действия:

1. В Консоли администрирования перейдите в папку **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Просмотреть актуальные версии программ "Лаборатории Касперского"**.

   Появится список текущих версий программ "Лаборатории Касперского".
3. Выберите инсталляционный пакет Kaspersky Endpoint Agent.
4. Нажмите на кнопку **Загрузить программу и создать инсталляционный пакет**.

   Инсталляционный пакет отображается в списке инсталляционных пакетов.
5. Чтобы изменить свойства инсталляционного пакета, в контекстном меню инсталляционного пакета выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета Kaspersky Endpoint Agent. Вы можете настроить:

   - состав компонентов программы;
   - папку для установки программы;
   - режим восстановления программы;
   - параметры файла ключа для активации программы.

Новый инсталляционный пакет теперь доступен в списке инсталляционных пакетов. Вы можете использовать этот инсталляционный пакет для задачи удаленной установки.

Создание инсталляционного пакета в Web Console и Cloud Console.

Чтобы создать инсталляционный пакет, выполните следующие действия:

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

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета.

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

   Отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Список содержит инсталляционные пакеты только тех программ, которые совместимы с текущей версией Kaspersky Security Center.

4. Выберите инсталляционный пакет Kaspersky Endpoint Agent.

   Откроется окно с информацией об инсталляционном пакете.

5. Ознакомьтесь с информацией и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить и создать инсталляционный пакет** отображается кнопка **Загрузить дистрибутив**. В этом случае вам необходимо выполнить следующие действия:

   a. Нажмите на кнопку **Загрузить дистрибутив**, чтобы загрузить дистрибутив на свой компьютер.

      Дождитесь окончания загрузки файла.

   b. Закройте окно мастера создания инсталляционного пакета и заново запустите мастер.

   c. На первой странице мастера выберите параметр **Создать инсталляционный пакет из файла**.

   d. На второй странице мастера укажите путь к файлу дистрибутива на вашем компьютере.

   e. Следуйте дальнейшим указаниям мастера.

6. Во время создания инсталляционного пакета необходимо принять условия Лицензионного соглашения и Политики конфиденциальности.

7. После завершения загрузки нажмите на кнопку **Закрыть**.

   Выбранный инсталляционный пакет загружен в папку общего доступа Сервера администрирования, во вложенную папку Packages. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.

8. Чтобы изменить свойства инсталляционного пакета, нажмите на имени инсталляционного пакета.

   Откроется окно свойств инсталляционного пакета Kaspersky Endpoint Agent. Вы можете настроить:

   - состав компонентов программы;
   - папку для установки программы;
   - режим восстановления программы;
   - параметры файла ключа для активации программы.

Новый инсталляционный пакет теперь доступен в списке инсталляционных пакетов. Вы можете использовать этот инсталляционный пакет для задачи удаленной установки.

При создании инсталляционного пакета в Kaspersky Security Center версии 12 и выше для установки Kaspersky Endpoint Agent на устройства под управлением Windows XP необходимо использовать файл запуска установки (setup.exe) из инсталляционного пакета, созданного в Kaspersky Security Center версии 10.5.

Создание задачи удаленной установки Kaspersky Endpoint Agent

Для удаленной установки Kaspersky Endpoint Agent с помощью Kaspersky Security Center предназначена задача Удаленная установка программы. Для установки программы задача использует инсталляционный пакет программы.

Создание задачи удаленной установки в Консоли администрирования.

Чтобы создать задачу удаленной установки, выполните следующие действия:

1. В Консоли администрирования перейдите в папку **Сервер администрирования → Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Сервер администрирования Kaspersky Security Center → Удаленная установка программы**.

Шаг 2. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите инсталляционный пакет Kaspersky Endpoint Agent.

Вы можете изменить свойства инсталляционного пакета в Kaspersky Security Center, например, выбрать компоненты программы, которые будут установлены на компьютер.

Шаг 3. Дополнительно

Совместно с Kaspersky Endpoint Agent может быть установлен Агент администрирования. Агент администрирования обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Если вы хотите установить Агент администрирования совместно с Kaspersky Endpoint Agent, выберите инсталляционный пакет Агента администрирования.

Шаг 4. Параметры

Настройте следующие дополнительные параметры программы:

- **Принудительно загрузить инсталляционный пакет**. Выберите средства установки программы:

  - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования устанавливается средствами операционной системы. Далее Kaspersky Endpoint Agent устанавливается средствами Агента администрирования.

  - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в *Справке Kaspersky Security Center*.

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

- **Поведение устройств, управляемых другими Серверами**. Выберите способ установки Kaspersky Endpoint Agent. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

- **Не устанавливать программу, если она уже установлена**. Снимите этот флажок, если вы хотите, например, установить программу более ранней версии.

Шаг 5. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера.

Шаг 6. Выбор устройств, которым будет назначена задача

Выберите устройства, на которые будет установлена программа Kaspersky Endpoint Agent.

Шаг 7. Выбор учетной записи для запуска задачи

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

Шаг 8. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 9. Определение названия задачи

Введите название задачи, например, `Установка Kaspersky Endpoint Agent.`

Шаг 10. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. Установка программы будет выполнена в тихом режиме.

Создание задачи удаленной установки в Web Console и Cloud Console.

Чтобы создать задачу удаленной установки, выполните следующие действия:

1. В главном окне Web Console перейдите в раздел **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Программа** выберите **Kaspersky Security Center**.

2. В раскрывающемся списке **Тип задачи** выберите **Удаленная установка программы**.

3. В поле **Название задачи** введите короткое описание, например, `Установка Kaspersky Endpoint Agent`.

4. В разделе **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор компьютеров для установки

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

Шаг 3. Настройка параметров инсталляционного пакета

На этом шаге настройте параметры инсталляционного пакета:

1. Выберите инсталляционный пакет Kaspersky Endpoint Agent.

2. Выберите инсталляционный пакет Агента администрирования.

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

3. В блоке **Принудительно загружать инсталляционный пакет** выберите средства установки программы:

   - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования устанавливается средствами операционной системы. Далее Kaspersky Endpoint Agent устанавливается средствами Агента администрирования.

   - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на управляемые устройства средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в *Справке Kaspersky Security Center*.

- **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на управляемые устройства будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на управляемом устройстве не установлен Агент администрирования, но управляемое устройство находится в той же сети, что и Сервер администрирования.

4. В поле **Максимальное количество одновременных загрузок** установите ограничение количества запросов к Серверу администрирования для загрузки инсталляционного пакета. Ограничение запросов позволит избежать перегрузки сети.

5. В поле **Количество попыток установки** установите ограничение попыток установить программу. Если установка Kaspersky Endpoint Agent завершается с ошибкой, задача автоматически запускает установку повторно.

6. Если требуется, снимите флажок **Не устанавливать программу, если она уже установлена**. Это позволит, например, установить программу более ранней версии.

7. Если требуется, снимите флажок **Предварительно проверять тип операционной системы перед загрузкой**. Это позволит избежать загрузки дистрибутива программы, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютера соответствует программным требованиям, проверку можно пропустить.

8. Если требуется, установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**. Установка Kaspersky Endpoint Agent выполняется средствами Агента администрирования или средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

9. Если требуется, установите флажок **Предлагать пользователю закрыть работающие программы**. Установка Kaspersky Endpoint Agent требует ресурсов компьютера. Для удобства пользователя мастер установки программы предлагает закрыть работающие программы перед началом установки. Это позволит избежать замедление в работе других программ и возможных сбоев в работе компьютера.

10. В блоке **Поведение устройств, управляемых другими Серверами** выберите способ установки Kaspersky Endpoint Agent. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

Шаг 4. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера.

Шаг 5. Выбор учетной записи для запуска задачи

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

Шаг 6. Завершение создания задачи

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

Установка средств администрирования Kaspersky Endpoint Agent

Этот раздел содержит информацию о том, как установить плагин управления Kaspersky Endpoint Agent для управления Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center или веб-плагин управления Kaspersky Endpoint Agent для управления Kaspersky Endpoint Agent в Kaspersky Security Center Web Console.

Установка и обновление плагина управления Kaspersky Endpoint Agent

Для управления Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center вам потребуется установить плагин управления Kaspersky Endpoint Agent.

Чтобы установить плагин управления Kaspersky Endpoint Agent,

скопируйте файл klcfginst.msi, входящий в комплект поставки, на устройство с установленной Консолью администрирования Kaspersky Security Center и запустите его.

Запустится мастер установки программы.

Обновление предыдущей установленной версии плагина управления Kaspersky Endpoint Agent

Обновление доступно только для плагинов управления Kaspersky Endpoint Agent версий 3.7 и выше.

При установке плагина на устройство с установленной предыдущей версией плагина:

- все значения параметров (включая созданные и настроенные политики, групповые и локальные задачи) переносятся в новую версию плагина, а предыдущая установленная версия плагина автоматически удаляется;
- параметры Kaspersky Endpoint Agent, которые были недоступны в обновляемой версии плагина, доступны к настройке и имеют значения по умолчанию;

  Чтобы применить ранее недоступные параметры, необходимо внести и сохранить любое изменение в нужную политику или задачу после обновления плагина.

- шаблоны политик, созданные в обновляемой версии плагина, доступны в новой версии плагина.

Вы можете использовать новый плагин для управления предыдущими версиями программы Kaspersky Endpoint Agent. При этом Kaspersky Endpoint Agent не поддерживает параметры, появившиеся в новой версии плагина. Неподдерживаемые параметры не применяются.

Установка и обновление веб-плагина управления Kaspersky Endpoint Agent

Для управления Kaspersky Endpoint Agent с помощью Kaspersky Security Center Web Console вам потребуется установить веб-плагин управления Kaspersky Endpoint Agent.

Вы можете установить веб-плагин следующими способами:

- С помощью мастера первоначальной настройки Kaspersky Security Center Web Console.
- Из списка доступных дистрибутивов в Kaspersky Security Center Web Console.

  Подробная информация об установке веб-плагинов управления доступна в справке Kaspersky Security Center.
- Загрузив дистрибутив в Kaspersky Security Center Web Console из стороннего источника.

  Для установки веб-плагина требуется добавить ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Agent в интерфейсе Web Console (Параметры Консоли → Плагины). Дистрибутив веб-плагина вы можете загрузить, например, с веб-сайта "Лаборатории Касперского".

Обновление предыдущей установленной версии веб-плагина управления Kaspersky Endpoint Agent

При установке плагина на устройство с установленной предыдущей версией плагина:

- все значения параметров (включая созданные и настроенные политики, групповые и локальные задачи) переносятся в новую версию плагина, а предыдущая установленная версия плагина автоматически удаляется;
- параметры Kaspersky Endpoint Agent, которые были недоступны в обновляемой версии плагина, доступны к настройке и имеют значения по умолчанию;

  > Чтобы применить ранее недоступные параметры, необходимо внести и сохранить любое изменение в нужную политику или задачу после обновления плагина.

- шаблоны политик, созданные в обновляемой версии плагина, доступны в новой версии плагина.

Вы можете использовать новый плагин для управления предыдущими версиями программы Kaspersky Endpoint Agent. При этом Kaspersky Endpoint Agent не поддерживает параметры, появившиеся в новой версии плагина. Неподдерживаемые параметры не применяются.

Обновление предыдущей версии Kaspersky Endpoint Agent

В процессе установки Kaspersky Endpoint Agent 3.11 на устройство с установленной предыдущей версией Kaspersky Endpoint Agent все данные, которые можно перенести, сохраняются и используются при установке Kaspersky Endpoint Agent 3.11, а предыдущая версия программы автоматически удаляется.

Обновление с предыдущей версии Kaspersky Endpoint Agent до версии 3.11 доступно только для Kaspersky Endpoint Agent версий 3.7 и выше. Обновление возможно для предыдущих версий программы, установленных как в составе программ Endpoint Protection Platform, так и отдельно.

Если на устройстве установлен и используется Endpoint Sensor версии 3.6.X в составе Kaspersky Endpoint Security, необходимо 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.

При обновлении Kaspersky Endpoint Agent в составе EPP можно передать пароль в качестве значения ключа `UNLOCK_PASSWORD` в конфигурационном файле install_props.json.

Пароль программы, передаваемый через конфигурационный файл install_props.json, хранится в файле в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется ограничить доступ к файлу install_props.json и удалить его с устройства после установки или обновления программы.

При установке путем обновления предыдущей версии Kaspersky Endpoint Agent, если обновляемая версия активирована, новая версия программы автоматически активируется лицензионным ключом от обновляемой версии программы. Срок действия лицензии остается без изменений. При обновлении программы с истекшим сроком действия лицензии новая версия программы после установки работает в режиме ограниченной функциональности.

Только при обновлении с Kaspersky Endpoint Agent версии 3.7 доступна активация программы во время обновления. Можно передать файл ключа одним из указанных способов.

Начиная с версии 3.10 в Kaspersky Endpoint Agent нет возможности настроить использование службы Kaspersky Managed Protection (далее KMP). Если в предыдущей установленной версии Kaspersky Endpoint Agent было включено использование службы KMP, то после обновления программы до версии 3.10 и выше служба KMP продолжает работать как раньше. После обновления вы можете отключить службу KMP только при помощи Плагина управления Kaspersky Endpoint Agent или Веб-плагина Kaspersky Endpoint Agent версий ниже 3.10.

Восстановление Kaspersky Endpoint Agent

Установщик Kaspersky Endpoint Agent, запущенный вами в режиме Восстановление, проверяет и восстанавливает целостность всех поврежденных модулей программы и ключей системного реестра, созданных при установке программы.

Вы можете запустить установщик в режиме восстановления одним из следующих способов:

- локально с помощью Мастера установки Kaspersky Endpoint Agent;
- локально с помощью командной строки;
- удаленно с помощью Kaspersky Security Center, выполнив одно из следующих действий (подробнее см. в *справке Kaspersky Security Center*):
  - установив флажок **Выполнять восстановление, если программа уже установлена** при создании инсталляционного пакета;
  - указав параметр `REINSTALL=ALL` при создании пользовательского инсталляционного пакета.

Если установщик Kaspersky Endpoint Agent запущен в режиме восстановления, а *программа не требует восстановления*, то установщик не выполняет никаких изменений на устройстве.

Если установщик Kaspersky Endpoint Agent запущен в режиме восстановления, а *программа не установлена на устройстве*, то будет запущена установка программы.

Если установщик Kaspersky Endpoint Agent запущен в режиме восстановления локально с помощью командной строки или удаленно с помощью с помощью Kaspersky Security Center, а *параметры установленной программы отличаются от параметров, указанных при запуске установщика*, то запустится режим изменения параметров установленной программы.

Изменения в системе после установки Kaspersky Endpoint Agent

При установке Kaspersky Endpoint Agent служба установщика Windows выполняет на защищаемом устройстве следующие изменения:

- создает папки Kaspersky Endpoint Agent;
- регистрирует в системном реестре ключи Kaspersky Endpoint Agent;
- регистрирует службы и драйверы Kaspersky Endpoint Agent.

Папки Kaspersky Endpoint Agent на защищаемом устройстве

При установке Kaspersky Endpoint Agent на устройстве создаются следующие папки:

- Заданная по умолчанию папка установки Kaspersky Endpoint Agent, содержащая исполняемые файлы Kaspersky Endpoint Agent:
  - В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\
  - В 64-х разрядной версии Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\
- Папка, содержащая драйверы Kaspersky Endpoint Agent(x86):

- В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\drivers\<версия_ОС>\<имя драйвера>
- В 64-х разрядной версии Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\drivers\x64\<версия ОС>\<имя драйвера>

- Папки, содержащие файлы IOC:
  - В 32-х разрядной версии Microsoft Windows:
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.1
  - В 64-х разрядной версии Microsoft Windows:
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.1
- Папки, содержащие служебные файлы Kaspersky Endpoint Agent:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Images
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kata
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kmp
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Syslog
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Hunts
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\killchain
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Settings
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Tasks
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\DSKM
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp\Tasks
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Bases

- Папка, содержащая служебные файлы для работы с Kaspersky Security Network.
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Ksn
- Папка, содержащая файлы, помещенные на карантин:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Quarantine
- Папка, содержащая файлы, восстановленные из карантина:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Restored
- Папка, содержащая файлы конфигурации политики Kaspersky Security Center:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Policy
- Папки, содержащие служебные файлы для работы с Kaspersky Sandbox:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox\Queue
- Папка, содержащая файлы обновляемых компонентов:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Update
- Папка, содержащая файлы ярлыков для меню Пуск:
  - %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Kaspersky Endpoint Agent

Службы и драйверы Kaspersky Endpoint Agent

Следующие службы Kaspersky Endpoint Agent регистрируются и запускаются под системной учетной записью (SYSTEM):

- SOYUZ.exe – это основная служба Kaspersky Endpoint Agent, которая управляет задачами и рабочими процессами программы.
- VOSTOK.dll (исполняется в proton.exe) – это служба, которая обеспечивает взаимодействие между Kaspersky Endpoint Agent и компонентом Central Node.
- ANGARA.dll (исполняется в proton.exe) – это служба, которая обеспечивает взаимодействие между Kaspersky Endpoint Agent и EPP в сценариях интеграции с Kaspersky Sandbox.

Следующие драйверы Kaspersky Endpoint Agent регистрируются на устройстве:

- klsnsr.sys – это драйвер для работы с трассировкой событий Windows (ETW).
- klncap.sys – это анализатор сетевых пакетов ETW.

  При установке на устройство с ОС Microsoft Windows XP вместо klncap.sys регистрируется драйвер klncapxp.sys.

Ключи системного реестра

В результате установки Kaspersky Endpoint Agent создаются следующие ключи системного реестра:

Ключи системного реестра указаны в представлении для 32-разрядных приложений.

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdDispla
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdVersi
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\NagentMi
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\ProductCode
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\NoPPL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\BFESDDL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EnableKillChain]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\SvmUpdateMode]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\MsiPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\AgentPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EventsExpirationTimeout]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallTime]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLCID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLocalization]

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallPlatformType]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\Version]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration(Example)]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\StartMenu]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\UninstallShortcut2]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\RelNotes]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\License]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Ksn]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Kmp]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\ProductUrl]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\angara]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncap]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncapxp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klsnsr]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vostok]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\soyuz]

Лицензирование программы

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

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Endpoint Agent.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

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

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании 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.

Предусмотрены следующие типы лицензий:

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

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

  Вы можете активировать программу по пробной лицензии только один раз.

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

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

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

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.

О лицензионном ключе

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

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

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

Лицензионный ключ может быть активным и дополнительным (или резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного лицензионного ключа.

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

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Endpoint Agent. Вы получаете код активации по указанному вами адресу электронной почты после приобретения программного решения, в состав которого входит Kaspersky Endpoint Agent, или после заказа пробной версии этого программного решения.

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

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского".

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 программного решения, в состав которого входит Kaspersky Endpoint Agent, или после заказа пробной версии этого программного решения.

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

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

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

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.

Активация Kaspersky Endpoint Agent

Этот раздел содержит информацию об активации Kaspersky Endpoint Agent.

Управление активацией Kaspersky Endpoint Agent

Вы можете активировать Kaspersky Endpoint Agent одним из следующих способов:

- Во время установки программы:
  - указав файл ключа на отдельном шаге Мастера установки;
  - предварительно разместив файл ключа в одной папке с файлом endpointagent.msi при установке в неинтерактивном режиме (в том числе при удаленной установке);
  - указав путь к файлу ключа при помощи параметра `LICENSEKEYPATH` при установке в неинтерактивном режиме (в том числе при удаленной установке).

    При наличии в папке нескольких файлов ключа, Kaspersky Endpoint Agent будет активирован при помощи файла ключа с самой поздней датой окончания срока действия лицензии.

    Если установщик Kaspersky Endpoint Agent не обнаружит файл ключа пригодный для активации Kaspersky Endpoint Agent, то программа будет установлена без активации.

  При установке путем обновления предыдущей версии Kaspersky Endpoint Agent, если обновляемая версия активирована, новая версия программы автоматически активируется лицензионным ключом от обновляемой версии программы. Срок действия лицензии остается без изменений. При обновлении программы с истекшим сроком действия лицензии новая версия программы после установки работает в режиме ограниченной функциональности.

  Только при обновлении с Kaspersky Endpoint Agent версии 3.7 доступна активация программы во время обновления. Можно передать файл ключа одним из указанных способов.

- После установки программы:
  - при помощи задачи активации программы в Консоли администрирования Kaspersky Security Center или Kaspersky Security Center Web Console;
  - через командную строку локально на устройстве.

Вы можете использовать Kaspersky Security Center в качестве прокси-сервера при активации Kaspersky Endpoint Agent.

Информацию о действующей лицензии можно просмотреть в Kaspersky Security Center в разделе **Лицензии Лаборатории Касперского**, в свойствах устройства или через командную строку.

Подробную информацию об управлении ключами с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

После окончания срока действия лицензии программа продолжит работу в режиме ограниченной функциональности.

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.

- Недоступно построение графа цепочки развития угрозы.

- 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, Выполнить программу, 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 в Консоли администрирования Kaspersky Security Center:

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.

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

3. Выберите устройство, для которого вы хотите настроить параметры Kaspersky Endpoint Agent.

4. В контекстном меню устройства выберите пункт **Свойства**.

Откроется окно свойств устройства.

5. Выберите раздел **Программы**.

   В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.

6. 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".

7. Выберите раздел **Ключи**.

Информация о действующей лицензии отобразится в рабочей области окна.

Чтобы посмотреть информацию о действующей лицензии в Kaspersky Security Center Web Console:

1. На закладке **Устройства** выберите **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства перейдите на закладку **Программы**.
4. В списке программ нажмите на **Kaspersky Endpoint Agent**.
5. В открывшемся окне свойств программы перейдите на закладку **Общие** и откройте раздел **Лицензия**.

Отобразится основная информация об активных и резервных лицензионных ключах.

Данные программы Kaspersky Endpoint Agent

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

Для обеспечения основных функций, аудита и повышения скорости решения возникших проблем специалистами Службы технической поддержки "Лаборатории Касперского" Kaspersky Endpoint Agent хранит и обрабатывает данные локально.

На устройствах с Kaspersky Endpoint Agent хранятся данные, подготовленные для автоматической отправки на серверы решений Kaspersky Sandbox, KATA и в Kaspersky Security Center. Файлы хранятся на устройствах с Kaspersky Endpoint Agent в открытом незашифрованном виде в папке, которая по умолчанию используется для хранения файлов перед отправкой.

Администратору решения, в состав которого входит Kaspersky Endpoint Agent, необходимо обеспечить безопасность устройств с Kaspersky Endpoint Agent и серверов решения с перечисленными выше данными самостоятельно. Администратор решения несет ответственность за доступ к данной информации.

В этом разделе содержится следующая информация о персональных данных, хранящихся на устройствах с Kaspersky Endpoint Agent, а также передаваемых в Kaspersky Security Center или на серверы "Лаборатории Касперского":

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

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

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

Конкретный состав данных зависит от решения, в составе которого используется Kaspersky Endpoint Agent.

Служебные данные

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 KATA Central Node;
- данные, обрабатываемые при интеграции с Kaspersky Industrial CyberSecurity for Networks.

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.

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 KATA 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 KATA Central Node:

- Обновляемые схемы фильтрации телеметрии.
- Очередь пакетов событий телеметрии.
- Кеш идентификаторов IOC-файлов, полученных от компонента KATA Central Node.
- Объекты для передачи на сервер в рамках задачи Получить файл.
- Отчеты о результатах задачи Получить список файлов, процессов.

Kaspersky Endpoint Agent хранит локально следующие данные при интеграции с сервером KICS for Networks:

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent:

- 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 KICS for Networks.
  - Данные о лицензии.

2. Данные, необходимые для интеграции с KICS for Networks:

- Обновляемые схемы фильтрации телеметрии.
- Очередь пакетов событий телеметрии.

Данные о событиях Журнала событий Windows

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.

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.
- Об объектах, заблокированных по правилам Запрета запуска.
- О результатах выполнения задач Удалить файл.
- О результатах выполнения задач Завершить процесс.
- О результатах выполнения задач Выполнить программу.
- О результатах выполнения задач Получить файл.
- О действующей лицензии Kaspersky Endpoint Detection and Response Optimum.
- О статусе активации программы.

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

Данные в запросах к Kaspersky Sandbox

При интеграции с решением Kaspersky Sandbox следующие данные из запросов к Kaspersky Sandbox хранятся локально на устройстве:

- MD5-хеш задачи проверки.
- Идентификатор задачи проверки.
- Проверяемый объект и все связанные с ним файлы.

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

Данные, предоставляемые при использовании кода активации

При активации Kaspersky Endpoint Agent с помощью кода активации следующие данные отправляются на сервер активации:

- Тип, идентификатор, версия и локализация установленной программы Kaspersky Endpoint Agent.
- Идентификатор устройства.
- Идентификатор установки Kaspersky Endpoint Agent на компьютере.
- Код активации и уникальный идентификатор активации действующей лицензии.
- Время активации Kaspersky Endpoint Agent.
- Тип, версия и разрядность операционной системы.

Для передачи данных используется защищенный протокол HTTPS с шифрованием при помощи SSL/TLS.

Данные в результатах выполнения задач поиска IOC

Kaspersky Endpoint Agent автоматически передает данные из результатов выполнения задач поиска IOC в Kaspersky Security Center для построения цепочки развития угрозы.

Данные хранятся в базах данных Kaspersky Security Center. По умолчанию данные хранятся 7 дней.

Данные в результатах выполнения задач поиска IOC могут содержать следующую информацию:

- IP-адрес из ARP-таблицы.

- Физический адрес из ARP-таблицы.
- Тип и имя записи DNS.
- IP-адрес защищаемого устройства.
- Физический адрес (MAC) защищаемого устройства.
- Идентификатор записи в журнале событий.
- Имя источника данных в журнале.
- Имя журнала.
- Пользователь.
- Время события.
- MD5-хеш файла.
- SHA256-хеш файла.
- Полное имя файла (включая путь).
- Размер файла.
- Удаленный IP-адрес, с которым было установлено соединение в момент проверки.
- Удаленный порт, с которым было установлено соединение в момент проверки.
- IP-адрес локального адаптера.
- Порт, открытый на локальном адаптере.
- Протокол в виде числа (в соответствии со стандартом IANA).
- Имя процесса.
- Аргументы процесса.
- Путь к файлу процесса.
- Windows идентификатор (PID) процесса.
- Windows идентификатор (PID) родительского процесса.
- Имя учетной записи пользователя, запустившего процесс.
- Дата и время запуска процесса.
- Имя службы.
- Описание службы.
- Путь и имя DLL-службы (для svchost).

- Путь и имя исполняемого файла службы.
- Windows идентификатор (PID) службы.
- Тип службы (например, драйвер ядра или адаптер).
- Статус службы.
- Режим запуска службы.
- Имя учетной записи пользователя.
- Наименование тома.
- Буква тома.
- Тип тома.
- Значение реестра Windows.
- Значение куста реестра.
- Путь к ключу реестра (без куста и без имени значения).
- Параметр реестра.
- Система (окружение).
- Имя ОС с версией.
- Сетевое имя защищаемого устройства.
- Домен или группа, к которой принадлежит защищаемое устройство.
- Имя браузера.
- Версия браузера.
- Время последнего обращения к веб-ресурсу.
- URL из HTTP-запроса.
- Имя учетной записи, под которой выполнен HTTP-запрос.
- Имя файла процесса, выполнившего HTTP-запрос.
- Полный путь к файлу процесса, выполнившего HTTP-запрос.
- Windows идентификатор (PID) процесса, выполнившего HTTP-запрос.
- HTTP referer (URL источника HTTP-запроса).
- URI ресурса, запрошенного по протоколу HTTP.
- Информация о HTTP агенте пользователя (приложении, выполнившем HTTP-запрос).

- Время выполнения HTTP-запроса.
- Уникальный идентификатор процесса, выполнившего HTTP-запрос.

Данные в запросах к компоненту KATA Central Node

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 о запущенных процессах:
  - Имя исполняемого файла, включая полный путь и расширение.
  - Параметры автозапуска процесса.
  - Идентификатор процесса.
  - Код сеанса входа в систему.
  - Имя сеанса входа в систему.
  - Дата и время запуска процесса.
- Данные о файлах:
  - Путь к файлу.
  - Имя файла.
  - Размер файла.
  - Атрибуты файла.
  - Дата и время создания файла.
  - Дата и время последнего изменения файла.
- Данные в ошибках получения информации об объектах:
  - Полное имя объекта, при обработке которого возникла ошибка.
  - Код ошибки.

4. Данные телеметрии:

- Тип данных в реестре до зафиксированной операции изменения.
- Данные в ключе реестра до зафиксированной операции изменения.
- Текст обрабатываемого скрипта или его части.
- Тип обрабатываемого объекта.
- Способ передачи команды в командный интерпретатор.

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.
   - Папки, для которых необходимо получить результаты задачи Получить список файлов, процессов.
   - Маски имен объектов и расширений для задачи Получить список файлов, процессов.
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.

Данные в запросах к серверу KICS for Networks

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

При интеграции с программой Kaspersky Industrial CyberSecurity for Networks следующие данные могут локально храниться на устройстве с Kaspersky Endpoint Agent в папке %ProgramData%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kics.

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

Данные, отправляемые программой Kaspersky Endpoint Agent на сервер Kaspersky Industrial CyberSecurity for Networks:

- Данные сетевых интерфейсов:
  - Описание сетевого интерфейса.
  - Домен.
  - MAC-адрес.
  - Номер метрики.

    - Список IP-адресов, состоящий из набора записей следующего вида: IP-адрес / маска подсети / адрес шлюза.

- Списки патчей:
    - Номер патча.
    - Дата установки патча.
- Списки установленных программ EPP:
    - Имя программы EPP.
    - Версия программы.
    - Версия баз программы.
    - Дата последнего обновления программы.
    - Список лицензионных ключей (номер, тип, срок истечения, статус ключа).
- Данные по установленным сетевым соединениям:
    - Локальный IP-адрес.
    - Локальный MAC-адрес.
    - Удалённый IP-адрес.
    - Удалённый MAC-адрес.
    - IP-адрес шлюза.
    - Тип протокола (по IANA).

Данные для построения цепочки развития угрозы

Данные для построения цепочки развития угрозы хранятся в папке %ProgramData%\Kaspersky Lab\Endpoint Agent\4.0\Data\killchain\detects в открытом незашифрованном виде. По умолчанию данные хранятся 7 дней. Эти данные автоматически передаются в Kaspersky Security Center.

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

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 для построения Цепочки развития угрозы могут содержать следующую информацию:

- Дата и время инцидента.

- Имя обнаружения.
- Режим проверки.
- Статус последнего действия, связанного с обнаружением.
- Причина неудачной обработки обнаружения.
- Тип обнаруженного объекта.
- Имя обнаруженного объекта.
- Статус угрозы после обработки объекта программой EPP.
- Причина неудачного выполнения действий над объектом.
- Действия, выполняемые EPP для отката вредоносных действий (для EPP, поддерживающих Откат вредоносных действий).
- Об обрабатываемом объекте:
  - Уникальный идентификатор процесса.
  - Уникальный идентификатор родительского процесса.
  - Уникальный идентификатор файла процесса.
  - Идентификатор процесса Windows.
  - Командная строка процесса.
  - Имя учетной записи пользователя, запустившего процесс.
  - Код сеанса входа в систему, в котором запущен процесс.
  - Тип сеанса (например, "интерактивный", "удаленный интерактивный"), в котором запущен процесс.
  - Уровень целостности обрабатываемого процесса.
  - Принадлежность учетной записи пользователя, запустившего процесс, к привилегированным локальным и доменным группам (например, "Администраторы", "Администраторы домена", "Администраторы предприятия", "Администраторы схемы").
  - Идентификатор обрабатываемого объекта.
  - Полное имя обрабатываемого объекта.
  - Идентификатор защищаемого устройства.
  - Полное имя объекта (имя локального файла или веб-адрес загружаемого файла).
  - MD5-хеш обрабатываемого объекта.
  - SHA256-хеш обрабатываемого объекта.
  - Тип обрабатываемого объекта.

- Дата создания обрабатываемого объекта.
- Дата последнего изменения обрабатываемого объекта.
- Размер обрабатываемого объекта.
- Атрибуты обрабатываемого объекта.
- Организация, подписавшая обрабатываемый объект.
- Результат проверки цифрового сертификата обрабатываемого объекта.
- Идентификатор безопасности (SID) обрабатываемого объекта.
- Идентификатор часового пояса обрабатываемого объекта.
- Веб-адрес загрузки обрабатываемого объекта (только для файла на диске).
- Название программы, загрузившей файл.
- MD5-хеш программы, загрузившей файл.
- SHA256-хеш программы, загрузившей файл.
- Название программы, последний раз модифицировавшей файл.
- MD5-хеш программы, последний раз модифицировавшей файл.
- SHA256-хеш программы, последний раз модифицировавшей файл.
- Количество запусков обрабатываемого объекта.
- Дата и время первого запуска обрабатываемого объекта.
- Уникальный идентификатор файла.
- Полное имя файла (имя локального файла или веб-адрес загружаемого файла).
- Путь к обрабатываемой переменной реестра Windows.
- Имя обрабатываемой переменной реестра Windows.
- Значение обрабатываемой переменной реестра Windows.
- Тип обрабатываемой переменной реестра Windows.
- Показатель принадлежности обрабатываемого ключа реестра к точке автозапуска.
- Веб-адрес обрабатываемого веб-запроса.
- Источник ссылок обрабатываемого веб-запроса.
- Агент пользователя обрабатываемого веб-запроса.
- Тип обрабатываемого веб-запроса ("GET" или "POST").

- Локальный IP-порт для обрабатываемого веб-запроса.
- Удаленный IP-порт для обрабатываемого веб-запроса.
- Направление соединения ("входящее" или "исходящее") обрабатываемого веб-запроса.
- Идентификатор процесса, в который произошло внедрение вредоносного кода.

Предоставление расширенной диагностической информации Kaspersky Endpoint Agent специалистам Службы технической поддержки

Для оказания поддержки при неполадках в работе программы Kaspersky Endpoint Agent специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия:

- Активировать функциональность получения расширенной диагностической информации.
- Дополнительно настроить отдельные компоненты программы, недоступные для изменения стандартными средствами пользовательского интерфейса.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся информация, необходимая для выполнения перечисленных действий (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и т.д.), а также состав данных, анализируемых в отладочных целях, будут озвучены вам специалистами Службы технической поддержки. Расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка сохраненных данных в "Лабораторию Касперского" не выполняется.

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 документации программы 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.

Данные в файлах трассировки и дампов

Kaspersky Endpoint Agent может выполнять запись отладочной информации в файлы трассировки в соответствии с заданными параметрами. Файлы трассировки используются для получения поддержки при работе с 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 персональные данные пользователей или конфиденциальные данные организации.

Не используйте Kaspersky Endpoint Agent на устройствах, 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 устройства, 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 удалении 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 устройстве.
- Информация об объектах, обрабатываемых Kaspersky Endpoint Agent.
- Ошибки, возникшие в процессе работы Kaspersky Endpoint Agent.

Данные о принятии условий Положения о KSN

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

Данные о принятии условий Положения 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:

- Идентификатор соглашения (KSN, 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.

Сетевая изоляция

Этот раздел содержит информацию о сетевой изоляции и настройке ее параметров.

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.

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, применяются, 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.

Управление сетевой изоляцией

Интерфейс управления	Возможности	Примечания
Консоль администрирования Kaspersky Security Center	• Включение и отключение сетевой изоляции. • Настройка автоматического отключения сетевой изоляции. • Настройка уведомления пользователя устройства о сетевой изоляции. • Настройка исключений из сетевой изоляции.	В свойствах политики вы можете настроить 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. • Отключение сетевой изоляции	Включение сетевой изоляции, а также настройка параметров сетевой изоляции недоступны через интерфейс командной строки.

	на устройстве.	
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.

Запрет запуска

Этот раздел содержит информацию о функции Запрет запуска и настройке ее параметров.

О Запрете запуска

Вы можете управлять правилами запрета запуска исполняемых файлов и скриптов, а также открытия файлов офисного формата на выбранных устройствах. Например, вы можете запретить запуск программ, использование которых считается небезопасным, на выбранном устройстве с Kaspersky Endpoint Agent. Программа идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Правило запрета запуска – это набор критериев, которые учитываются при выполнении блокировки. Объект должен соответствовать всем критериям правила защиты, чтобы программа заблокировала его исполнение.

Параметрами правил запрета запуска можно управлять с помощью Kaspersky Security Center или из командной строки локально на устройстве.

При использовании Kaspersky Endpoint Agent версии 3.9 правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Исполнение или открытие этих файлов *не* будет заблокировано программой.

Режим применения правил запрета запуска

Можно выбрать один из двух режимов применения правил запрета запуска:

- **Только статистика**.

  В этом режиме Kaspersky Endpoint Agent публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках исполнения объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их исполнение или открытие.

- **Активный**.

  В этом режиме Kaspersky Endpoint Agent блокирует исполнение объектов или открытие документов, соответствующих критериям правил запрета.

При включении Запрета запуска в Kaspersky Security Center по умолчанию выбран режим **Только статистика**.

Уведомление пользователя о сработавшем правиле запрета запуска

Вы можете выбрать опцию **Уведомлять пользователя устройства при запрете**. Если Запрет запуска включен в режиме **Активный** и выбрана опция **Уведомлять пользователя устройства при запрете**, на защищаемых устройствах будут отображаться всплывающие уведомления с информацией о сработавших правилах Запрета запуска. Если пользователь устройства не закроет всплывающее уведомление, то оно закроется автоматически через 60 секунд после появления. По умолчанию опция **Уведомлять пользователя устройства при запрете** выключена.

Управление Запретом запуска

Параметрами Запрета запуска можно управлять с помощью Kaspersky Security Center или из командной строки.

С помощью Kaspersky Security Center вы можете:

- включить или отключить использование Запрета запуска;
- выбрать режим применения правил запрета запуска;
- настроить уведомление пользователей о сработавшем правиле запрета запуска;
- настроить список правил запрета запуска;
- включить Запрет запуска из карточки инцидента.

С помощью командной строки вы можете отключить Запрет запуска или просмотреть текущие параметры Запрета запуска.

Поддерживаемые расширения файлов для Запрета запуска

Kaspersky Endpoint Agent поддерживает запрет открытия файлов офисного формата через определенные программы. Информация о поддерживаемых расширениях имен файлов и программ приведена в следующей таблице.

Поддерживаемые расширения имен файлов для запрета открытия через указанные программы

Имя программы	Исполняемый файл	Расширение имени файла
Microsoft Word	winword.exe	• rtf • doc • dot • docm • docx • dotx • dotm • docb
WordPad	wordpad.exe	• docx • rtf

Microsoft Excel	excel.exe	• xls • xlt • xlm • xlsx • xlsm • xltx • xltm • xlsb • xla • xlam • xll • xlw
Microsoft PowerPoint	powerpnt.exe	• ppt • pot • pps • pptx • pptm • potx • potm • ppam • ppsx • ppsm • sldx • sldm
Adobe Acrobat Microsoft Edge Google Chrome	acrord32.exe MicrosoftEdge.exe chrome.exe	• pdf

Поддерживаемые интерпретаторы запуска скриптов

Запрет запуска скрипта обрабатывается Kaspersky Endpoint Agent, если скрипт запущен с помощью одного из следующих интерпретаторов:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe

- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Kaspersky Endpoint Agent поддерживает запрет запуска Java-приложений, работающих в среде выполнения Java (процессы java.exe и javaw.exe).

Поиск IOC

Этот раздел содержит информацию о задачах поиска IOC и настройке их параметров.

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* – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.

- *Автономные задачи поиска IOC* – групповые задачи, которые создаются автоматически при реагировании на угрозы, обнаруженные Kaspersky Sandbox. Kaspersky Endpoint Agent автоматически формирует IOC-файл. Работа с пользовательскими IOC-файлами не предусмотрена. Задачи автоматически удаляются через семь дней после последнего запуска или с момента создания, если задачи не запускались. Подробнее об автономных задачах поиска IOC см. в *Справке Kaspersky Sandbox*.

- *Поиск IOC по IOC-файлам, загружаемым вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform* – 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.

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 настроек в параметрах политик. Для задач доступен режим **Ретроспективный поиск IOC**. 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.	Локальные или групповые

Автономные задачи поиска IOC	Задачи создаются автоматически, если в политике Kaspersky Endpoint Agent задано действие **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.	Групповые
Поиск IOC по IOC-файлам, загружаемым вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform	IOC-файлы загружаются вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform. Также есть возможность настроить расписание IOC-проверки компьютеров с программой Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. 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.

Требования к IOC-файлам

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

При создании задач Поиск IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- 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.
- Размер одного IOC-файла не должен превышать 3 МБ. Использование файлов большего размера приводит к завершению задач Поиск IOC с ошибкой. При этом суммарный размер всех добавленных файлов в IOC-коллекции может превышать 3 МБ.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

Особенности и ограничения поддержки стандарта OpenIOC программой приведены в следующей таблице.

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	Полный список поддерживаемых программой IOC-терминов приведен в отдельной таблице.

Поддерживаемые IOC-термины

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC, поддерживаемых программой Kaspersky Endpoint Agent.

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX

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 Anti Targeted Attack Platform. Описание каждого типа задач поиска IOC и информация о доступных возможностях управления задачами поиска IOC приведены в таблице ниже.

Управление задачами поиска IOC.

Тип задачи	С помощью Kaspersky Security Center	С помощью	Через

		компонента Central Node	интерфейс командной строки

Стандартная задача поиска IOC	• Создание, удаление и запуск задачи вручную.
	• Просмотр детальных отчетов в результатах выполнения задачи в виде сводной таблицы и в карточке обнаруженных IOC.
	• Экспорт IOC-коллекции.
	• Настройка следующих параметров в мастере создания задачи или в свойствах задачи после ее создания:
	  • 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).
		Управление не предусмотрено.	• Создание и запуск задачи с требуемыми параметрами.
			• Просмотр данных о выполнении задачи.

Автономная задача поиска IOC	• Настройка запуска задач. • Запуск и удаление задачи вручную. • Включение выполнения действий по реагированию на угрозы, обнаруженные Kaspersky Sandbox. • Добавление действия автоматического создания Автономной задачи поиска IOC. • Просмотр детальных отчетов в результатах выполнения задачи в виде сводной таблицы и в карточке обнаруженных IOC. • Экспорт IOC-коллекции. • Настройка следующих параметров в свойствах задачи: • Действия программы при обнаружении IOC (помещение объекта на карантин и удаление с устройства; запуск проверки на устройстве с помощью EPP).	Управление не предусмотрено.	Управление не предусмотрено.

	• 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, настройка расписания IOC-проверки.	Управление не предусмотрено.

Работа с карточкой инцидента

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Карточка инцидента автоматически удаляется через один месяц после того, как была сформирована.

В карточке инцидента вы можете ознакомиться с информацией, необходимой для анализа инцидента, а также выполнить действия в качестве реакции на инцидент.

В карточке инцидента приведена следующая информация:

- Граф цепочки развития угрозы. На графе отображается цепочка действий в системе, приведших к инциденту.
- Общая информация об инциденте.
- Информация о защищаемом устройстве, на котором произошел инцидент.
- Сведения об объекте, обнаруженном в ходе инцидента.

Из карточки инцидента вы можете выполнить следующие действия:

- Изолировать устройство, на котором произошел инцидент.
- Поместить файл на карантин.
- Запретить запуск файла, обнаруженного в ходе инцидента.
- Создать задачу Поиск IOC.

Вы также можете воспользоваться функционалом для работы с недоверенными объектами, который доступен в программах Endpoint Protection Platform. Например, вы можете использовать стандартные средства Kaspersky Security Center Web Console, чтобы добавить файл в список разрешенных объектов Контроля запуска программ Kaspersky Endpoint Security для Windows или отправить файл на анализ специалистам "Лаборатории Касперского". Подробнее см. в *справке Kaspersky Endpoint Security для Windows*.

Настройка отчета об угрозах для просмотра карточек инцидентов

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить отчет об угрозах для просмотра карточек инцидентов, выполните следующие действия:

1. В главном окне веб-консоли перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Нажмите на имя отчета **Отчет об угрозах**.
3. В открывшемся окне изменения отчета перейдите на закладку **Графы**.
4. Убедитесь, что в блоке параметров **Детальные данные** в списке полей отчета присутствует поле с именем **Открыть инцидент**.
5. Если поле **Открыть инцидент** отсутствует в списке, выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.
   b. В правой части окна в раскрывающемся списке выберите поле с именем **Открыть инцидент**.
   c. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**.

Просмотр карточки инцидента настроен в параметрах отчета об угрозах.

Предусловия построения цепочки развития угрозы

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Необходимо выполнение следующих предусловий для построения цепочки развития угрозы:

- На управляемом устройстве с установленным Kaspersky Endpoint Agent установлена совместимая версия Endpoint Protection Platform (Kaspersky Security for Windows Server версии 11 или выше или Kaspersky Endpoint Security для Windows версии 11.4.0 или выше).
- Kaspersky Endpoint Agent активирован ключом Kaspersky EDR Optimum или Kaspersky EDR Expert.
- Kaspersky Endpoint Agent и Endpoint Protection Platform находятся под управлением веб-консоли Kaspersky Security Center.
- На устройстве с установленной веб-консолью Kaspersky Security Center установлен веб-плагин Kaspersky Endpoint Agent.
- К устройству применена активная политика, в свойствах которой включено построение цепочки развития угрозы и принудительное применение этих параметров.

  Если к управляемому устройству не применяется политика, необходимо включить построение цепочки развития угрозы в свойствах программы.

  По умолчанию построение цепочки развития угрозы выключено в свойствах программы для управляемого устройства.

Просмотр карточки инцидента

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Карточка инцидента доступна в окне со списком инцидентов. Список инцидентов доступен в отчете **Отчет об угрозах** или в подразделе **Оповещения** в разделе **Мониторинг и отчеты** веб-консоли Kaspersky Security Center или Kaspersky Security Center Cloud Console.

Чтобы программа строила цепочку развития угрозы, необходимо выполнить предусловия построения цепочки развития угрозы.

Если вы добавите лицензионный ключ для EDR Optimum, подраздел **Оповещения** автоматически отобразится в главном меню в разделе **Мониторинг и отчеты**. Вы также можете настроить отображение подраздела **Оповещения** в свойствах интерфейса в Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console. Подробную информацию см. в *Справке Kaspersky Security Center*.

Чтобы просмотреть карточку инцидента в подразделе Оповещения:

1. В главном окне веб-консоли перейдите в раздел **Мониторинг и отчеты** → **Оповещения**.
2. Выберите инцидент и нажмите на ссылку **больше информации**.

   Отобразится карточка инцидента.

Чтобы просмотреть карточку инцидента в отчете об угрозах:

1. В главном окне веб-консоли перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Выберите отчет типа **Отчет об угрозах** и нажмите на кнопку **Показать отчет**.
3. В окне отчета на вкладке **Подробнее** выберите инцидент и нажмите на ссылку **Представить**.

   Отобразится карточка инцидента.

Выбор действия с файлом из карточки инцидента

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Для выполнения правил Запрета запуска на устройстве, на котором произошел инцидент, к этому устройству должна быть применена активная политика Kaspersky Endpoint Agent. Если устройство, на котором произошел инцидент, не находится под управлением активной политики, то правило запрета запуска не будет создано.

Чтобы выбрать действие с файлом из карточки инцидента, выполните следующие действия:

1. Откройте карточку инцидента.
2. Если вы хотите поместить на карантин файл, обнаруженный в ходе инцидента, в блоке **Файл** нажмите на кнопку **Поместить на карантин**.
3. Если вы хотите запретить запуск файла, обнаруженного в ходе инцидента, в блоке **Файл** нажмите на кнопку **Запретить запуск**.

При использовании Kaspersky Endpoint Agent версии 3.9 правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Исполнение или открытие этих файлов *не* будет заблокировано программой.

Изоляция устройства из карточки инцидента

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы изолировать устройство из карточки инцидента, выполните следующие действия:

1. Откройте карточку инцидента.
2. Если вы хотите изолировать устройство, на котором произошел инцидент, в блоке **Устройство** нажмите на кнопку **Изолировать устройство от сети**.

Создание задачи Поиск IOC из карточки инцидента

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы создать задачу Поиск IOC из карточки инцидента, выполните следующие действия:

1. Откройте карточку инцидента.

2. На закладке **Все события инцидента** выберите элементы списка, на основе которых вы хотите создать задачу поиска IOC.

3. Нажмите на кнопку **Создание задачи поиска IOC**.

4. Выполните одно из следующих действий:

   - Если вы хотите, чтобы индикатор компрометации срабатывал при обнаружении любого из выбранных объектов, в правой части экрана выберите **ИЛИ (любой IOC обнаружен)**.

   - Если вы хотите, чтобы индикатор компрометации срабатывал только при обнаружении всех выбранных объектов, в правой части экрана выберите **И (все IOC обнаружены)**.

5. В группе параметров **Действия при обнаружении IOC** выберите одно из следующих действий:

   - **Изолировать устройство от сети**, чтобы программа Kaspersky Endpoint Agent выполняла сетевую изоляцию устройства, на котором обнаружен индикатор компрометации.

   - **Поместить на карантин и удалить**, чтобы поместить обнаруженный объект на карантин и удалить его с устройства.

   - **EPP запустить проверку важных областей на устройстве**, чтобы программа Kaspersky Endpoint Agent отправляла программе EPP команду на выполнение проверки важных областей на всех устройствах группы администрирования, на которых обнаружен индикатор компрометации.

6. Нажмите на кнопку **Создать задачу**.

По умолчанию для задач поиска IOC, созданных из карточки инцидента, используются параметры, описанные в таблице ниже. Вы можете изменять эти значения в параметрах созданной задачи.

Параметры по умолчанию для задачи Поиск IOC, созданной из карточки инцидента

Параметр	Значение по умолчанию	Описание
Параметры на закладке Расписание		
Запускать по расписанию	Опция выбрана.	Задача запускается по расписанию, с заданными параметрами.
Периодичность	**В указанное время**	Задача запускается один раз в указанные дату и время.
Время запуска	Через 15 минут после создания задачи.	Задача запускается в указанное время.
Дата запуска	Дата создания задачи.	Задача запускается в указанную дату.
Завершать задачу, выполняющуюся более	Опция выбрана. Задано значение в 1 час.	Программа завершает задачу через указанное время после запуска вне зависимости от прогресса выполнения задачи.
Отменить расписание с	Опция *не* выбрана.	Автоматическая отмена расписания запуска задачи не применяется.
Запускать пропущенные задачи	Опция выбрана.	Программа перезапускает задачу, которая не была запущена по расписанию по какой-то причине. Например, если служба Kaspersky Endpoint Agent не выполнялась в запланированный момент запуска задачи.
Распределять	Опция выбрана. Задано значение в 10	Задача запустится в произвольный момент

время запуска задач в интервале	минут.	в течение указанного времени от времени, заданного в поле **Время запуска**.
Параметры в разделе Дополнительно		
Выберите типы данных (IOC-документы) для анализа во время поиска IOC	При анализе данных файлов (FileItem) выбрана опция **Анализировать данные файлов (FileItem)**. В дополнительных настройках IOC-документа в блоке параметров **Искать индикаторы компрометации в следующих областях** выбрана опция **Важные области на устройстве**.	Программа проверяет критические области на устройстве, а также папку, в которой изначально был обнаружен опасный объект. К критическим областям относятся следующие: • Временные файлы в папках системных и пользовательских учетных записей. • Временные файлы в папке операционной системы и в папке %TEMP% для учетной записи Local System, если эти пути отличаются.
	При анализе данных реестра Windows (RegistryItem) выбрана опция **Анализировать реестр Windows (RegistryItem)**.	Программа проверяет пути пользовательских разделов реестра.

Kaspersky Endpoint Agent версии 3.9 по умолчанию для задач поиска IOC, созданных из карточки инцидента, использует параметры, заданные в разделе **Интеграция с Kaspersky Sandbox** в блоке параметров **Реагирование на угрозы**. Подробную информацию см. в *Справке Kaspersky Sandbox*.

О виджете EDR-оповещений

В виджете EDR-оповещений отображается информация о количестве инцидентов, обнаруженных на устройствах за последний месяц. Виджет EDR-оповещений доступен для отображения на закладке **Панель мониторинга** в Kaspersky Security Center Web Console или в Kaspersky Security Center Cloud Console. Из виджета EDR-оповещений вы можете открыть раздел **Оповещения** со списком инцидентов, обнаруженных на устройствах.

Чтобы добавить виджет EDR-оповещений на информационную панель:

1. Перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
3. В списке доступных веб-виджетов выберите веб-виджет **Оповещения** в категории **Статистика угроз**.
4. Нажмите на кнопку **Добавить**.

Веб-виджет будет добавлен в конец информационной панели.

О Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum – решение, предназначенное для защиты IT-инфраструктуры организации от сложных кибернетических угроз. Функционал решения сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противостояния сложным атакам, в том числе новым эксплойтам (exploits), программам-шантажистам (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим законные системные инструменты. Решение предназначено для корпоративных пользователей.

Архитектура решения

Решение состоит из следующих компонентов:

- Kaspersky Endpoint Agent в составе Endpoint Protection Platform (например, в составе Kaspersky Endpoint Security) 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 Security Center с Kaspersky Security Center Web Console (или Kaspersky Security Center Cloud Console с облачной Консолью администрирования) позволяют централизованно управлять решением и его настройками через единый веб-интерфейс.

- Kaspersky Sandbox (опциональный компонент – приобретается отдельно) предназначен для дополнительной проверки подозрительных объектов, обнаруженных EPP. Подробную информацию о Kaspersky Sandbox см. в *Справке Kaspersky Sandbox*.

Обнаружение угроз

Kaspersky Endpoint Detection and Response Optimum выполняет обзор и анализ развития угрозы и предоставляет Сотруднику службы безопасности или Администратору информацию о потенциальной атаке, необходимую для принятия своевременных ответных действий.

Карточка инцидента – инструмент для просмотра всей собранной информации об обнаруженной угрозе и управления ответными действиями. Карточка инцидента отображается в Kaspersky Security Center и может содержать, например, следующую информацию об обнаруженной угрозе:

- Граф цепочки развития угрозы.

- Информация об устройстве, на котором обнаружена угроза (например, имя, IP-адрес, MAC-адрес, список пользователей, операционная система).

- Общая информация об обнаружении, включая режим обнаружения (например, обнаружение при сканировании по требованию или при автоматическом сканировании).

- Изменения в реестре, связанные с обнаружением.

- История появления файлов на устройстве.

- Принятые программой ответные действия.

Граф цепочки развития угрозы – инструмент для анализа причин появления угрозы. Граф предоставляет визуальную информацию об объектах, задействованных в инциденте, например, о ключевых процессах на устройстве, сетевых соединениях, библиотеках, кустах реестра.

Решение 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.

Реагирование на угрозы

Функционал реагирования на угрозы имеет следующие автоматические ответные действия, принимаемые программой при обнаружении угроз:

- Помещение объекта на карантин.

- Удаление файла.

- Сетевая изоляция устройства.

- Запуск проверки важных областей на устройстве.

- Запуск поиска индикаторов компрометации (IOC) на группе устройств.

Дополнительно Сотруднику службы безопасности или Администратору доступны следующие действия:

- Помещение объекта в список правил Запрета запуска.

- Запуск процесса на устройстве.

- Завершение процесса на устройстве.

Функционал Kaspersky Endpoint Agent

Kaspersky Endpoint Agent в рамках решения Kaspersky Endpoint Detection and Response Optimum выполняет следующие действия:

- Собирает информацию об обнаружениях от Endpoint Protection Platform (например, от Kaspersky Endpoint Security).

- Дополняет информацию о вердиктах данными, связанными с обнаружением.

- Отправляет данные в Kaspersky Security Center для построения цепочки развития угрозы.

- Запускает задачи поиска индикаторов компрометации (IOC) на группах защищаемых устройств.

- Запускает ответные действия на обнаруженные индикаторы компрометации, например:
  - включает сетевую изоляцию устройства;
  - запускает проверку важных областей на устройстве.
- Отправляет объекты на проверку в Kaspersky Sandbox (если настроена интеграция с Kaspersky Sandbox).

Об интеграции с Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform – решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (далее также "APT"). Программа разработана для корпоративных пользователей.

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

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

Kaspersky Endpoint Detection and Response включает в себя следующие компоненты:

- Central Node.
- Kaspersky Endpoint Agent.

Компоненты взаимодействуют между собой по следующему принципу:

Программа Kaspersky Endpoint Agent устанавливается на отдельных компьютерах под управлением операционных систем Windows, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере отправляются на сервер с компонентом Central Node.

При интеграции сервера Central Node с программой Kaspersky Endpoint Agent вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и программами путем выполнения задач на устройствах с Kaspersky Endpoint Agent.
- Настраивать политики запрета запуска файлов и процессов на выбранных устройствах с Kaspersky Endpoint Agent.
- Изолировать отдельные устройства с Kaspersky Endpoint Agent от сети.
- Работать с правилами TAA (IOA) для классификации и анализа событий.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на устройствах с Kaspersky Endpoint Agent и в базе обнаружений.

Вы можете настроить интеграцию Kaspersky Endpoint Agent с компонентом KATA Central Node в Консоли администрирования Kaspersky Security Center, в Kaspersky Security Center Web Console или через интерфейс командной строки локально на устройстве.

Полную информацию о решении Kaspersky Anti Targeted Attack Platform, а также информацию о настройке интеграции с Kaspersky Endpoint Agent со стороны решения KATA см. в *Справке Kaspersky Anti Targeted Attack Platform*.

Об интеграции с Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response (MDR) обеспечивает круглосуточную защиту от растущего количества угроз, способных обойти автоматические средства защиты, для организаций, которым сложно найти квалифицированных специалистов или у которых ограничены внутренние ресурсы. В отличие от аналогичных предложений на рынке, решение использует успешный опыт эффективного исследования целевых атак для обеспечения непрерывной защиты даже от самых сложных угроз. Решение помогает повысить устойчивость компании к киберугрозам и освободить сотрудников, чтобы они могли сосредоточиться на других задачах.

Kaspersky Endpoint Agent интегрируется в инфраструктуру клиента с помощью Kaspersky Security Center. Kaspersky Endpoint Agent обрабатывает данные и отправляет их в Kaspersky Managed Detection and Response с помощью потоков Kaspersky Security Network.

Вы можете настроить интеграцию Kaspersky Endpoint Agent с решением MDR в Консоли администрирования Kaspersky Security Center или в Kaspersky Security Center Web Console.

Полную информацию о решении Kaspersky Managed Detection and Response, а также информацию о настройке интеграции с Kaspersky Endpoint Agent со стороны решения MDR см. в *Справке Kaspersky Managed Detection and Response*.

Об интеграции с Kaspersky Sandbox

Решение Kaspersky Sandbox обнаруживает и автоматически блокирует сложные угрозы на клиентских устройствах (рабочих станциях, компьютерах, серверах, далее также "рабочих станциях").

Решение разработано для корпоративных пользователей.

Решение Kaspersky Sandbox состоит из:

- Программы Kaspersky Sandbox, отвечающей за серверную часть решения. Kaspersky Sandbox устанавливается на один или несколько серверов внутри сети вашей организации. Серверы можно объединять в кластер. На серверах с Kaspersky Sandbox развернуты виртуальные образы операционных систем Microsoft Windows, в которых запускаются проверяемые объекты. Kaspersky Sandbox анализирует поведение объектов для выявления вредоносной активности и сложных угроз в IT-инфраструктуре организации.

- Программы защиты рабочих станций (Endpoint Protection Platform (далее также "EPP")) Kaspersky Endpoint Security для Windows и Kaspersky Security для Windows Server. Программы Kaspersky Endpoint Security для Windows и Kaspersky Security для Windows Server устанавливаются на рабочих станциях сети вашей организации и обеспечивают комплексную защиту рабочих станций от различного вида угроз, сетевых и мошеннических атак.

- Программы Kaspersky Endpoint Agent для Windows, которая устанавливается в составе EPP. Программа Kaspersky Endpoint Agent для Windows устанавливается на рабочих станциях и серверах сети вашей организации и обеспечивает коммуникацию EPP и Kaspersky Sandbox, а также выполнение действий по автоматическому реагированию на обнаруженные угрозы, настроенных в политиках Kaspersky Security Center.

Вы можете настроить интеграцию Kaspersky Endpoint Agent с решением Kaspersky Sandbox в Консоли администрирования Kaspersky Security Center или через интерфейс командной строки локально на устройстве.

Полную информацию о решении Kaspersky Sandbox, а также информацию о настройке интеграции с Kaspersky Endpoint Agent со стороны решения Kaspersky Sandbox см. в *Справке Kaspersky Sandbox*.

Об интеграции с Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks – программа для защиты инфраструктуры промышленных предприятий от угроз информационной безопасности и для обеспечения непрерывности технологических процессов. Kaspersky Industrial CyberSecurity for Networks анализирует трафик промышленной сети для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети. Программа входит в состав решения Kaspersky Industrial CyberSecurity.

Kaspersky Industrial CyberSecurity for Nodes – это средство комплексной защиты серверов и рабочих станций в промышленных системах управления от информационных угроз.

Программа Kaspersky Endpoint Agent позволяет настроить интеграцию между Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes. Программа Kaspersky Endpoint Agent устанавливается на отдельные устройства с установленной программой Kaspersky Industrial CyberSecurity for Nodes. Данные о событиях на устройстве, собранные программой Kaspersky Industrial CyberSecurity for Nodes, отправляются на сервер Kaspersky Industrial CyberSecurity for Networks посредством Kaspersky Endpoint Agent. Интеграция между программами расширяет возможности Kaspersky Industrial CyberSecurity for Networks по расследованию и реагированию на угрозы в сетях промышленных предприятий.

Вы можете настроить интеграцию Kaspersky Endpoint Agent с программой Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования Kaspersky Security Center, в Kaspersky Security Center Web Console или через интерфейс командной строки локально на устройстве.

Полную информацию о программе Kaspersky Industrial CyberSecurity for Networks, а также информацию о настройке интеграции с Kaspersky Endpoint Agent со стороны программы Kaspersky Industrial CyberSecurity for Networks см. в *Справке Kaspersky Industrial CyberSecurity for Networks*.

В рамках интеграции с Kaspersky Industrial CyberSecurity for Networks программа Kaspersky Endpoint Agent предоставляет только данные об узле, срабатываниях антивирусной программы и информацию о сетевых коммуникациях. Ответные действия на обнаруживаемые угрозы, сетевая изоляция, а также поиск IOC недоступны.

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*.

Консоль администрирования Kaspersky Security Center (далее также *Консоль администрирования*) предоставляет пользовательский интерфейс для работы с Kaspersky Security Center. Консоль администрирования реализована в виде компонента расширения к Консоли управления (Microsoft Management Console, MMC).

Вы можете управлять Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center 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.

Управление политиками Kaspersky Endpoint Agent

В этом разделе приведены инструкции по созданию политик Kaspersky Endpoint Agent и включению параметров в политиках.

Создание политики Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 включили параметр **Использовать параметры политики для предыдущей версии программы**, то по умолчанию выбирается 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:

   - **Интеграция с Kaspersky Sandbox**
   - **Endpoint Detection and Response Expert (KATA EDR)**

7. Нажмите на кнопку **Далее**.

8. 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.

9. 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**.

10. 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.
    - **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организаций.

11. Установите флажок **Открыть свойства политики сразу после создания**, если требуется выполнить дополнительную настройку политики сразу после ее создания.

12. 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. Параметры в разделах политики разделены на блоки. В рамках одной политики вы можете включить как часть блоков, так и все блоки.

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 после сохранения изменений.

Настройка параметров Kaspersky Endpoint Agent

В этом разделе приведены инструкции по настройке параметров Kaspersky Endpoint Agent.

Открытие окна параметров Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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**, кроме параметров сетевой изоляции.

В свойствах политики вы можете настроить параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

Настройка параметров безопасности Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Для обеспечения максимального уровня безопасности IT-инфраструктуры организации вы можете настроить доступ пользователей и сторонних процессов к Kaspersky Endpoint Agent.

Настройка прав пользователей

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете предоставить доступ к Kaspersky Endpoint Agent отдельным пользователям или группам 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 настроены и применены.

Включение защиты паролем

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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.

   Мы рекомендуем задать пароль, который удовлетворяет следующим условиям:
   - Длина пароля составляет не менее 8 символов.
   - Пароль не содержит имя учетной записи пользователя.
   - Пароль не совпадает с именем устройства, на котором установлена программа Kaspersky Endpoint Agent.
   - Пароль содержит символы как минимум трех групп из следующего списка:
     - верхний регистр (A-Z);
     - нижний регистр (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. Мы рекомендуем 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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** включите или выключите параметр **Включить самозащиту модулей программы в памяти**.

   По умолчанию параметр включен.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **OK**.

Механизм самозащиты будет включен или отключен.

Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Программа использует параметры соединения с прокси-сервером для обновления баз, активации программы и работы внешних служб.

Если вы хотите использовать заданный прокси-сервер при соединении с сервером KATA или Kaspersky Sandbox, убедитесь, что выбрана опция **Подключаться через прокси-сервер, если это задано в общих параметрах** при настройке интеграции с KATA или Kaspersky Sandbox. По умолчанию опция не выбрана.

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 **Общие 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 (протокол сетевой аутентификации NT LAN Manager) 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 из учетной записи, которая 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 **Политика не применяется** на **Политика применяется**.

11. Нажмите на кнопку **OK**.

Параметры соединения с прокси-сервером будут настроены.

Настройка Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы включить использование Kaspersky Security Center в качестве прокси-сервера для активации программы:

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 **Общие параметры**.
5. В блоке параметров **Лицензирование** установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **OK**.

Включено использование Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent.

Настройка параметров сетевой изоляции

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе приведены инструкции по настройке параметров сетевой изоляции с помощью плагина управления Kaspersky Endpoint Agent.

Включение и отключение сетевой изоляции

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы включить или отключить сетевую изоляцию устройства, выполните следующие действия:

1. **Откройте окно свойств программы для отдельного устройства**

   1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
   2. В рабочей области выберите закладку **Устройства**.
   3. Выберите устройство, для которого вы хотите настроить параметры Kaspersky Endpoint Agent.
   4. В контекстном меню устройства выберите пункт **Свойства**.

      Откроется окно свойств устройства.
   5. Выберите раздел **Программы**.

      В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
   6. 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".

2. В разделе **Сетевая изоляция** выберите **Общие параметры**.
3. В блоке параметров **Изолировать устройство** включите или выключите параметр **Изолировать данное 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В свойствах политики вы можете настроить 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.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Сетевая изоляция** выберите **Общие параметры**.
3. В блоке параметров **Уведомление** включите или выключите параметр **Уведомить пользователя, когда его устройство будет изолировано**.
4. Нажмите **ОК**, чтобы сохранить внесенные изменения.

Настройка автоматического отключения сетевой изоляции

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В свойствах политики вы можете настроить 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.

     1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
     2. В рабочей области выберите закладку **Устройства**.
     3. Выберите устройство, для которого вы хотите настроить параметры Kaspersky Endpoint Agent.
     4. В контекстном меню устройства выберите пункт **Свойства**.

        Откроется окно свойств устройства.
     5. Выберите раздел **Программы**.

        В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
     6. 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".

   - Откройте окно свойств политики программы.

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**.

2. В разделе **Сетевая изоляция** выберите **Общие параметры**.
3. В блоке параметров **Условия изоляции устройства** включите или выключите параметр **Автоматически прекращать изоляцию устройства по истечении**, чтобы включить или выключить функцию автоматического отключения сетевой изоляции по истечении заданного периода времени.
   - По умолчанию функция включена.
4. Задайте период, по истечении которого сетевая изоляция должна быть отключена.

   По умолчанию задан период в 30 минут.
5. Нажмите **OK**, 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена программой автоматически, в результате реагирования на обнаружение. Исключения, заданные в свойствах устройства, применяются, 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.

     1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
     2. В рабочей области выберите закладку **Устройства**.
     3. Выберите устройство, для которого вы хотите настроить параметры Kaspersky Endpoint Agent.
     4. В контекстном меню устройства выберите пункт **Свойства**.

        Откроется окно свойств устройства.
     5. Выберите раздел **Программы**.

        В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
     6. 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".

   - Откройте окно свойств политики программы.

     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**.

2. Если вы открыли окно свойств программы для отдельного устройства, то в разделе **Сетевая изоляция** выберите **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**

  Чтобы добавить пользовательское исключение, выполните следующие действия:

  1. Нажмите на кнопку **Добавить**.
  2. В раскрывающемся списке выберите пункт **Добавить пользовательское правило**.

     Откроется окно **Свойства правила**.
  3. Задайте необходимые параметры исключения и нажмите на кнопку **OK**.

     Новое правило будет добавлено в список исключений.

- **Добавить исключения из списка стандартных сетевых профилей**

  Чтобы добавить исключения из списка стандартных сетевых профилей, выполните следующие действия:

  1. Нажмите на кнопку **Добавить**.
  2. В раскрывающемся списке выберите пункт **Добавить из словаря сетевых профилей**.
  3. В открывшемся окне выберите необходимый сетевой профиль из списка **Список стандартных сетевых профилей**.

     В нижней части окна отобразится описание выбранного вами сетевого профиля.
  4. Если вы хотите посмотреть исключения, которые будут применены с выбранным сетевым профилем, нажмите на кнопку **Показать список правил**.
  5. Если вы хотите добавить выбранный сетевой профиль в список применяемых, нажмите на кнопку **-->**.

     Вы можете добавить сразу несколько сетевых профилей.
  6. Нажмите на кнопку **Добавить выбранные**.

     Исключения из выбранных вами сетевых профилей добавлены в список исключений.

- **Изменить параметры добавленного исключения**

Чтобы изменить параметры добавленного исключения, выполните следующие действия:

1. Выберите нужное исключение в списке **Исключения**.
2. Нажмите на кнопку **Просмотреть и изменить**.
3. Откроется окно **Свойства правила**.
4. Внесите необходимые изменения и нажмите на кнопку **OK**.

   Изменения внесены в выбранное исключение.

При изменении параметров исключения, заданного при помощи сетевого профиля, это исключение становится пользовательским.

- **Включить или отключить использование исключения**

  Чтобы включить использование исключения,

  установите флажок рядом с именем исключения в списке **Исключения**.

  Чтобы отключить использование исключения,

  снимите флажок рядом с именем исключения в списке **Исключения**.

- **Удалить исключение из списка**

  Чтобы удалить исключение из списка, выполните следующие действия:

  1. В списке **Исключения** выберите исключение, которое необходимо удалить.
  2. Нажмите на кнопку **Удалить**.

     Исключение удалено из списка исключений.

5. Чтобы сохранить изменения, нажмите на кнопку **Применить**.

Настройка использования KSN в Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 программы EPP 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.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Endpoint Agent передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. По умолчанию использование KSN отключено. После включения использования KSN, вы можете отключить эту опцию в любой момент времени.

Начиная с версии 3.10 в Kaspersky Endpoint Agent нет возможности настроить использование службы Kaspersky Managed Protection (далее KMP). Если в предыдущей установленной версии Kaspersky Endpoint Agent было включено использование службы KMP, то после обновления программы до версии 3.10 и выше служба KMP продолжает работать как раньше. После обновления вы можете отключить службу KMP только при помощи Плагина управления Kaspersky Endpoint Agent или Веб-плагина Kaspersky Endpoint Agent версий ниже 3.10.

Чтобы включить использование KSN, 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 **Kaspersky Security Network**.
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 ("KSN")**.

8. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

9. Нажмите на кнопку **OK**.

Использование KSN будет включено.

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с Kaspersky Sandbox. Интеграцию требуется настроить как на стороне Kaspersky Endpoint Agent с помощью Консоли администрирования Kaspersky Security Center, так и на стороне Kaspersky Sandbox с помощью веб-интерфейса.

Включение и отключение интеграции с Kaspersky Sandbox

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы включить или отключить интеграцию с 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 **Параметры интеграции с Kaspersky Sandbox**.

5. В блоке параметров **Параметры интеграции с Kaspersky Sandbox** включите или выключите параметр **Включить интеграцию с Kaspersky Sandbox**.

6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

7. Нажмите на кнопку **OK**.

Интеграция с Kaspersky Sandbox будет включена или отключена.

Настройка доверенного соединения Kaspersky Sandbox с Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить доверенное соединение Kaspersky Sandbox с Kaspersky Endpoint Agent в веб-интерфейсе сервера Kaspersky Sandbox, не входящего в кластер.

Если вы уже объединили серверы в кластер, то вам нужно удалить сервер из кластера, затем создать новый кластер на базе этого сервера и добавить в новый кластер все серверы, предназначенные для работы решения Kaspersky Sandbox.

Если нужные вам серверы входят в другой кластер, вам нужно последовательно удалить их из кластера, в который они входят в настоящий момент, а затем добавить в новый кластер.

Установка и настройка доверенного соединения Kaspersky Sandbox с Kaspersky Endpoint Agent состоит из следующих этапов:

1. **Удаление сервера из кластера (если сервер входит в кластер в настоящий момент)**
2. **Формирование или загрузка TLS-сертификата соединения с Kaspersky Endpoint Agent на этот сервер**
3. **Создание нового кластера на базе этого сервера**
4. **Удаление всех серверов, которые вы хотите добавить в этот кластер, из кластеров, в которые они входят в настоящий момент**
5. **Добавление всех нужных серверов в новый кластер**
6. **Добавление всех серверов нового кластера Kaspersky Sandbox в список Kaspersky Endpoint Agent**
7. **Настройка доверенного соединения с Kaspersky Sandbox на стороне Kaspersky Endpoint Agent**

Настройка доверенного соединения на стороне Kaspersky Sandbox

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Для настройки доверенного соединения вам потребуется сформировать или загрузить TLS-сертификат на стороне Kaspersky Sandbox, а затем сохранить его на компьютере для загрузки в программу Kaspersky Endpoint Agent.

Чтобы сгенерировать TLS-сертификат соединения Kaspersky Sandbox с Kaspersky Endpoint Agent, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В разделе **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Сгенерировать**.

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

Kaspersky Sandbox сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Sandbox.

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.

Чтобы загрузить TLS-сертификат через веб-интерфейс Kaspersky Sandbox, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В разделе **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Загрузить**.

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

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Sandbox.

Чтобы сохранить файл TLS-сертификата соединения с Kaspersky Endpoint Agent на компьютере, выполните следующие действия:

1. В окне веб-интерфейса Kaspersky Sandbox выберите раздел **TLS-сертификаты**.
2. В разделе **TLS-сертификат для соединения с Kaspersky Endpoint Agent** нажмите на кнопку **Скачать**.

Файл TLS-сертификата будет сохранен в папке загрузки браузера.

Настройка доверенного соединения на стороне Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить доверенное соединение на стороне 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. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры интеграции с Kaspersky Sandbox**.
5. В блоке параметров **Параметры интеграции с Kaspersky Sandbox** включите параметр **Использовать закреплённый сертификат для защиты соединения**.
6. Нажмите на кнопку **Добавить TLS-сертификат**.
7. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Sandbox:
   - 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 Kaspersky Sandbox. 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 **Параметры интеграции с Kaspersky Sandbox**.
9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

10. Нажмите на кнопку **OK**.

Доверенное соединение с сервером Kaspersky Sandbox будет настроено.

Обновление данных TLS-сертификата Kaspersky Sandbox в Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

При замене TLS-сертификата сервера Kaspersky Sandbox необходимо обновить данные TLS-сертификата в Kaspersky Endpoint Agent и заново настроить доверенное соединение с Kaspersky Sandbox.

Чтобы обновить данные TLS-сертификата Kaspersky Sandbox в 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. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры интеграции с Kaspersky Sandbox**, блок параметров **Параметры интеграции с Kaspersky Sandbox**.
5. Установите флажок **Использовать закреплённый сертификат для защиты соединения**.
6. Нажмите на кнопку **Добавить TLS-сертификат**.

   Откроется окно **Добавление TLS-сертификата**.
7. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Sandbox:
   - 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 Kaspersky Sandbox. 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 **Параметры интеграции с Kaspersky Sandbox**.

9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

10. Нажмите на кнопку **OK**.

В результате будут обновлены данные TLS-сертификата сервера Kaspersky Sandbox и установлено доверенное соединение с Kaspersky Sandbox.

Настройка времени ожидания ответа от Kaspersky Sandbox и параметров очереди запросов

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить время ожидания ответа от Kaspersky Sandbox и параметры очереди запросов на обработку объектов, поступающих от Kaspersky Endpoint Agent в 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 **Расширенные параметры Kaspersky Sandbox**.

5. В блоке параметров **Время ожидания** укажите максимальное время ожидания ответа от сервера Kaspersky Sandbox.

   По умолчанию задано 5 секунд.

6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

7. В блоке параметров **Очередь запросов Kaspersky Sandbox** в поле **Папка очереди** укажите путь к папке, в которой будет храниться информация о запросах, отправляемых в Kaspersky Sandbox.

   По умолчанию задан путь %SOYUZAPPDATA%\Sandbox\Queue.

8. В поле **Максимальный размер очереди (МБ)** укажите максимально допустимый размер очереди запросов в мегабайтах.

   По умолчанию задано 100 МБ.

9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

10. Нажмите на кнопку **ОК**.

Добавление серверов Kaspersky Sandbox в список Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы используете Nginx в качестве прокси-сервера между устройством с Kaspersky Endpoint Agent и сервером Kaspersky Sandbox, 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 Kaspersky Sandbox. Иначе Nginx не будет пропускать объекты, размер которых превышает установленное значение. Значение по умолчанию – 1 МБ.

Если вы включили интеграцию с Kaspersky Sandbox, вы можете добавить серверы Kaspersky Sandbox в список Kaspersky Endpoint Agent. Можно добавить несколько серверов Kaspersky Sandbox.

В рамках одной политики мы рекомендуем добавлять серверы, входящие в один кластер. Если серверы входят в разные кластеры, результат работы решения непредсказуем.

Все серверы в кластере равноправны независимо от того, на базе какого сервера был создан кластер. Результат обработки одного и того же объекта будет одинаковым на всех серверах кластера.

Программа Kaspersky Sandbox балансирует нагрузку между серверами. Объекты, поступающие на обработку в Kaspersky Sandbox от Kaspersky Endpoint Agent, обрабатываются на наименее загруженном сервере.

Чтобы кластер Kaspersky Sandbox обрабатывал объекты от Kaspersky Endpoint Agent, необходимо добавить в Kaspersky Endpoint Agent хотя бы один сервер, входящий в кластер при интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox.

В списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent отображаются только те серверы, которые вы добавили в этот список. При этом объекты могут обрабатываться любым сервером кластера с учетом балансировки нагрузки. Актуальный список серверов кластера можно просмотреть в веб-интерфейсе Kaspersky Sandbox.

Рекомендуется добавить в Kaspersky Endpoint Agent все серверы кластера.

Kaspersky Endpoint Agent может подключиться к другому серверу Kaspersky Sandbox из списка при возникновении одной из следующих ошибок:

- Истекло время ожидания ответа от Kaspersky Sandbox (connection timeout).
- Kaspersky Sandbox недоступен (код ошибки 503 или 504).
- Проблема самодиагностики, за исключением проблем с лицензией (код ошибки 500).

При удалении сервера из кластера возможны следующие сценарии обработки объектов:

- Если в списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent остается хотя бы один сервер этого кластера с актуальным IP-адресом или FQDN, Kaspersky Sandbox продолжит обрабатывать объекты от Kaspersky Endpoint Agent.
- Если в списке серверов Kaspersky Sandbox программы Kaspersky Endpoint Agent не остается ни одного сервера, входящего в этот кластер, или IP-адреса или FQDN серверов кластера неактуальны, Kaspersky Sandbox не сможет получать и обрабатывать объекты от Kaspersky Endpoint Agent.

  Для корректной обработки объектов необходимо добавить в Kaspersky Endpoint Agent хотя бы один сервер, входящий в кластер Kaspersky Sandbox.

Чтобы добавить серверы Kaspersky Sandbox в список 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. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры интеграции с Kaspersky Sandbox**.
5. В блоке параметров **Параметры интеграции с Kaspersky Sandbox** включите параметр **Включить интеграцию с Kaspersky Sandbox**.
6. В блоке параметров **Параметры интеграции с Kaspersky Sandbox** включите или выключите параметр **Подключаться через прокси-сервер, если это задано в общих параметрах**.

   По умолчанию параметр выключен. Программа подключается к Kaspersky Sandbox только напрямую и не использует общие параметры соединения с прокси-сервером. Вы можете включить параметр, если вы хотите, чтобы программа использовала общие параметры соединения с прокси-сервером при подключении к Kaspersky Sandbox.
7. В блоке параметров **Список серверов Kaspersky Sandbox** нажмите на кнопку **Добавить**.

   Откроется окно **Свойства сервера**.

8. Введите IP-адрес или полное доменное имя сервера Kaspersky Sandbox, а также порт подключения к серверу.

9. Нажмите на кнопку **Добавить**.

   Добавленный сервер отобразится в таблице серверов.

10. Повторите действия для добавления каждого сервера Kaspersky Sandbox в список.

11. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

12. Нажмите на кнопку **OK**.

Серверы Kaspersky Sandbox будут добавлены в список Kaspersky Endpoint Agent.

Настройка действий Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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.

- **EPP выполнять проверку важных областей на устройстве**.

  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 на 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.

- **EPP выполнять проверку важных областей на устройстве 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.

Включение и отключение выполнения действий по реагированию на угрозы

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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**

     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.
   - **EPP выполнять проверку важных областей на устройстве**

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.

- **Запустить Поиск IOC на 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.

- **EPP выполнять проверку важных областей на устройстве 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.

Действие будет добавлено в список **Выбранные 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**.

Настройка аутентификации на Сервере администрирования для Автономных задач поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы хотите, чтобы программа Kaspersky Endpoint Agent создавала Автономные задачи поиска IOC при реагировании на угрозы, необходимо настроить аутентификацию на Сервере администрирования.

Программа использует специальную учетную запись пользователя на Сервере администрирования, которая имеет ограниченные права и предназначена только для создания Автономных задач поиска IOC.

Специальную учетную запись можно создать только через окно **Реагирование на угрозы** в свойствах политики Kaspersky Endpoint Agent или в свойствах программы для отдельного устройства. Специальную учетную запись необходимо создать на Сервере администрирования один раз и использовать ее пароль для настройки параметров **Реагирование на угрозы** в свойствах других устройств или других политик, относящихся к тому же Серверу администрирования.

Невозможно изменить пароль созданной специальной учетной записи для Автономных задач поиска IOC. Если вы забыли пароль от учетной записи, удалите ее стандартными средствами Kaspersky Security Center и повторно создайте учетную запись через окно **Реагирование на угрозы**.

Чтобы настроить аутентификацию на Сервере администрирования для Автономных задач поиска IOC:

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. Если вы хотите проверить наличие специальной учетной записи для Автономных задач поиска IOC или создать такую учетную запись:
   a. В блоке параметров **Аутентификация на Сервере администрирования** нажмите на кнопку **Проверить наличие пользователя**.

      Блок параметров **Аутентификация на Сервере администрирования** доступен для редактирования, только если в списке **Выбранные действия** выбран параметр **Запустить Поиск IOC на управляемой группе устройств**.

   b. В открывшемся окне в блоке параметров **Подключение к Серверу администрирования** введите данные для подключения к Серверу администрирования, а также логин и пароль учетной записи Сервера администрирования, у которой есть права на создание новых пользователей.

   c. Нажмите на кнопку **Подключиться и проверить наличие пользователя**.

   d. Во всплывающем окне ознакомьтесь с информацией о наличии специальной учетной записи и закройте его.

   e. Если учетной записи не существует и вы хотите ее создать, в блоке параметров **Создание специального пользователя для Автономных задач поиска IOC** в поле **Пароль** задайте пароль длиной от 8 до 16 символов и нажмите на кнопку **Создать специального пользователя**.

Блок параметров **Создание специального пользователя для Автономных задач поиска IOC** становится доступным для редактирования только после проверки наличия специальной учетной записи.

f. Нажмите на кнопку **Выйти**, чтобы закрыть окно **Пользователь Сервера администрирования для Автономных задач поиска IOC**.

6. В блоке параметров **Аутентификация на Сервере администрирования** в поле **Имя пользователя Сервера администрирования** введите пароль специальной учетной записи для Автономных задач поиска IOC, созданной ранее.

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

8. Нажмите на кнопку **OK**.

Аутентификация на Сервере администрирования для Автономных задач поиска IOC настроена.

Защита устройств от легальных программ, которые могут быть использованы злоумышленниками

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 – это 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, например, 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 **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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 на системных дисках устройства**.

- **Важные файловые области на устройстве**.

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 после того, как Kaspersky Sandbox обнаружит угрозу**. Задачи поиска IOC будут автоматически создаваться и запускаться.

   - **Запускать 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 **Запускать 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.

     Например, 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.

Настройка интеграции Kaspersky Endpoint Agent с KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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.

Включение и отключение интеграции с KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы используете Nginx в качестве прокси-сервера между устройством с Kaspersky Endpoint Agent и сервером KATA, 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 KATA. Иначе Nginx не будет пропускать объекты, размер которых превышает установленное значение. Значение по умолчанию – 1 МБ.

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 **Серверы сбора телеметрии** выберите подраздел **Интеграция с KATA**.
5. В блоке параметров **Параметры подключения** включите или отключите интеграцию с KATA Central Node. Если вы включили интеграцию, укажите IP-адрес или полное доменное имя сервера KATA, а также порт подключения к серверу.
6. В блоке параметров **Параметры подключения** включите или выключите параметр **Подключаться через прокси-сервер, если это задано в общих параметрах**.

   По умолчанию параметр выключен. Программа подключается к серверу KATA только напрямую и не использует общие параметры соединения с прокси-сервером. Вы можете включить параметр, если вы хотите, чтобы программа использовала общие параметры соединения с прокси-сервером при подключении к серверу KATA.

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

8. Нажмите на кнопку **ОК**.

Интеграция с KATA Central Node будет включена или отключена.

Настройка доверенного соединения с KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 **Серверы сбора телеметрии** выберите подраздел **Интеграция с KATA**.

5. В блоке параметров **Параметры подключения** установите флажок **Использовать закреплённый сертификат для защиты соединения**.

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 **Добавить сертификат клиента**.

10. В открывшемся окне **Добавить сертификат клиента** выполните следующие действия:

    a. Установите флажок **Защита подключения с помощью сертификата клиента**.

    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 **OK**.

11. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

12. Нажмите на кнопку **OK**.

Доверенное соединение с сервером KATA будет настроено.

Настройка параметров синхронизации Kaspersky Endpoint Agent с KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 **Серверы сбора телеметрии** выберите подраздел **Интеграция с KATA**.

5. В блоке параметров **Параметры подключения** настройте следующие параметры:

- **Время ожидания (сек.)**. Укажите максимальное время ожидания ответа от сервера KATA. По умолчанию задано 10 секунд.

- **Адрес**. 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. По умолчанию задано 5 минут.

- Установите или снимите флажок **Использовать период TTL при отправке событий**. По умолчанию флажок снят.

  При установленном флажке Kaspersky Endpoint Agent не отправляет на сервер KATA информацию о процессах, которые запускаются повторно. Kaspersky Endpoint Agent не считает запуск процесса повторным, если запуск происходит после окончания очередного периода TTL.

- Если вы установили флажок **Использовать период TTL при отправке событий**, укажите время в поле **Порт**. По умолчанию задано 1440 минут.

6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

7. Нажмите на кнопку **OK**.

Настройка параметров передачи данных

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры передачи данных, 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 **Серверы сбора телеметрии** выберите подраздел **Общие параметры**.

5. В блоке параметров **Параметры передачи данных** выполните следующие действия:

   - Укажите значения в поле **Максимальное время передачи событий (сек.)**.

     По умолчанию задано 30 секунд.

   - Укажите значения в поле **Максимальное количество событий в одном пакете**.

По умолчанию задано 1024 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**.

Настройка параметров регулирования количества запросов

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Функция регулирования количества запросов позволяет ограничить поток событий низкой важности от Kaspersky Endpoint Agent к компоненту Central Node. Степень важности событий программа оценивает самостоятельно.

Чтобы настроить параметры регулирования количества запросов:

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 **Серверы сбора телеметрии** выберите подраздел **Общие параметры**.

5. В блоке параметров **Регулирование количества запросов** вы можете выполнить следующие действия:

   - Включить или выключить параметр **Включить регулирование количества запросов**.

     По умолчанию параметр включен.

   - Указать количество событий в поле **Максимальное количество событий в час**.

     Программа анализирует поток данных телеметрии и ограничивает передачу событий низкой важности, если поток передаваемых событий стремится превысить указанную в этом поле величину. По умолчанию задано 3000 событий в час.

   - Указать порог потока однотипных событий низкой важности в поле **Процент превышения лимита событий**.

     Если поток однотипных событий низкой важности превысит указанный в этом поле порог в процентах от общего количества событий, то именно этот тип событий будет ограничен. Можно задать величину от 5% до 100%. По умолчанию задано 15%.

6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

   По умолчанию переключатель находится в положении **Политика применяется**.

7. Нажмите на кнопку **OK**.

Настройка интеграции Kaspersky Endpoint Agent с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с программой Kaspersky Industrial CyberSecurity for Networks при помощи Консоли администрирования Kaspersky Security Center.

Включение интеграции с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

Чтобы включить интеграцию с программой KICS for Networks:

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 **Серверы сбора телеметрии** выберите подраздел **KICS for Networks**.

5. В блоке параметров **Параметры подключения** включите или отключите интеграцию с KICS for Networks. Если вы включили интеграцию, укажите IP-адрес или полное доменное имя сервера KICS for Networks, а также порт подключения к серверу.

6. В блоке параметров **Параметры подключения** включите параметр **Подключаться через прокси-сервер, если это задано в общих параметрах**.

   По умолчанию параметр выключен. Программа подключается к серверу KICS for Networks только напрямую и не использует общие параметры соединения с прокси-сервером. Вы можете включить параметр, если вы хотите, чтобы программа использовала общие параметры соединения с прокси-сервером при подключении к серверу KICS for Networks.

7. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

8. Нажмите на кнопку **OK**.

Интеграция с KICS for Networks включена.

Настройка доверенного соединения с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

Чтобы настроить доверенное соединение Kaspersky Endpoint Agent с KICS for Networks, 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 **Серверы сбора телеметрии** выберите подраздел **KICS for Networks**.

5. В блоке параметров **Параметры подключения** установите флажок **Использовать закреплённый сертификат для защиты соединения**.

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 KICS for Networks. 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 **Добавить сертификат клиента**.

10. В открывшемся окне **Добавить сертификат клиента** выполните следующие действия:

    a. Установите флажок **Защита подключения с помощью сертификата клиента**.

    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 KICS for Networks будет настроено.

Настройка параметров синхронизации Kaspersky Endpoint Agent с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

Чтобы настроить параметры синхронизации Kaspersky Endpoint Agent с KICS for Networks, 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 **Серверы сбора телеметрии** выберите подраздел **KICS for Networks**.
5. В блоке параметров **Параметры подключения** укажите максимальное время ожидания ответа от сервера KICS for Networks в поле **Время ожидания (сек.)**.

   По умолчанию задано 10 секунд.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **ОК**.

Параметры синхронизации Kaspersky Endpoint Agent с сервером KICS for Networks настроены и применяются.

Настройка параметров передачи данных

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры передачи данных, 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 **Серверы сбора телеметрии** выберите подраздел **Общие параметры**.
5. В блоке параметров **Параметры передачи данных** выполните следующие действия:
   - Укажите значения в поле **Максимальное время передачи событий (сек.)**.
     По умолчанию задано 30 секунд.
   - Укажите значения в поле **Максимальное количество событий в одном пакете**.
     По умолчанию задано 1024 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 **ОК**.

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Перед выполнением следующих инструкций требуется получить конфигурационный файл MDR. Он содержит конфигурационный файл (BLOB), необходимый для интеграции.

Если требуется, чтобы программа Kaspersky Endpoint Agent обрабатывала данные о событиях, формируемых Kaspersky Industrial CyberSecurity for Networks, и отправляла эти данные в Kaspersky Managed Detection and Response, то в параметрах Kaspersky Industrial CyberSecurity for Networks необходимо настроить взаимодействие с Kaspersky Security Center. Подробная информация о настройке взаимодействия программ приведена в *справке Kaspersky Industrial CyberSecurity for Networks*.

Функция интеграции с Kaspersky Managed Detection and Response доступна только в плагине управления Kaspersky Endpoint Agent версии 3.9.2 и выше.

Чтобы настроить интеграцию Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response с помощью Консоли администрирования Kaspersky Security Center, 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 **Managed Detection and Response**.

5. В блоке параметров **Параметры Managed Detection and Response** выполните следующие действия:

   a. Установите флажок **Включить Managed Detection and Response**.

   b. Нажмите на кнопку **Загрузить конфигурационный файл (BLOB)**, а затем выберите конфигурационный файл BLOB для загрузки.

   > Загружая конфигурационный файл Managed Detection and Response, вы соглашаетесь автоматически передавать указанные данные с устройства с установленной программой Kaspersky Endpoint Agent в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку указанных данных.

   c. В поле **Идентификатор пользователя** введите произвольное значение.

6. В окне свойств политики нажмите на кнопку **OK**.

Интеграция Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response настроена.

Работа MDR при совместном использовании Kaspersky Endpoint Agent и Kaspersky Endpoint Security

Программа Kaspersky Endpoint Security версии 11 или выше с актуальной версией баз поддерживает взаимодействие с решением MDR. В Kaspersky Endpoint Security версии 11.6.0 или выше поддержка взаимодействия с решением MDR доступна сразу после установки.

Если на устройстве вы использовали Kaspersky Endpoint Agent для работы с решением MDR и установили Kaspersky Endpoint Security версии, поддерживающей взаимодействие с решением MDR, или обновили базы Kaspersky Endpoint Security 11 или выше до актуальной версии, решение MDR прекращает работу с Kaspersky Endpoint Agent и становится доступным для работы с Kaspersky Endpoint Security, при этом:

- переключение между Kaspersky Endpoint Agent и Kaspersky Endpoint Security выполняется в тихом режиме;
- в Kaspersky Endpoint Agent доступна настройка параметров взаимодействия с решением MDR, но эти параметры не применяются на устройстве;
- при недоступности Kaspersky Endpoint Security (например, вы удалили программу), решение MDR может возобновить работу с Kaspersky Endpoint Agent, если перезапустить службу Kaspersky Endpoint Agent;
- компонент Managed Detection and Response в параметрах Kaspersky Endpoint Agent на устройстве остается в статусе *Запущен*, т.к. Kaspersky Endpoint Agent продолжает поддерживать связь с решением MDR (например, чтобы возобновить работу с решением при необходимости).

Настройка параметров EDR-телеметрии

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе содержится информация о том, как настроить исключения для EDR-телеметрии, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом KATA Central Node.

Включение и настройка исключений для EDR-телеметрии

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить исключения для EDR-телеметрии с помощью Консоли администрирования: как в свойствах отдельного устройства, так и в свойствах политики для группы устройств.

Чтобы включить и настроить исключения для EDR-телеметрии:

1. Выполните одно из следующих действий:

   - **Откройте окно свойств программы для отдельного устройства**.

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.
3. Выберите устройство, для которого вы хотите настроить параметры Kaspersky Endpoint Agent.
4. В контекстном меню устройства выберите пункт **Свойства**.

   Откроется окно свойств устройства.
5. Выберите раздел **Программы**.

   В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
6. 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".

- Откройте окно свойств политики программы.

  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**.

2. Перейдите в раздел **EDR-телеметрия** → **Исключения**.
3. Чтобы включить применение исключений для EDR-телеметрии, в блоке параметров **EDR-телеметрия** включите параметр **Использовать исключения**.
4. Чтобы добавить новое исключение, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Свойства правила** настройте следующие критерии исключения:

   Критерии применяются при помощи логического И.

Для создания правила необходимо обязательно задать значение в поле **Полный путь** и выбрать хотя бы один из типов событий в списке **Использовать это исключение для следующих типов событий**.

Если для критерия **Использовать это исключение для следующих типов событий** выбрана опция **Сетевые события**, в поле **Полный путь** необходимо указать полный путь к файлу.

Объект, для которого вы создаете исключение, должен присутствовать на защищаемом устройстве в момент применения параметров исключения. Например, если вы сначала настроите исключение для определенного приложения, а потом установите это приложение на защищаемое устройство, такое исключение не будет применяться.

- В блоке **Информация о процессе** задайте значения в следующих полях:
  - **Полный путь**. Полный путь к файлу, включая его имя и расширение. Можно использовать маски файлов (с помощью символов ? и *), а также системные переменные окружения.
  - **Текст командной строки**. Командная строка для запуска объекта.
  - **Родительский путь**. Путь до папки, в которой находится файл.
- В блоке **Свойства файла** задайте значения в следующих полях:
  - **Описание файла**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo).
  - **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo).
  - **Версия файла**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo).
- В блоке **Контрольные суммы файла** задайте значения в следующих полях:
  - **MD5**. MD5-хеш файла.
  - **SHA256**. SHA256-хеш файла.
- В списке **Использовать это исключение для следующих типов событий** выберите как минимум одну из следующих опций:
  - **Изменение файла**.
  - **Сетевые события**.
  - **Интерактивный ввод в консоли**. По умолчанию эта опция выбрана.
  - **Загрузка модуля процесса**.
  - **Изменения в реестре**.

c. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Свойства правила**.

Новое правило создано и отображается в списке исключений.

5. Чтобы удалить правило из списка исключений, выберите правило и нажмите на кнопку **Удалить**.

6. Чтобы открыть окно свойств уже созданного правила для изменения заданных критериев, выберите правило из списка исключений и нажмите на кнопку **Изменить**.

7. Если вы настраиваете параметры политики, убедитесь, что положение переключателя в правом верхнем углу блока параметров находится в положении **Политика применяется**. Переключатель находится в это положении по умолчанию.

8. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Исключения для EDR-телеметрии используются по настроенным правилам.

Настройка параметров хранилищ в Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе приведены инструкции по настройке параметров карантина и параметров синхронизации данных с Сервером администрирования с помощью плагина управления Kaspersky Endpoint Agent.

О карантине Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Через Kaspersky Security Center можно настраивать параметры карантина, просматривать свойства объектов, находящихся на карантине на защищаемых устройствах, 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 документации 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 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.

Kaspersky Endpoint Agent помещает объект 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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. Например, если 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 соответствующее 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 соответствующее 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. Например, если 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 кнопку **Применить** и затем на кнопку **ОК**.

Параметры карантина и папка для восстановления объектов из карантина будут настроены.

Настройка синхронизации данных с Сервером администрирования

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить синхронизацию данных об объектах, помещенных на карантин на управляемых устройствах, с Сервером администрирования Kaspersky Security Center. Синхронизация данных нужна для управления карантином через 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 **Отправлять 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 кнопку **Применить** и затем на кнопку **ОК**.

Синхронизация данных с Сервером администрирования будет настроена.

Настройка диагностики сбоев

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent не создает папку для сохранения файлов трассировки или файлов дампа на устройстве автоматически. Необходимо указать папку, которая уже доступна на устройстве.

Чтобы настроить диагностику сбоев, выполните следующие действия:

1. **Откройте окно свойств программы для отдельного устройства**

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
2. В рабочей области выберите закладку **Устройства**.
3. Выберите устройство, для которого вы хотите настроить параметры Kaspersky Endpoint Agent.
4. В контекстном меню устройства выберите пункт **Свойства**.

   Откроется окно свойств устройства.
5. Выберите раздел **Программы**.

   В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
6. 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".

2. В разделе **Параметры программы** выберите подраздел **Диагностика сбоев**.
3. Если вы хотите включить запись отладочной информации в файлы трассировки:

   a. Включите параметр **Записывать отладочную информацию в файлы трассировки**.

   b. В поле **Папка файлов трассировки** укажите путь к папке на устройстве, в которую программа должна сохранять файлы трассировки.

   > Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе отладочная информация не будет записана.

   c. В поле **Максимальный размер файла трассировки (МБ)** укажите размер файла в мегабайтах.

   По умолчанию задано 50 МБ. При достижении заданного размера файла программа продолжает запись в новый файл.
4. Если вы хотите, чтобы программа выполняла перезапись старых файлов трассировки:

   a. Включите параметр **Перезаписывать старые файлы трассировки**.

   b. В поле **Максимальное количество файлов для одного журнала трассировки** укажите желаемое значение.

   По умолчанию задан 1 файл. Когда достигается указанное количество файлов, программа перезаписывает старые файлы, начиная с самого старого. Указанное ограничение применяется для каждого отлаживаемого процесса Kaspersky Endpoint Agent отдельно, поэтому суммарное количество файлов для всех процессов может превышать заданное значение.

5. Если вы хотите включить запись файлов дампа:

   a. Включите параметр **Создавать файлы дампа**.

   b. В поле **Папка файлов дампа** укажите папку для сохранения файлов дампа.

   > Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе отладочная информация не будет записана.

6. Нажмите на кнопку **OK**.

Диагностика сбоев настроена и включена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы для диагностики сбоев будут создаваться в папках, которые вы указали.

Управление задачами Kaspersky Endpoint Agent

В этом разделе приведены инструкции по управлению задачами Kaspersky Endpoint Agent.

Создание локальной задачи

Локальные задачи – это задачи, которые выполняются на конкретном устройстве. Подробнее о задачах см. в документации Kaspersky Security Center.

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

Групповые задачи – это задачи, которые выполняются на устройствах выбранной группы администрирования. Подробнее о задачах см. в документации Kaspersky Security Center.

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

Вы можете запускать созданные задачи вручную. Например, вручную можно запускать задачи, в которых не настроен запуск по расписанию.

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.

Запуск задач по расписанию

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить запуск задачи по расписанию, 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 **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.
4. Если вы выбрали запуск задачи **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, один раз в день или два 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 настройте следующие параметры в окне **Дополнительно**:

- **Завершать задачи, выполняющиеся более**

  Включите этот параметр, если вы хотите задать максимальное время ожидания выполнения задачи. Через указанное время задача будет автоматически завершаться.

- **Отменить расписание с**

  Включите этот параметр, если вы хотите указать дату окончания действия расписания. После указанной даты расписание перестает действовать.

- **Запускать пропущенные задачи**

  Включите этот параметр, если вы хотите, чтобы программа при первой возможности запускала задачи, не выполненные вовремя.

- **Распределять время запуска задач в интервале**

  Включите этот параметр, 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 указанного интервала времени.

6. Нажмите на кнопку **OK**.

Запуск задач по расписанию настроен и применяется на устройствах.

Просмотр результатов выполнения задач

Вы можете просмотреть результаты выполнения задач в течение срока их хранения. Вы также можете 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 кнопку **Применить**, а затем на кнопку **ОК**.

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

Создание задачи активации Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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**.

     Локальные задачи – это задачи, которые выполняются на конкретном устройстве. Подробнее о задачах см. в документации Kaspersky Security Center.

     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.

   - **Запустите мастер создания групповой задачи**.

Групповые задачи – это задачи, которые выполняются на устройствах выбранной группы администрирования. Подробнее о задачах см. в документации Kaspersky Security Center.

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.

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 документации Kaspersky Security Center.
4. Если вы хотите добавить этот лицензионный ключ в качестве дополнительного 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 документации 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 документации 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 и модулей Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе приведены инструкции, как создать и настроить задачу обновления баз и модулей программы.

Создание задачи обновления баз и модулей программы

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 баз** 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 указанные пользователем серверы 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 адрес сервера обновлений (HTTP или FTP), либо путь к сетевой или локальной папке, содержащей файлы обновлений.
         3. Если вы хотите использовать этот сервер для обновления баз, установите флажок рядом с его адресом. Вы также можете добавить в список серверы и снять флажки рядом с адресами серверов, которые вы не хотите использовать сейчас, а планируете использовать в будущем.

            Выполняйте аналогичные действия по добавлению каждого сервера.

         4. Нажмите на кнопку **ОК**.
         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**.

2. 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.
   - **Только проверять наличие важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.
   - **Загружать и устанавливать важные 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 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 задачи, выполняющиеся 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 **Распределять время запуска задач в интервале** и задайте интервал запуска в минутах.

   e. Нажмите на кнопку **OK**.

4. 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.

5. 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**.

6. Указание названия задачи

   В окне **Определение название задачи** в поле **Имя** введите название задачи и нажмите на кнопку **Далее**.

7. Запуск задачи сразу после создания

   Если вы хотите, чтобы задача запустилась сразу после создания, установите флажок **Запустить задачу после завершения работы мастера** и нажмите на кнопку **Готово**.

Настройка параметров задачи обновления баз и модулей программы

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

После создания задачи обновления баз и модулей программы вы можете настроить параметры этой задачи.

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:

- Название задачи

Выполните следующие действия:

1. Выберите раздел **Общие**.
2. Измените имя задачи в верхней строке.

- **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*.

- **Источник обновления баз**

Выполните следующие действия:

1. В блоке **Источник обновлений баз** 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 указанные пользователем серверы 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 адрес сервера обновлений (HTTP или FTP), либо путь к сетевой или локальной папке, содержащей файлы обновлений.
      3. Если вы хотите использовать этот сервер для обновления баз, установите флажок рядом с его адресом. Вы также можете добавить в список серверы и снять флажки рядом с 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**.

- Настройка дополнительных параметров 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.
   - **Только проверять наличие важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.
   - **Загружать и устанавливать важные 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**.

- 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 задачи, выполняющиеся 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 **Распределять время запуска задач в интервале** и задайте интервал запуска в минутах.
   e. Нажмите на кнопку **OK**.

- 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.

- 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.

Управление задачами поиска IOC в Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе приведены инструкции по управлению задачами поиска IOC в Kaspersky Endpoint Agent с помощью плагина управления Kaspersky Endpoint Agent.

Управление стандартными задачами поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Стандартные задачи поиска IOC – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.

В этом разделе приведены инструкции по управлению стандартными задачами поиска IOC.

Требования к IOC-файлам

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

При создании задач Поиск IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- 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.
- Размер одного IOC-файла не должен превышать 3 МБ. Использование файлов большего размера приводит к завершению задач Поиск IOC с ошибкой. При этом суммарный размер всех добавленных файлов в IOC-коллекции может превышать 3 МБ.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

Особенности и ограничения поддержки стандарта OpenIOC программой приведены в следующей таблице.

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	Полный список поддерживаемых программой IOC-терминов приведен в отдельной таблице.

Поддерживаемые IOC-термины

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC, поддерживаемых программой Kaspersky Endpoint Agent.

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX

Создание и настройка стандартной задачи поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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.

  Локальные задачи – это задачи, которые выполняются на конкретном устройстве. Подробнее о задачах см. в документации Kaspersky Security Center.

  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.

- Запустите мастер создания групповой задачи.

Групповые задачи – это задачи, которые выполняются на устройствах выбранной группы администрирования. Подробнее о задачах см. в документации Kaspersky Security Center.

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.

Мастер создания задачи позволяет настроить следующие параметры:

- IOC-коллекция

Чтобы настроить IOC-коллекцию, выполните следующие действия:

1. В блоке параметров **IOC-коллекция** нажмите на кнопку **Обзор**.
2. В раскрывшемся контекстном меню выполните одно из следующих действий:
   - Выберите элемент **Выбрать папку**, чтобы добавить группу IOC-файлов в IOC-коллекцию.
   - Выберите элемент **Выбрать файл**, чтобы добавить один IOC-файл в IOC-коллекцию.
3. В зависимости от вашего выбора, в открывшемся окне выполните одно из следующих действий:
   - Укажите путь к папке с IOC-файлами и нажмите на кнопку **OK**.
   - Укажите путь к IOC-файлу и нажмите на кнопку **Открыть**.

   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.
4. Чтобы посмотреть список всех IOC-файлов, которые включены в IOC-коллекцию, а также получить информацию о каждом IOC-файле, нажмите на кнопку **Просмотр**.

   Откроется окно **Выбрать папку**. В этом окне можно исключить любой файл из базы, сняв флажок, расположенный рядом с именем IOC-файла.
5. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Выбрать папку**.
6. Чтобы экспортировать созданную IOC-коллекцию, нажмите на кнопку **Экспортировать**.

   В открывшемся окне можно задать имя файла, а также выбрать папку, в которую вы хотите его сохранить.
7. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной папке.

- Типы данных (IOC-документы) для анализа во время поиска IOC

Чтобы выбрать типы данных (IOC-документы), которые необходимо анализировать во время поиска IOC, и настроить дополнительные параметры поиска, выполните следующие действия:

1. Нажмите на кнопку **Настроить IOC термины и документы**.

   Откроется окно **IOC термины и документы**.

2. В блоке параметров **Выберите типы данных (IOC-документы) для анализа во время поиска IOC** установите флажки рядом с нужными IOC-документами.

   В зависимости от загруженных IOC-файлов, некоторые флажки могут быть неактивными.

   Kaspersky Endpoint Agent автоматически выбирает типы данных (IOC-документы) для задачи Поиск IOC в соответствии с содержанием загруженных IOC-файлов. Не рекомендуется самостоятельно отменять выбор типов данных.

3. Чтобы настроить дополнительные параметры для выбранного IOC-документа ProcessItem, выполните следующие действия:

   a. Нажмите на кнопку **Дополнительно (ProcessItem)**.

      Откроется окно **Параметры проверки документа ProcessItem**.

   b. В блоке параметров **Индикаторы** выберите данные, которые необходимо анализировать во время выполнения задачи.

   c. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа ProcessItem**.

4. Чтобы настроить дополнительные параметры для выбранного IOC-документа FileItem, выполните следующие действия:

   a. Нажмите на кнопку **Дополнительно (FileItem)**.

      Откроется окно **Параметры проверки документа FileItem**.

   b. На закладке **Области** выберите данные, которые необходимо анализировать во время выполнения задачи.

   c. На закладке **Области** выберите области на дисках защищаемого устройства, в которых необходимо искать индикаторы компрометации.

      Вы можете выбрать одну из предзаданных областей, а также указать пути до нужных областей самостоятельно.

   d. На закладке **Исключения** установите флажок **Применять исключения** и добавьте пути до областей на дисках защищаемого устройства, которые не нужно сканировать во время выполнения задачи.

   e. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа FileItem**.

5. Чтобы настроить дополнительные параметры для выбранного IOC-документа RegistryItem, выполните следующие действия:

   a. Нажмите на кнопку **Дополнительно (RegistryItem)**.

      Откроется окно **Параметры проверки документа RegistryItem**.

b. Задайте ключи реестра Windows, которые необходимо проверять во время выполнения задачи.

Вы можете выбрать проверку по предзаданным ключам реестра или указать список нужных ключей реестра самостоятельно.

c. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа RegistryItem**.

6. Чтобы настроить дополнительные параметры для выбранного IOC-документа EventLogItem, выполните следующие действия:

a. Нажмите на кнопку **Дополнительно (EventLogItem)**.

Откроется окно **Параметры проверки документа EventLogItem**.

b. Чтобы во время выполнения задачи не учитывать события, зафиксированные ранее определенного момента, установите флажок **Проверять только события, зафиксированные в течение указанного периода** и укажите дату и время.

c. Ниже в том же окне, если необходимо, отредактируйте предзаданный список каналов, которые необходимо анализировать во время выполнения задачи.

d. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа EventLogItem**.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно.

Сохраненные параметры будут применены при выполнении задачи.

- **Ретроспективный поиск IOC**

Ретроспективный поиск IOC - это режим работы задачи Поиск IOC, при котором Kaspersky Endpoint Agent выполняет поиск индикаторов компрометации по данным, собранным за указанный пользователем интервал времени. Режим предназначен для поиска индикаторов компрометации по данным сетевой активности защищаемых устройств. Kaspersky Endpoint Agent анализирует данные в журналах операционной системы и браузеров на устройствах.

Режим **Ретроспективный поиск IOC** доступен только для Стандартных задач поиска IOC.

Чтобы включить режим Ретроспективный поиск IOC:

1. В блоке параметров **Ретроспективный поиск IOC** включите параметр **Выполнять Ретроспективный поиск IOC в интервале**.

2. Укажите временной интервал.

Во время выполнения задачи программа анализирует данные, собранные за указанный вами интервал времени, включая границы указанного интервала (с 00:00 даты начала до 23:59 даты окончания). По умолчанию задан интервал, начинающийся в 00:00 дня, предшествующего дню создания задачи, и заканчивающийся в 23:59 дня создания задачи.

Если во время выполнения задачи Поиск IOC со включенным параметром **Выполнять Ретроспективный поиск IOC в интервале** программа не обнаруживает данных для анализа за указанный временной интервал, программа не информирует об этом. В этом случае программа сообщает об отсутствии индикаторов компрометации в отчете о выполнении задачи.

- **Действия программы при обнаружении IOC**

  Чтобы настроить действия Kaspersky Endpoint Agent при обнаружении IOC, выполните следующие действия:

  1. В разделе **Действия** установите флажок **Принять ответные действия при обнаружении индикатора компрометации**.
  2. Установите флажок **Изолировать устройство от сети**, чтобы программа Kaspersky Endpoint Agent выполняла сетевую изоляцию устройства, на котором обнаружен индикатор компрометации.
  3. Установите флажок **EPP выполнять проверку важных областей на устройстве**, чтобы программа Kaspersky Endpoint Agent отправляла программе EPP команду на выполнение проверки важных областей на всех устройствах группы администрирования, на которых обнаружены индикаторы компрометации.

  При настройке параметров задачи через Консоль администрирования Kaspersky Security Center флажок **Не выполнять действий над критическими системными файлами** доступен, только если для задачи выбрано ответное действие **Поместить на карантин и удалить** (этот параметр можно настроить только через Kaspersky Security Center Web Console).

- **Расписание запуска задачи**

Чтобы настроить расписание запуска задач поиска IOC, выполните следующие действия:

1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.
2. В списке **Периодичность** выберите один из следующих вариантов запуска задач поиска IOC: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.
3. Если вы выбрали запуск задачи **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.
4. Если вы выбрали запуск задачи **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, установите флажок **Завершать задачи, выполняющиеся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.
   b. Если вы хотите, чтобы расписание запуска задачи 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 поиска IOC, 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 **Распределять время запуска задач в интервале** и задайте интервал запуска в минутах.
   e. Нажмите на кнопку **OK**.

- Учетную запись пользователя Kaspersky Security Center для запуска задачи

Чтобы выбрать учетную запись пользователя Kaspersky Security Center, с правами которой запускать задачу,

в блоке параметров выбора 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, с правами учетной записью которого вы хотите выполнять задачу.

- Название задачи

Название задачи не должно превышать 100 символов и не должно содержать специальные символы ("*<>?\:|).

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 кнопку **Применить**, а затем на кнопку **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.

- **IOC-коллекция**

Чтобы настроить IOC-коллекцию, выполните следующие действия:

1. В блоке параметров **IOC-коллекция** нажмите на кнопку **Обзор**.
2. В раскрывшемся контекстном меню выполните одно из следующих действий:
   - Выберите элемент **Выбрать папку**, чтобы добавить группу IOC-файлов в IOC-коллекцию.
   - Выберите элемент **Выбрать файл**, чтобы добавить один IOC-файл в IOC-коллекцию.
3. В зависимости от вашего выбора, в открывшемся окне выполните одно из следующих действий:
   - Укажите путь к папке с IOC-файлами и нажмите на кнопку **ОК**.
   - Укажите путь к IOC-файлу и нажмите на кнопку **Открыть**.

   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.
4. Чтобы посмотреть список всех IOC-файлов, которые включены в IOC-коллекцию, а также получить информацию о каждом IOC-файле, нажмите на кнопку **Просмотр**.

   Откроется окно **Выбрать папку**. В этом окне можно исключить любой файл из базы, сняв флажок, расположенный рядом с именем IOC-файла.
5. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Выбрать папку**.
6. Чтобы экспортировать созданную IOC-коллекцию, нажмите на кнопку **Экспортировать**.

   В открывшемся окне можно задать имя файла, а также выбрать папку, в которую вы хотите его сохранить.
7. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной папке.

- Ретроспективный поиск IOC

Ретроспективный поиск IOC - это режим работы задачи Поиск IOC, при котором Kaspersky Endpoint Agent выполняет поиск индикаторов компрометации по данным, собранным за указанный пользователем интервал времени. Режим предназначен для поиска индикаторов компрометации по данным сетевой активности защищаемых устройств. Kaspersky Endpoint Agent анализирует данные в журналах операционной системы и браузеров на устройствах.

Режим **Ретроспективный поиск IOC** доступен только для Стандартных задач поиска IOC.

Чтобы включить режим Ретроспективный поиск IOC:

1. В блоке параметров **Ретроспективный поиск IOC** включите параметр **Выполнять Ретроспективный поиск IOC в интервале**.

2. Укажите временной интервал.

   Во время выполнения задачи программа анализирует данные, собранные за указанный вами интервал времени, включая границы указанного интервала (с 00:00 даты начала до 23:59 даты окончания). По умолчанию задан интервал, начинающийся в 00:00 дня, предшествующего дню создания задачи, и заканчивающийся в 23:59 дня создания задачи.

Если во время выполнения задачи Поиск IOC со включенным параметром **Выполнять Ретроспективный поиск IOC в интервале** программа не обнаруживает данных для анализа за указанный временной интервал, программа не информирует об этом. В этом случае программа сообщает об отсутствии индикаторов компрометации в отчете о выполнении задачи.

- Действия программы при обнаружении IOC

Чтобы настроить действия Kaspersky Endpoint Agent при обнаружении IOC, выполните следующие действия:

1. В разделе **Действия** установите флажок **Принять ответные действия при обнаружении индикатора компрометации**.

2. Установите флажок **Изолировать устройство от сети**, чтобы программа Kaspersky Endpoint Agent выполняла сетевую изоляцию устройства, на котором обнаружен индикатор компрометации.

3. Установите флажок **EPP выполнять проверку важных областей на устройстве**, чтобы программа Kaspersky Endpoint Agent отправляла программе EPP команду на выполнение проверки важных областей на всех устройствах группы администрирования, на которых обнаружены индикаторы компрометации.

При настройке параметров задачи через Консоль администрирования Kaspersky Security Center флажок **Не выполнять действий над критическими системными файлами** доступен, только если для задачи выбрано ответное действие **Поместить на карантин и удалить** (этот параметр можно настроить только через Kaspersky Security Center Web Console).

- Типы данных (IOC-документы) для анализа во время поиска IOC

Чтобы выбрать типы данных (IOC-документы), которые необходимо анализировать во время поиска IOC, и настроить дополнительные параметры поиска, выполните следующие действия:

1. Перейдите в раздел **Дополнительно**.
2. В блоке параметров **Выберите типы данных (IOC-документы) для анализа во время поиска IOC** установите флажки рядом с нужными IOC-документами.

   В зависимости от загруженных IOC-файлов, некоторые флажки могут быть неактивными.

   Kaspersky Endpoint Agent автоматически выбирает типы данных (IOC-документы) для задачи Поиск IOC в соответствии с содержанием загруженных IOC-файлов. Не рекомендуется самостоятельно отменять выбор типов данных.

3. Чтобы настроить дополнительные параметры для выбранного IOC-документа ProcessItem, выполните следующие действия:

   a. Нажмите на кнопку **Дополнительно (ProcessItem)**.

      Откроется окно **Параметры проверки документа ProcessItem**.

   b. В блоке параметров **Индикаторы** выберите данные, которые необходимо анализировать во время выполнения задачи.

   c. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа ProcessItem**.

4. Чтобы настроить дополнительные параметры для выбранного IOC-документа FileItem, выполните следующие действия:

   a. Нажмите на кнопку **Дополнительно (FileItem)**.

      Откроется окно **Параметры проверки документа FileItem**.

   b. На закладке **Области** выберите данные, которые необходимо анализировать во время выполнения задачи.

   c. На закладке **Области** выберите области на дисках защищаемого устройства, в которых необходимо искать индикаторы компрометации.

      Вы можете выбрать одну из предзаданных областей, а также указать пути до нужных областей самостоятельно.

   d. На закладке **Исключения** установите флажок **Применять исключения** и добавьте пути до областей на дисках защищаемого устройства, которые не нужно сканировать во время выполнения задачи.

   e. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа FileItem**.

5. Чтобы настроить дополнительные параметры для выбранного IOC-документа RegistryItem, выполните следующие действия:

   a. Нажмите на кнопку **Дополнительно (RegistryItem)**.

      Откроется окно **Параметры проверки документа RegistryItem**.

   b. Задайте ключи реестра Windows, которые необходимо проверять во время выполнения задачи.

Вы можете выбрать проверку по предзаданным ключам реестра или указать список нужных ключей реестра самостоятельно.

c. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа RegistryItem**.

6. Чтобы настроить дополнительные параметры для выбранного IOC-документа EventLogItem, выполните следующие действия:

a. Нажмите на кнопку **Дополнительно (EventLogItem)**.

Откроется окно **Параметры проверки документа EventLogItem**.

b. Чтобы во время выполнения задачи не учитывать события, зафиксированные ранее определенного момента, установите флажок **Проверять только события, зафиксированные в течение указанного периода** и укажите дату и время.

c. Ниже в том же окне, если необходимо, отредактируйте предзаданный список каналов, которые необходимо анализировать во время выполнения задачи.

d. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа EventLogItem**.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно.

Сохраненные параметры будут применены при выполнении задачи.

- Расписание запуска задачи поиска IOC

Чтобы настроить расписание запуска задач поиска IOC, выполните следующие действия:

1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.
2. В списке **Периодичность** выберите один из следующих вариантов запуска задач поиска IOC: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.
3. Если вы выбрали запуск задачи **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.
4. Если вы выбрали запуск задачи **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, установите флажок **Завершать задачи, выполняющиеся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.
   b. Если вы хотите, чтобы расписание запуска задачи 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 поиска IOC, 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 **Распределять время запуска задач в интервале** и задайте интервал запуска в минутах.
   e. Нажмите на кнопку **OK**.

- Учетная запись пользователя Kaspersky Security Center для запуска задачи

Чтобы выбрать учетную запись пользователя Kaspersky Security Center, с правами которой запускать задачу,

в блоке параметров выбора 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, с правами учетной записью которого вы хотите выполнять задачу.

- 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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**.

   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.

Управление автономными задачами поиска IOC

> Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Автономные задачи поиска IOC – групповые задачи, которые создаются автоматически при реагировании на угрозы, обнаруженные Kaspersky Sandbox. Kaspersky Endpoint Agent автоматически формирует IOC-файл. Работа с пользовательскими IOC-файлами не предусмотрена. Задачи автоматически удаляются через семь дней после последнего запуска или с момента создания, если задачи не запускались. Подробнее об автономных задачах поиска IOC см. в *Справке Kaspersky Sandbox*.

В этом разделе приведены инструкции по настройке параметров автономных задач поиска IOC с помощью плагина управления Kaspersky Endpoint Agent.

Настройка прав пользователей для управления задачами поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 **OK**.

Настройка параметров автономной задачи поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры автономной 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 **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.

- **Действия программы, при обнаружении IOC**

  Чтобы настроить действия программы при обнаружении IOC, выполните следующие действия:

  1. Выберите раздел **Параметры поиска IOC**.
  2. В блоке параметров **Действия** установите флажок **Принять ответные действия при обнаружении индикатора компрометации**.
  3. Установите флажок **Поместить на карантин и удалить**, чтобы поместить обнаруженный объект на карантин и удалить его с устройства.
  4. Установите флажок **EPP выполнять проверку важных областей на устройстве**, чтобы программа Kaspersky Endpoint Agent отправляла программе EPP команду на выполнение проверки важных областей на всех устройствах группы администрирования, на которых обнаружен объект.
  5. Нажмите на кнопку **Применить**.

- **Расписание запуска задач поиска IOC**

Чтобы настроить расписание запуска задач поиска IOC, выполните следующие действия:

1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.
2. В списке **Периодичность** выберите один из следующих вариантов запуска задач поиска IOC: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.
3. Если вы выбрали запуск задачи **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.
4. Если вы выбрали запуск задачи **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, установите флажок **Завершать задачи, выполняющиеся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.
   b. Если вы хотите, чтобы расписание запуска задачи 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 поиска IOC, 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 **Распределять время запуска задач в интервале** и задайте интервал запуска в минутах.
   e. Нажмите на кнопку **OK**.

- Учетная запись пользователя Kaspersky Security Center для запуска задачи

Чтобы выбрать учетную запись пользователя Kaspersky Security Center, с правами которой запускать задачу,

в блоке параметров выбора 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, с правами учетной записью которого вы хотите выполнять задачу.

- 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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**.

   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.

Управление программой с помощью Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console

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*.

Вы управляете Kaspersky Security Center с помощью *Kaspersky Security Center Web Console* (далее также *Web Console*). Web Console представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.

Kaspersky Security Center Cloud Console

Kaspersky *Security Center Cloud Console* – это программа, которая размещается и поддерживается "Лабораторией Касперского". Вам не нужно устанавливать Kaspersky Security Center Cloud Console на свой компьютер или сервер. Kaspersky Security Center Cloud Console позволяет администратору устанавливать программы безопасности "Лаборатории Касперского" на устройства в корпоративной сети, удаленно запускать задачи проверки и обновления, а также управлять политиками безопасности управляемых программ. Администратор может использовать подробную панель мониторинга, где можно просмотреть моментальные снимки состояния корпоративных устройств, подробные отчеты и детальные параметры политик защиты.

Kaspersky Security Center Cloud Console как и Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Agent, настраивать параметры работы программы, запускать и останавливать задачи программы.

Вы управляете Kaspersky Security Center Cloud Console с помощью *облачной Консоли администрирования*, которая представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Security Center Cloud Console.

Подробную информацию о Kaspersky Security Center Cloud Console см. в *Справке Kaspersky Security Center Cloud Console*.

Управление программой Kaspersky Endpoint Agent

Далее в этом разделе приведены универсальные инструкции по управлению Kaspersky Endpoint Agent, которые пригодны как для управления программой с помощью Kaspersky Security Center Web Console, так и с помощью облачной Консоли администрирования.

Для управления Kaspersky Endpoint Agent через Web Console необходимо установить веб-плагин управления Kaspersky Endpoint Agent.

Управление политиками Kaspersky Endpoint Agent

В этом разделе приведены инструкции по созданию политик Kaspersky Endpoint Agent и включению параметров в политиках.

Создание политики Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы создать политику Kaspersky Endpoint Agent в Kaspersky Security Center Web Console, выполните следующие действия:

1. В главном окне перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
3. Выберите программу Kaspersky Endpoint Agent и нажмите **Далее**.
4. Выберите необходимый способ развертывания Kaspersky Endpoint Agent, установив соответствующие флажки:

   - **Интеграция с Kaspersky Sandbox**
   - **Endpoint Detection and Response Optimum**
   - **Endpoint Detection and Response Expert (KATA EDR)**

   Выбор типа политики и интеграция с Kaspersky Sandbox и KATA EDR недоступны в Kaspersky Security Center Cloud Console.
5. Нажмите **Далее**.
6. На закладке **Общие** вы можете выполнить следующие действия:

   - Изменить имя политики.
   - Выбрать состояние политики:

- **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.
- **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.
- **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.

- Настроить наследование параметров:
  - **Наследовать параметры родительской политики**. Если переключатель включен, значения параметров политики наследуются из политики верхнего уровня иерархии. Параметры политики недоступны для изменения, если в родительской политике установлен переключатель **Обеспечить принудительное наследование параметров для дочерних политик**.
  - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики будут распространены на дочерние политики. В свойствах дочерней политики будет автоматически включен и недоступен для выключения переключатель **Наследовать параметры родительской политики**.

7. На закладке **Параметры программы** вы можете настроить параметры политики Kaspersky Endpoint Agent.
8. Нажмите на кнопку **Сохранить**.

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 окно свойств политики программы.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. Выберите раздел и блок параметров, к которым относятся нужные параметры.
3. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

Все параметры блока будут применяться в политике.

Настройка параметров Kaspersky Endpoint Agent

В этом разделе приведены инструкции по настройке параметров Kaspersky Endpoint Agent.

Открытие окна параметров Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы открыть окно параметров политики Kaspersky Endpoint Agent, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

Чтобы открыть окно параметров Kaspersky Endpoint Agent для отдельного устройства, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите устройство.
3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
4. Выберите **Kaspersky Endpoint Agent**.
5. В открывшемся окне выберите закладку **Параметры программы**.

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**, кроме параметров сетевой изоляции.

В свойствах политики вы можете настроить параметры автоматической сетевой изоляции, а в свойствах отдельного устройства настраиваются параметры сетевой изоляции по требованию (включаемой вручную).

Настройка параметров безопасности Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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.

Настройка прав пользователей

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете предоставить доступ к Kaspersky Endpoint Agent отдельным пользователям или группам пользователей. В результате только заданные пользователи смогут управлять параметрами или службами программы.

Чтобы настроить права пользователей, выполните следующие действия:

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.
     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.
   - Откройте окно свойств политики программы.

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. В блоке параметров **Права пользователей на управление службами программы** нажмите на кнопку **Настроить** рядом с названием нужного параметра (**Права пользователей на управление программой** или **Настройка прав пользователей на управление программой**).

   Чтобы добавить пользователей и группы пользователей, необходимо указать строки дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL).
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **OK**.
6. Нажмите на кнопку **Сохранить**.

Включение защиты паролем

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

- Откройте окно свойств политики программы.

  1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
  2. Выберите политику, которую вы хотите настроить.
  3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. В блоке параметров **Защита паролем** установите флажок **Применить защиту паролем**.
4. 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);
     - цифры (0-9);
     - специальные символы (!$#%).
5. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**.

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. В блоке параметров **Самозащита** включите или выключите параметр **Включить самозащиту модулей программы в памяти**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **OK**.
6. Нажмите на кнопку **Сохранить**.

Механизм самозащиты будет включен или отключен.

Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Программа использует параметры соединения с прокси-сервером для обновления баз, активации программы и работы внешних служб.

Если вы хотите использовать заданный прокси-сервер при соединении с сервером KATA или Kaspersky Sandbox, убедитесь, что выбрана опция **Подключаться через прокси-сервер, если это задано в общих параметрах** при настройке интеграции с KATA или Kaspersky Sandbox. По умолчанию опция не выбрана.

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

1. Выполните одно из следующих действий:

   - **Откройте окно свойств программы для отдельного устройства**.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - **Откройте окно свойств политики программы**.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. Выберите один из следующих вариантов использования прокси-сервера:

- **Не использовать прокси-сервер**.
- **Использовать прокси-сервер с указанными параметрами**.

4. 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.

5. 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**.

6. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.

7. Если вы настраиваете свойства политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

8. Нажмите на кнопку **ОК**.

9. В окне свойств политики нажмите на кнопку **Сохранить**.

Параметры соединения с прокси-сервером будут настроены.

Настройка Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы включить использование Kaspersky Security Center в качестве прокси-сервера для активации программы:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите устройство.
3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
4. Выберите **Kaspersky Endpoint Agent**.
5. В открывшемся окне выберите закладку **Параметры программы**.

- Откройте окно свойств политики программы.

  1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
  2. Выберите политику, которую вы хотите настроить.
  3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. В блоке параметров **Лицензирование** установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **ОК**.
6. В окне свойств политики нажмите на кнопку **Сохранить**.

Включено использование Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent.

Настройка параметров сетевой изоляции

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе приведены инструкции по настройке параметров сетевой изоляции с помощью плагина управления Kaspersky Endpoint Agent.

Включение и отключение сетевой изоляции

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы включить или отключить сетевую изоляцию устройства, выполните следующие действия:

1. Откройте окно свойств программы для отдельного устройства.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
   2. Выберите устройство.
   3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
   4. Выберите **Kaspersky Endpoint Agent**.
   5. В открывшемся окне выберите закладку **Параметры программы**.

2. В разделе **Сетевая изоляция** выберите **Общие параметры**.
3. В блоке параметров **Изолировать устройство** установите или снимите флажок **Изолировать данное 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В свойствах политики вы можете настроить 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.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Сетевая изоляция** выберите **Общие параметры**.
3. В блоке параметров **Уведомление** установите или снимите флажок **Уведомить пользователя, когда его устройство будет изолировано**.
4. Нажмите **OK**, чтобы сохранить внесенные изменения.

Настройка автоматического отключения сетевой изоляции

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В свойствах политики вы можете настроить 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.

  1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
  2. Выберите устройство.
  3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
  4. Выберите **Kaspersky Endpoint Agent**.
  5. В открывшемся окне выберите закладку **Параметры программы**.

- Откройте окно свойств политики программы.

  1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
  2. Выберите политику, которую вы хотите настроить.
  3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Сетевая изоляция** выберите **Общие параметры**.
3. В блоке параметров **Условия изоляции устройства** включите или выключите параметр **Автоматически прекращать изоляцию устройства по истечении**.
4. Задайте период, по истечении которого сетевая изоляция должна быть отключена.

   По умолчанию задан период в 30 минут.
5. Нажмите **OK**, 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Исключения, заданные в свойствах политики, применяются, только если сетевая изоляция включена программой автоматически, в результате реагирования на обнаружение. Исключения, заданные в свойствах устройства, применяются, 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.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. Если вы открыли окно свойств программы для отдельного устройства, то в разделе **Сетевая изоляция** выберите **Исключения**.

3. Если вы открыли окно свойств политики программы, то в разделе **Сетевая изоляция** выберите **Изоляция при обнаружении**.

   Вы можете выполнить следующие действия:

   - Добавить пользовательское исключение

     Чтобы добавить пользовательское исключение, выполните следующие действия:

     1. Нажмите на кнопку **Добавить**.

        Откроется окно **Свойства правила**.

     2. Задайте необходимые параметры исключения и нажмите на кнопку **OK**.

        Новое правило будет добавлено в список исключений.

   - Добавить исключения из списка стандартных сетевых профилей

Чтобы добавить исключения из списка стандартных сетевых профилей, выполните следующие действия:

1. Нажмите на кнопку **Добавить**.

   В открывшемся окне выберите необходимый сетевой профиль из списка **Список стандартных сетевых профилей**.

   Вы можете выбрать сразу несколько сетевых профилей.

2. Нажмите на кнопку **OK**.

   Исключения из выбранных вами сетевых профилей добавлены в список исключений.

- **Изменить параметры добавленного исключения**

  Чтобы изменить параметры добавленного исключения, выполните следующие действия:

  1. Нажмите на имя нужного правила.
  2. Откроется окно **Свойства правила**.
  3. Внесите необходимые изменения и нажмите на кнопку **OK**.

  Изменения внесены в выбранное исключение.

  При изменении параметров исключения, заданного при помощи сетевого профиля, это исключение становится пользовательским.

- **Удалить исключение из списка**

  Чтобы удалить исключение из списка, выполните следующие действия:

  1. В списке **Исключения** выберите исключение, которое необходимо удалить.
  2. Нажмите на кнопку **Удалить**.

  Исключение удалено из списка исключений.

4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Настройка типа политики Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Выбор типа политики Kaspersky Endpoint Agent необходим для того, чтобы состав отображаемых в политике параметров соответствовал выбранному способу развертывания Kaspersky Endpoint Agent.

Чтобы настроить тип политики, выполните следующие действия:

1. Откройте окно свойств политики программы.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Параметры программы** выберите подраздел **Интерфейс и управление**.
3. В открывшемся окне выберите необходимый способ развертывания Kaspersky Endpoint Agent, установив соответствующие флажки:

   - **Интеграция с Kaspersky Sandbox**
   - **Endpoint Detection and Response Optimum**
   - **Endpoint Detection and Response Expert (KATA EDR)**

   Выбор типа политики и интеграция с Kaspersky Sandbox и KATA EDR недоступны в Kaspersky Security Center Cloud Console.

4. Нажмите **OK**.

Тип политики изменен. В политике доступны параметры для выбранного способа развертывания Kaspersky Endpoint Agent.

Настройка использования KSN в Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 программы EPP 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.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Endpoint Agent передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. По умолчанию использование KSN отключено. После включения использования KSN, вы можете отключить эту опцию в любой момент времени.

Начиная с версии 3.10 в Kaspersky Endpoint Agent нет возможности настроить использование службы Kaspersky Managed Protection (далее KMP). Если в предыдущей установленной версии Kaspersky Endpoint Agent было включено использование службы KMP, то после обновления программы до версии 3.10 и выше служба KMP продолжает работать как раньше. После обновления вы можете отключить службу KMP только при помощи Плагина управления Kaspersky Endpoint Agent или Веб-плагина Kaspersky Endpoint Agent версий ниже 3.10.

Чтобы включить использование KSN, выполните следующие действия:

1. Выполните одно из следующих действий:

   - **Откройте окно свойств программы для отдельного устройства**.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - **Откройте окно свойств политики программы**.

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Kaspersky Security Network** нажмите на ссылку **Ознакомиться с условиями Положения о KSN** и выполните следующие действия:
   a. В правой части окна ознакомьтесь с условиями Положения о KSN.
   b. Если вы согласны с условиями Положения, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Положения о KSN**.
   c. Нажмите на кнопку **OK**.
3. Установите флажок **Включить использование Kaspersky Security Network (KSN)**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **OK**.
6. В окне свойств политики нажмите на кнопку **Сохранить**.

Использование KSN будет включено.

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox недоступна в интерфейсе Kaspersky Security Center Cloud Console.

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с Kaspersky Sandbox. Интеграцию требуется настроить как на стороне Kaspersky Endpoint Agent с помощью веб-консоли Kaspersky Security Center, так и на стороне Kaspersky Sandbox с помощью веб-интерфейса.

Включение и отключение интеграции с Kaspersky Sandbox

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox недоступна в интерфейсе Kaspersky Security Center Cloud Console.

Чтобы включить или отключить интеграцию с Kaspersky Sandbox, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры подключения**.
3. В блоке параметров **Параметры интеграции с Kaspersky Sandbox** включите или отключите параметр **Включить интеграцию с Kaspersky Sandbox**.
4. Если вы настраиваете параметры через окно свойств политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **OK**.
6. Нажмите на кнопку **Сохранить**.

Интеграция с Kaspersky Sandbox будет включена или отключена на стороне Kaspersky Endpoint Agent.

Настройка доверенного соединения на стороне Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить доверенное соединение Kaspersky Sandbox с Kaspersky Endpoint Agent в веб-интерфейсе сервера Kaspersky Sandbox, не входящего в кластер.

Если вы уже объединили серверы в кластер, вам нужно удалить сервер из кластера, затем создать новый кластер на базе этого сервера и добавить в новый кластер все серверы, предназначенные для работы решения Kaspersky Sandbox.

Если нужные вам серверы входят в другой кластер, вам нужно последовательно удалить их из кластера, в который они входят в настоящий момент, а затем добавить в новый кластер.

Чтобы настроить доверенное соединение на стороне Kaspersky Endpoint Agent, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры подключения**.

3. В блоке параметров **Параметры интеграции с Kaspersky Sandbox** установите флажок **Использовать закреплённый сертификат для защиты соединения**.

4. Нажмите на кнопку **Использовать доверенное соединение**.

   Откроется окно **Добавить TLS-сертификат**.

5. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Sandbox:

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Загрузить**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Открыть**.
   - Скопируйте содержимое файла сертификата в поле **Данные TLS-сертификата**.

   В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Sandbox. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

6. Нажмите на кнопку **OK**.

   Информация о добавленном TLS-сертификате отобразится в блоке параметров **Параметры интеграции с Kaspersky Sandbox**.

7. Если вы настраиваете параметры через окно свойств политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

8. Нажмите на кнопку **OK**.

9. Нажмите на кнопку **Сохранить**.

Доверенное соединение с сервером Kaspersky Sandbox будет настроено.

Добавление серверов Kaspersky Sandbox в список Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы используете Nginx в качестве прокси-сервера между устройством с Kaspersky Endpoint Agent и сервером Kaspersky Sandbox, 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 Kaspersky Sandbox. Иначе Nginx не будет пропускать объекты, размер которых превышает установленное значение. Значение по умолчанию – 1 МБ.

Если вы включили интеграцию с Kaspersky Sandbox, вы можете добавить серверы Kaspersky Sandbox в список Kaspersky Endpoint Agent. Можно добавить несколько серверов Kaspersky Sandbox.

В рамках одной политики добавляйте серверы, входящие в один кластер. Если серверы входят в разные кластеры, результат работы решения непредсказуем.

Чтобы добавить серверы Kaspersky Sandbox в список Kaspersky Endpoint Agent, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Параметры подключения**.
3. Установите флажок **Включить интеграцию с Kaspersky Sandbox**, если он снят.
4. В блоке параметров **Параметры интеграции с Kaspersky Sandbox** включите или выключите параметр **Подключаться через прокси-сервер, если это задано в общих параметрах**.

   По умолчанию параметр выключен. Программа подключается к серверу Kaspersky Sandbox только напрямую и не использует общие параметры соединения с прокси-сервером. Вы можете включить параметр, если вы хотите, чтобы программа использовала общие параметры соединения с прокси-сервером при подключении к серверу Kaspersky Sandbox.
5. В блоке параметров **Список серверов Kaspersky Sandbox** нажмите на кнопку **Добавить**.
6. В правой части экрана введите IP-адрес или полное доменное имя сервера Kaspersky Sandbox, а также порт подключения к серверу.
7. Нажмите на кнопку **OK**.

   Добавленный сервер отобразится в таблице серверов.
8. Повторите действия для добавления каждого сервера Kaspersky Sandbox в список.

9. Если вы настраиваете параметры через окно свойств политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

10. Нажмите на кнопку **OK**.

11. Нажмите на кнопку **Сохранить**.

Серверы Kaspersky Sandbox будут добавлены в список Kaspersky Endpoint Agent.

Настройка времени ожидания ответа от Kaspersky Sandbox и параметров очереди запросов

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить время ожидания ответа от Kaspersky Sandbox и параметры очереди запросов на обработку объектов, поступающих от Kaspersky Endpoint Agent в Kaspersky Sandbox, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Расширенные параметры Kaspersky Sandbox**.

3. В блоке параметров **Время ожидания** укажите максимальное время ожидания ответа от сервера Kaspersky Sandbox.

   По умолчанию задано 5 секунд.

4. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

5. В блоке параметров **Очередь запросов Kaspersky Sandbox** в поле **Папка очереди** укажите путь к папке, в которой будет храниться информация о запросах, отправляемых в Kaspersky Sandbox.

   По умолчанию задана папка %SOYUZAPPDATA%\Sandbox\Queue.

6. В поле **Максимальный размер очереди (МБ)** укажите максимально допустимый размер очереди запросов в мегабайтах.

   По умолчанию задано 100 МБ.

7. Если вы настраиваете параметры в окне свойств политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

8. Нажмите на кнопку **ОК**.

9. В окне свойств политики нажмите на кнопку **Сохранить**.

Настройка действий Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent может выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox.

Вы можете настроить действия следующих типов:

- **Локальные действия**

Локальные действия – действия, которые будут выполняться на каждом устройстве, на котором обнаружена угроза:

- **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.

- **EPP запустить проверку важных областей на устройстве**.

  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**

  Групповые действия – действия, которые будут выполняться на всех устройствах группы администрирования, для которой вы настраиваете политику.

  - **Запустить Поиск IOC на 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.

  - **EPP выполнять проверку важных областей на устройстве 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.

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.

Если вы хотите, чтобы программа Kaspersky Endpoint Agent создавала Автономные задачи поиска IOC при реагировании на угрозы, необходимо настроить аутентификацию на Сервере администрирования.

Программа использует специальную учетную запись пользователя на Сервере администрирования, которая имеет ограниченные права и предназначена только для создания Автономных задач поиска IOC.

Специальную учетную запись можно создать только через окно **Реагирование на угрозы** в свойствах политики Kaspersky Endpoint Agent или в свойствах программы для отдельного устройства. Специальную учетную запись необходимо создать на Сервере администрирования один раз и использовать ее пароль для настройки параметров **Реагирование на угрозы** в свойствах других устройств или других политик, относящихся к тому же Серверу администрирования.

Невозможно изменить пароль созданной специальной учетной записи для Автономных задач поиска IOC. Если вы забыли пароль от учетной записи, удалите ее стандартными средствами Kaspersky Security Center и повторно создайте учетную запись через окно **Реагирование на угрозы**.

Чтобы настроить действия Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.

3. Установите флажок **Выполнять действия по реагированию на угрозы, обнаруженные Kaspersky Sandbox**.

4. В списке **Выбранные действия** установите флажки для тех действий, выполнение которых вы хотите включить.

5. Если вы выбрали действие **Запустить Поиск IOC на управляемой группе устройств**, в блоке параметров **Аутентификация на Сервере администрирования** выполните следующие действия:

   a. Нажмите на кнопку **Создать специального пользователя**.

   > Если кнопка **Создать специального пользователя** недоступна, значит специальная учетная запись для Автономных задач поиска IOC уже создана. Перейдите на шаг инструкции "d".

   b. В открывшемся окне в поле **Пароль для Сервера администрирования** задайте пароль длиной от 8 до 16 символов и нажмите на кнопку **Создать пользователя**.

   c. Нажмите на кнопку **OK**.

   Специальная учетная запись Сервера администрирования для Автономных задач поиска IOC создана.

   d. В поле **Пароль для Сервера администрирования** введите пароль специальной учетной записи для Автономных задач поиска IOC, созданной ранее.

6. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

7. Нажмите на кнопку **OK**.

8. В окне свойств политики нажмите на кнопку **Сохранить**.

Действия Kaspersky Endpoint Agent по реагированию на угрозы, обнаруженные Kaspersky Sandbox, настроены и готовы применяться на устройствах.

Включение обнаружения легальных программ, которые могут быть использованы злоумышленниками

> Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете включить обнаружение легальных программ, при использовании которых злоумышленники могут нанести вред компьютерной сети вашей организации. Kaspersky Endpoint Agent будет считать такие программы угрозой и выполнять над ними действия по реагированию на угрозы.

Легальные программы – программы, разрешенные к установке и использованию на компьютерах пользователей и предназначенные для выполнения задач пользователя. Однако легальные программы некоторых типов при использовании злоумышленниками могут нанести вред компьютеру пользователя или компьютерной сети организации. Если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые функции таких программ для нарушения безопасности компьютера пользователя или компьютерной сети организации.

Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Если вы хотите включить обнаружение таких программ, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
3. В блоке параметров **Дополнительные параметры** установите флажок **Включить обнаружение легальных программ, которые могут быть использованы злоумышленниками**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **ОК**.
6. В окне свойств политики нажмите на кнопку **Сохранить**.

Настройка запуска задач поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить запуск задач поиска IOC, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Интеграция с Kaspersky Sandbox** выберите подраздел **Реагирование на угрозы**.
3. В блоке параметров **Дополнительные параметры** нажмите на ссылку **Настроить поиск IOC**.
4. В правой части экрана в блоке параметров **Области поиска** выберите одну из следующих областей, в которых Kaspersky Endpoint Agent будет выполнять поиск IOC:

   - **Файловые области на системных дисках устройства**.
   - **Важные файловые области на устройстве**.

5. В блоке параметров **Настроить поиск IOC** выберите один из следующих вариантов запуска задач поиска IOC:

   - **Вручную**.

     Задачи поиска IOC будут создаваться автоматически, но не будут запускаться. Вы сможете запускать вручную каждую задачу или все задачи.

   - **Сразу после того, как Kaspersky Sandbox обнаружит угрозу**.

     Задачи поиска IOC будут автоматически создаваться и запускаться.

- **Запускать в заданный период**.

  Задачи поиска IOC будут создаваться автоматически, а запускаться будут в заданный период. Например, в нерабочее время с 20:00 до 7:00.

  Если вы выбрали вариант **Запускать в заданный период**, в полях **Начало периода (чч:мм)** и **Конец периода (чч:мм)** настройте начало и конец периода.

  Все задачи поиска IOC, автоматически созданные ДО указанного начала периода, запустятся в произвольное время В ПРЕДЕЛАХ указанного периода.

  Все задачи поиска IOC, автоматически созданные В ПРЕДЕЛАХ указанного периода, запустятся немедленно.

  Все задачи поиска IOC, автоматически созданные ПОСЛЕ указанного начала периода, запустятся на следующий день.

Пример:
Если вы настроили запуск задач в заданный 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.

6. Нажмите на кнопку **OK**.
7. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
8. Нажмите на кнопку **OK**.
9. В окне свойств политики нажмите на кнопку **Сохранить**.

Настройка интеграции Kaspersky Endpoint Agent с KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с компонентом KATA Central Node с помощью Kaspersky Security Center Web Console.

Включение и отключение интеграции с KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы используете Nginx в качестве прокси-сервера между устройством с Kaspersky Endpoint Agent и сервером KATA, 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 KATA. Иначе Nginx не будет пропускать объекты, размер которых превышает установленное значение. Значение по умолчанию – 1 МБ.

Чтобы включить или отключить интеграцию с компонентом KATA Central Node, выполните следующие действия:

1. Откройте окно свойств политики программы.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KATA**.

   Откроется окно **Интеграция с KATA**.

3. 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**.

4. Включите или выключите параметр **Подключаться через прокси-сервер, если это задано в общих параметрах**.

   По умолчанию параметр выключен. Программа подключается к серверу KATA только напрямую и не использует общие параметры соединения с прокси-сервером. Вы можете включить параметр, если вы хотите, чтобы программа использовала общие параметры соединения с прокси-сервером при подключении к серверу KATA.

5. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

6. Нажмите на кнопку **OK**.

Интеграция с KATA Central Node будет включена или отключена.

Настройка доверенного соединения с KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить доверенное соединение Kaspersky Endpoint Agent с KATA Central Node, выполните следующие действия на стороне Kaspersky Endpoint Agent:

1. **Откройте окно свойств политики программы**.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KATA**.

   Откроется окно **Интеграция с KATA**.

3. В блоке параметров **Параметры подключения** установите флажок **Использовать закреплённый сертификат для защиты соединения**.

4. Нажмите на кнопку **Добавить TLS-сертификат**.

   Откроется окно добавления TLS-сертификата.

5. Выполните одно из следующих действий по добавлению TLS-сертификата:

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Загрузить**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Открыть**.
   - Скопируйте содержимое файла сертификата в поле **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.

6. Нажмите на кнопку **OK**.

   Информация о добавленном TLS-сертификате отобразится в блоке параметров **Данные TLS-сертификата**.

7. Если вы хотите настроить дополнительную защиту подключения с использованием пользовательского сертификата, выполните следующие действия:

   a. Установите флажок **Защита подключения с помощью сертификата клиента**.

b. Нажмите на кнопку **Загрузить крипто-контейнер**.

c. В открывшемся окне выберите архив формата PFX и нажмите на кнопку **Открыть**.

d. В поле **Пароль крипто-контейнера** введите пароль к архиву формата PFX.

e. Нажмите на кнопку **OK**.

8. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

9. Нажмите на кнопку **OK**.

Доверенное соединение с сервером KATA настроено.

Настройка параметров синхронизации Kaspersky Endpoint Agent с KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры синхронизации Kaspersky Endpoint Agent с KATA Central Node, выполните следующие действия:

1. **Откройте окно свойств политики программы**.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KATA**.

   Откроется окно **Интеграция с KATA.**

3. В блоке параметров **Дополнительные параметры** настройте следующие параметры:

   - **Время ожидания (сек.)**. Укажите максимальное время ожидания ответа от сервера KATA. По умолчанию задано 10 секунд.
   - **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. По умолчанию задано 5 минут.

- Установите или снимите флажок **Использовать период TTL при отправке событий**. По умолчанию флажок снят.

  При установленном флажке Kaspersky Endpoint Agent не отправляет на сервер KATA информацию о процессах, которые запускаются повторно. Kaspersky Endpoint Agent не считает запуск процесса повторным, если запуск происходит после окончания очередного периода TTL.

- Если вы установили флажок **Использовать период TTL при отправке событий**, укажите время в поле **Период TTL (мин.)**. По умолчанию задано 1440 минут.

4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

5. Нажмите на кнопку **OK**.

Настройка параметров передачи данных

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры передачи данных, выполните следующие действия:

1. Откройте окно свойств политики программы.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Общие параметры**.

   Откроется окно **Общие параметры**.

3. В блоке параметров **Параметры передачи данных** выполните следующие действия:

   - Укажите значения в поле **Максимальное время передачи событий (сек.)**.
   - Укажите значения в поле **Максимальное количество событий в одном пакете**.

4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

5. Нажмите на кнопку **OK**.

Настройка параметров регулирования количества запросов

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Функция регулирования количества запросов позволяет ограничить поток событий низкой важности от Kaspersky Endpoint Agent к компоненту Central Node.

Чтобы настроить параметры регулирования количества запросов:

1. **Откройте окно свойств политики программы**.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Общие параметры**.

   Откроется окно **Общие параметры**.

3. В блоке параметров **Регулирование количества запросов** вы можете выполнить следующие действия:

   - Установить или снять флажок **Включить регулирование количества запросов**, чтобы включить или отключить функцию.

     По умолчанию функция включена.

   - Указать значения в поле **Максимальное количество событий в час**.

     Программа анализирует поток данных телеметрии и ограничивает передачу событий низкой важности, если поток передаваемых событий стремится превысить указанную в этом поле величину. По умолчанию задано 3000 событий в час.

   - Указать значения в поле **Процент превышения лимита событий**.

     Если поток однотипных событий низкой важности превысит указанный в этом поле порог в процентах от общего количества событий, то именно этот тип событий будет ограничен. Можно задать величину от 5% до 100%. По умолчанию задано 15%.

4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

5. Нажмите на кнопку **OK**.

Настройка интеграции Kaspersky Endpoint Agent с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с программой Kaspersky Industrial CyberSecurity for Networks при помощи Kaspersky Security Center Web Console.

Включение интеграции с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

Чтобы включить интеграцию с программой KICS for Networks:

1. **Откройте окно свойств политики программы**.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KICS for Networks**.

   Откроется окно **Интеграция с KICS for Networks**.

3. В блоке параметров **Параметры подключения** установите флажок **Включить интеграцию с KICS for Networks**.
4. Укажите IP-адрес или полное доменное имя сервера **KICS for Networks**, а также порт подключения к серверу.
5. Включите или выключите параметр **Подключаться через прокси-сервер, если это задано в общих параметрах**.

По умолчанию параметр выключен. Программа подключается к серверу KICS for Networks только напрямую и не использует общие параметры соединения с прокси-сервером. Вы можете включить параметр, если вы хотите, чтобы программа использовала общие параметры соединения с прокси-сервером при подключении к серверу KICS for Networks.

6. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

7. Нажмите на кнопку **OK**.

Интеграция с KICS for Networks будет включена.

Настройка доверенного соединения с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

Чтобы настроить доверенное соединение Kaspersky Endpoint Agent с KICS for Networks, выполните следующие действия на стороне Kaspersky Endpoint Agent:

1. **Откройте окно свойств политики программы**.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KICS for Networks**.

   Откроется окно **Интеграция с KICS for Networks**.

3. В блоке параметров **Параметры подключения** установите флажок **Использовать закреплённый сертификат для защиты соединения**.

4. Нажмите на кнопку **Добавить TLS-сертификат**.

   Откроется окно добавления TLS-сертификата.

5. Выполните одно из следующих действий по добавлению TLS-сертификата:

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Загрузить**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Открыть**.

- Скопируйте содержимое файла сертификата в поле **Данные TLS-сертификата**.

В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера KICS for Networks. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

6. Нажмите на кнопку **OK**.

   Информация о добавленном TLS-сертификате отобразится в блоке параметров **Данные TLS-сертификата**.

7. Если вы хотите настроить дополнительную защиту подключения с использованием пользовательского сертификата, выполните следующие действия:

   a. Установите флажок **Защита подключения с помощью сертификата клиента**.

   b. Нажмите на кнопку **Загрузить крипто-контейнер**.

   c. В открывшемся окне выберите архив формата PFX и нажмите на кнопку **Открыть**.

   d. В поле **Пароль крипто-контейнера** введите пароль к архиву формата PFX.

   e. Нажмите на кнопку **OK**.

8. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

9. Нажмите на кнопку **OK**.

Доверенное соединение с сервером KICS for Networks настроено.

Настройка параметров синхронизации Kaspersky Endpoint Agent с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

Чтобы настроить параметры синхронизации Kaspersky Endpoint Agent с KICS for Networks, выполните следующие действия:

1. Откройте окно свойств политики программы.

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KICS for Networks**.

   Откроется окно **Интеграция с KICS for Networks.**

3. В блоке параметров **Дополнительные параметры** укажите максимальное время ожидания ответа от сервера KICS for Networks в поле **Время ожидания (сек.)**.

   По умолчанию задано 10 секунд.

4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

5. Нажмите на кнопку **OK**.

Параметры синхронизации Kaspersky Endpoint Agent с сервером KICS for Networks настроены и применяются.

Настройка параметров передачи данных

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры передачи данных, выполните следующие действия:

1. Откройте окно свойств политики программы.
   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
2. В разделе **Серверы сбора телеметрии** выберите **Общие параметры**.

   Откроется окно **Общие параметры**.

3. В блоке параметров **Параметры передачи данных** выполните следующие действия:

- Укажите значения в поле **Максимальное время передачи событий (сек.)**.
- Укажите значения в поле **Максимальное количество событий в одном пакете**.

4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

5. Нажмите на кнопку **OK**.

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Перед выполнением следующих инструкций требуется получить конфигурационный файл MDR. Он содержит конфигурационный файл (BLOB), необходимый для интеграции.

Загружая конфигурационный файл Kaspersky Managed Detection and Response, вы соглашаетесь автоматически передавать данные с устройства с установленной программой Kaspersky Endpoint Security в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку передаваемых данных.

Если требуется, чтобы программа Kaspersky Endpoint Agent обрабатывала данные о событиях, формируемых Kaspersky Industrial CyberSecurity for Networks, и отправляла эти данные в Kaspersky Managed Detection and Response, в параметрах Kaspersky Industrial CyberSecurity for Networks необходимо настроить взаимодействие с Kaspersky Security Center. Подробная информация о настройке взаимодействия программ приведена в документации Kaspersky Industrial CyberSecurity for Networks.

Чтобы настроить интеграцию Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response с помощью Kaspersky Security Center Web Console:

1. Откройте Kaspersky Security Center Web Console.
2. Перейдите на закладку **Устройства** → **Политики и профили**.
3. В списке политик выберите название политики Kaspersky Endpoint Agent, которую вы хотите настроить.

   Откроется окно параметров политики.

4. Включите **Использование KSN**.

   Перейдите на главное окно Kaspersky Security Center Web Console.

5. В дереве Консоли администрирования настройте параметры Локального KSN (Подробнее о настройке параметров прокси-сервера Kaspersky Security Network см. в *Справке Kaspersky Security Center*).

   Загрузите файл конфигурации Kaspersky Managed Detection and Response с расширением pkcs7, который включен в архив mdr_config.zip.

6. Откройте главное окно Kaspersky Security Center Web Console для продолжения настройки интеграции Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response.

7. Перейдите на закладку **Устройства** → **Политики и профили**.

8. В списке политик выберите название политики Kaspersky Endpoint Agent, которую вы хотите настроить.

   Откроется окно параметров политики.

9. На закладке **Параметры программы** выберите пункт **Managed Detection and Response**.

10. В блоке параметров **Параметры Managed Detection and Response** выполните следующие действия:

    a. Установите переключатель в положение **Managed Detection and Response включен**.

    b. Нажмите на кнопку **Загрузить конфигурационный файл (BLOB)**, а затем выберите конфигурационный файл BLOB для загрузки.

    c. В поле **Идентификатор пользователя** введите произвольное значение.

    d. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

Интеграция Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response настроена.

Работа MDR при совместном использовании Kaspersky Endpoint Agent и Kaspersky Endpoint Security

Программа Kaspersky Endpoint Security версии 11 или выше с актуальной версией баз поддерживает взаимодействие с решением MDR. В Kaspersky Endpoint Security версии 11.6.0 или выше поддержка взаимодействия с решением MDR доступна сразу после установки.

Если на устройстве вы использовали Kaspersky Endpoint Agent для работы с решением MDR и установили Kaspersky Endpoint Security версии, поддерживающей взаимодействие с решением MDR, или обновили базы Kaspersky Endpoint Security 11 или выше до актуальной версии, решение MDR прекращает работу с Kaspersky Endpoint Agent и становится доступным для работы с Kaspersky Endpoint Security, при этом:

- переключение между Kaspersky Endpoint Agent и Kaspersky Endpoint Security выполняется в тихом режиме;
- в Kaspersky Endpoint Agent доступна настройка параметров взаимодействия с решением MDR, но эти параметры не применяются на устройстве;
- при недоступности Kaspersky Endpoint Security (например, вы удалили программу), решение MDR может возобновить работу с Kaspersky Endpoint Agent, если перезапустить службу Kaspersky Endpoint Agent;
- компонент Managed Detection and Response в параметрах Kaspersky Endpoint Agent на устройстве остается в статусе *Запущен*, т.к. Kaspersky Endpoint Agent продолжает поддерживать связь с решением MDR (например, чтобы возобновить работу с решением при необходимости).

Настройка параметров EDR-телеметрии

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе содержится информация о том, как настроить исключения для EDR-телеметрии, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом KATA Central Node.

Включение и настройка исключений для EDR-телеметрии

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить исключения для EDR-телеметрии с помощью Kaspersky Security Center Web Console как в свойствах отдельного устройства, так и в свойствах политики для группы устройств.

Чтобы включить и настроить исключения для EDR-телеметрии:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **EDR-телеметрия** выберите **Исключения**.

   Откроется окно настройки параметров исключений для EDR-телеметрии.

3. Чтобы включить применение исключений для EDR-телеметрии, установите флажок **Использовать исключения**.

4. Чтобы добавить новое исключение, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Свойства правила** настройте следующие критерии исключения:

      Критерии применяются при помощи логического И.

      Для создания правила необходимо обязательно задать значение в поле **Полный путь** и выбрать хотя бы один из типов событий в списке **Использовать это исключение для следующих типов событий**.

      Если для критерия **Использовать это исключение для следующих типов событий** выбрана опция **Сетевые события**, в поле **Полный путь** необходимо указать полный путь к файлу.

      Объект, для которого вы создаете исключение, должен присутствовать на защищаемом устройстве в момент применения параметров исключения. Например, если вы сначала настроите исключение для определенного приложения, а потом установите это приложение на защищаемое устройство, такое исключение не будет применяться.

      - В блоке **Информация о процессе** задайте значения в следующих полях:
        - **Полный путь**. Полный путь к файлу, включая его имя и расширение. Можно использовать маски файлов (с помощью символов ? и *), а также системные переменные окружения.
        - **Текст командной строки**. Командная строка для запуска объекта.
        - **Родительский путь**. Путь до папки, в которой находится файл.
      - В блоке **Свойства файла** задайте значения в следующих полях:
        - **Описание файла**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo).
        - **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo).
        - **Версия файла**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo).
      - В блоке **Контрольные суммы файла** задайте значения в следующих полях:
        - **MD5**. MD5-хеш файла.
        - **SHA256**. SHA256-хеш файла.
      - В списке **Использовать это исключение для следующих типов событий** выберите как минимум одну из следующих опций:
        - **Изменение файла**.

- **Сетевые события**.
- **Интерактивный ввод в консоли**. По умолчанию эта опция выбрана.
- **Загрузка модуля процесса**.
- **Изменения в реестре**.

c. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Свойства правила**.

Новое правило создано и отображается в списке исключений.

5. Чтобы удалить правило из списка исключений, установите флажок рядом с именем правила и нажмите на кнопку **Удалить**.
6. Чтобы открыть окно свойств уже созданного правила для изменения заданных критериев, установите флажок рядом с именем правила и нажмите на кнопку **Изменить**.
7. Если вы настраиваете параметры политики, убедитесь, что положение переключателя в правом верхнем углу блока параметров находится в положении **Принудительно**. Переключатель находится в этом положении по умолчанию.
8. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Исключения**.

Исключения для EDR-телеметрии используются по настроенным правилам.

Настройка параметров Запрета запуска

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе приведены инструкции по настройке параметров Запрета запуска.

Включение Запрета запуска

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы включить Запрет запуска:

1. Выполните одно из следующих действий:
   - Откройте окно свойств программы для отдельного устройства.

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите устройство.
3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
4. Выберите **Kaspersky Endpoint Agent**.
5. В открывшемся окне выберите закладку **Параметры программы**.

- Откройте окно свойств политики программы.

  1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
  2. Выберите политику, которую вы хотите настроить.
  3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. Выберите раздел **Запрет запуска**.
3. В блоке параметров **Режим запрета** установите флажок **Включить запрет запуска недоверенных объектов**.
4. В раскрывающемся списке **Применять правила запрета в режиме** выберите требуемый режим применения правил запрета:

   - **Только статистика**.

     В этом режиме Kaspersky Endpoint Agent публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках исполнения объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их исполнение или открытие.

   - **Активный**.

     В этом режиме Kaspersky Endpoint Agent блокирует исполнение объектов или открытие документов, соответствующих критериям правил запрета.

   При включении Запрета запуска в Kaspersky Security Center по умолчанию выбран режим **Только статистика**.

5. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**.

Отключение Запрета запуска

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы отключить Запрет запуска:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. Выберите раздел **Запрет запуска**.
3. В блоке параметров **Режим запрета** снимите флажок **Включить запрет запуска недоверенных объектов**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **OK**.
6. Нажмите на кнопку **Сохранить**.

Включение и отключение уведомления пользователей о Запрете запуска

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете выбрать опцию **Уведомлять пользователя устройства при запрете**.

Если Запрет запуска включен в режиме **Активный** и выбрана опция **Уведомлять пользователя устройства при запрете**, на защищаемых устройствах будут отображаться всплывающие уведомления с информацией о сработавших правилах Запрета запуска. Если пользователь устройства не закроет всплывающее уведомление, то оно закроется автоматически через 60 секунд после появления. По умолчанию опция **Уведомлять пользователя устройства при запрете** выключена.

Предварительно необходимо включить Запрет запуска.

Чтобы включить или отключить уведомление пользователя о Запрете запуска:

1. Выполните одно из следующих действий:

   - **Откройте окно свойств программы для отдельного устройства**

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - **Откройте окно свойств политики программы**

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. Выберите раздел **Запрет запуска**.
3. В блоке параметров **Режим запрета** установите или снимите флажок **Уведомлять пользователя устройства при запрете**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **ОК**.
6. В окне свойств политики нажмите на кнопку **Сохранить**.

Управление списком правил Запрета запуска

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить список правил Запрета запуска:

1. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. Выберите раздел **Запрет запуска**.
3. В блоке параметров **Правила запрета** можно выполнить следующие действия:
   - Добавить правило запрета в список.
   - Изменить параметры правила запрета.
   - Удалить правило запрета из списка.
4. В блоке параметров **Правила запрета** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения правил запрета.
5. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

6. Нажмите на кнопку **OK**.

7. В окне свойств политики нажмите на кнопку **Сохранить**.

При использовании Kaspersky Endpoint Agent версии 3.9 правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Исполнение или открытие этих файлов *не* будет заблокировано программой.

При использовании Kaspersky Endpoint Agent версии 3.10 и выше, чтобы создать правило запрета по критерию пути к файлу, расположенному на компакт-диске или в ISO-образе, необходимо указать путь в формате `\?\GLOBALROOT\Device\<имя устройства>\<путь к файлу>`, где `<имя устройства>` - это имя устройства чтения компакт-дисков или смонтированного ISO-образа в вашей системе. Например, путь может выглядеть следующим образом: `\?\GLOBALROOT\Device\CdRom1\some_file.exe`.

При указании объектов по критерию пути к файлу можно использовать маски файлов (с помощью символов ? и *).

Настройка параметров хранилищ в Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе приведены инструкции по настройке параметров карантина и параметров синхронизации данных с Сервером администрирования с помощью плагина управления Kaspersky Endpoint Agent.

О карантине Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Через Kaspersky Security Center можно настраивать параметры карантина, просматривать свойства объектов, находящихся на карантине на защищаемых устройствах, 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 документации 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 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.

Kaspersky Endpoint Agent помещает объект 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры карантина, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.

2. Выберите политику, которую вы хотите настроить.

3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

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 мегабайтах.

   Например, вы можете задать максимальный размер карантина 200 МБ.

   При достижении максимального размера карантина Kaspersky Endpoint Agent публикует соответствующее 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 соответствующее 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. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

8. Нажмите на кнопки **Применить** и **ОК**.

Параметры карантина и папка для восстановления объектов из карантина будут настроены.

Настройка синхронизации данных с Сервером администрирования

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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. Выполните одно из следующих действий:

   - Откройте окно свойств программы для отдельного устройства.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - Откройте окно свойств политики программы.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.
3. Установите флажок **Данные об объектах в Карантине на управляемых устройствах**.
4. Нажмите на кнопку **OK**.
5. Нажмите на кнопку **Сохранить**.

Синхронизация данных с Сервером администрирования будет настроена.

Настройка построения цепочки развития угрозы

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Для построения цепочки развития угрозы необходимо выполнение определенных предусловий.

Вы можете включить построение цепочки развития угрозы для объектов, обнаруженных на управляемых устройствах. Цепочка развития угрозы отображается в карточке инцидента.

Чтобы включить построение цепочки развития угрозы, выполните следующие действия:

1. Выполните одно из следующих действий:

   - **Откройте окно свойств программы для отдельного устройства**.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

   - **Откройте окно свойств политики программы**.

     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
     2. Выберите политику, которую вы хотите настроить.
     3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.
3. Установите флажок **Отправлять данные для построения цепочки развития угрозы** в блоке параметров **Синхронизация с Сервером администрирования**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров **Синхронизация с Сервером администрирования** измените положение переключателя с **Не определено** на **Принудительно**.

5. Нажмите на кнопку **OK**.

6. Нажмите на кнопку **Сохранить**.

Построение цепочки развития угрозы настроено.

Настройка диагностики сбоев

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent не создает папку для сохранения файлов трассировки или файлов дампа на устройстве автоматически. Необходимо указать папку, которая уже доступна на устройстве.

Чтобы настроить диагностику сбоев, выполните следующие действия:

1. Откройте окно свойств программы для отдельного устройства.

    1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
    2. Выберите устройство.
    3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
    4. Выберите **Kaspersky Endpoint Agent**.
    5. В открывшемся окне выберите закладку **Параметры программы**.

2. В разделе **Параметры программы** выберите подраздел **Диагностика сбоев**.

3. Если вы хотите включить запись отладочной информации в файлы трассировки:

    a. Включите параметр **Записывать отладочную информацию в файлы трассировки**.

    b. В поле **Папка файлов трассировки** укажите путь к папке на устройстве, в которую программа должна сохранять файлы трассировки.

    Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе отладочная информация не будет записана.

    c. В поле **Максимальный размер файла трассировки (МБ)** укажите размер файла в мегабайтах.

    По умолчанию задано 50 МБ. При достижении заданного размера файла программа продолжает запись в новый файл.

4. Если вы хотите, чтобы программа выполняла перезапись старых файлов трассировки:

   a. Включите параметр **Перезаписывать старые файлы трассировки**.

   b. В поле **Максимальное количество файлов для одного журнала трассировки** укажите желаемое значение.

   По умолчанию задан 1 файл. Когда достигается указанное количество файлов, программа перезаписывает старые файлы, начиная с самого старого. Указанное ограничение применяется для каждого отлаживаемого процесса Kaspersky Endpoint Agent отдельно, поэтому суммарное количество файлов для всех процессов может превышать заданное значение.

5. Если вы хотите включить запись файлов дампа:

   a. Включите параметр **Создавать файлы дампа**.

   b. В поле **Папка файлов дампа** укажите папку для сохранения файлов дампа.

   > Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе отладочная информация не будет записана.

6. Нажмите на кнопку **OK**.

Диагностика сбоев настроена и включена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы для диагностики сбоев будут создаваться в папках, которые вы указали.

Управление задачами Kaspersky Endpoint Agent

В этом разделе приведены инструкции по управлению задачами Kaspersky Endpoint Agent.

Создание задач

> Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы создать задачу, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Agent**.

4. В раскрывающемся списке **Тип задачи** выберите нужный тип задачи и следуйте дальнейшим шагам мастера.

5. Чтобы изменить заданные по умолчанию значения параметров задачи сразу после ее создания, установите флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**.

   Если вы не установите этот флажок, задача будет создана с заданными по умолчанию значениями параметров, которые вы можете изменить позже в любое время для каждого из следующих типов задач:

   - **Активация программы**
   - **Поиск IOC**
   - **Удалить файл**
   - **Поместить файл на карантин**
   - **Завершить процесс**
   - **Запустить процесс**
   - **Обновление баз и модулей программы**

6. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Просмотр списка задач

Чтобы просмотреть список задач,

в главном окне веб-консоли перейдите в раздел **Устройства** → **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям программ, к которым они относятся.

Удаление задач из списка

Чтобы удалить задачи из списка задач на сервере Kaspersky Security Center, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

   Отобразится список задач.

2. В отобразившемся списке задач установите флажки напротив задач, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены из списка.

Настройка расписания запуска задач

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить запуск задачи по расписанию, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. На закладке **Расписание** в разделе **Общие** переведите переключатель из положения **Расписание выключено** в положение **Запускать по расписанию**.
4. В раскрывающемся списке **Периодичность** выберите один из следующих вариантов: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.
5. Если вы выбрали запуск задачи **В указанное время**, укажите время и дату запуска задачи.
6. Если вы выбрали запуск задачи **Каждый час**, **Каждый день** или **Каждую неделю**, настройте параметры запуска задачи:
   a. В поле **Каждый** задайте периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.
   b. В полях **Время запуска** и **Дата запуска** задайте время и дату начала действия расписания.
7. Чтобы выполнить расширенную настройку расписания, выберите раздел **Дополнительно** и выполните следующие действия:
   a. Если вы хотите задать максимальное время ожидания выполнения задачи, 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 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, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.
   d. Если вы хотите избежать одновременного обращения большого количества устройств к Серверу администрирования и запускать задачу на устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Распределять время запуска задач в интервале** и задайте интервал запуска в минутах.
8. Нажмите на кнопку **Сохранить**.

Запуск задач вручную

Программа запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время.

Чтобы запустить задачу вручную, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в графе **Статус** или нажав на кнопку **Результат выполнения**.

Просмотр результатов выполнения задач

Вы можете просмотреть результаты выполнения задач в течение срока их хранения. Вы также можете изменить срок хранения результатов выполнения задач.

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

Чтобы просмотреть результат выполнения задачи:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

   Отобразится список задач.
2. В отобразившемся списке задач нажмите на имя задачи.

   Откроется окно настройки параметров задачи.
3. Перейдите на закладку **Результаты**.

Информация отображается в списке **Результаты выполнения задачи**.

Вы также можете просмотреть **Результаты последнего выполнения** задачи на закладке **Общие**.

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:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

   Отобразится список задач.

2. В отобразившемся списке задач нажмите на имя задачи.

   Откроется окно настройки параметров задачи.

3. Перейдите на закладку **Параметры**.

4. В разделе **Уведомления** нажмите на кнопку **Параметры.**

5. Убедитесь, что в списке **Выберите поведение программы после завершения задачи** выбран параметр **Хранить в базе данных Сервера администрирования в течение (сут)** и укажите, в течение какого времени (в сутках) требуется хранить результат выполнения задачи.

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить.**

Изменения будут сохранены.

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

Создание задач активации Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете активировать Kaspersky Endpoint Agent с помощью лицензионного ключа из хранилища ключей Kaspersky Security Center. Подробную информацию об управлении лицензионными ключами с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Чтобы создать задачу активации Kaspersky Endpoint Agent, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Agent**.

4. В раскрывающемся списке **Тип задачи** выберите **Активация программы**.

5. В поле **Название задачи** задайте отображаемое имя задачи.

6. Если вы хотите создать задачу для устройств определенной группы Сервера администрирования, выполните следующие действия:

a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Группа устройств** и нажмите **Далее**.

b. Выберите нужную группу Сервера администрирования и нажмите **Далее**.

7. Если вы хотите создать задачу для определенных устройств по диапазону IP-адресов, NetBIOS-именам, DNS-именам или выбрать из списка устройств, обнаруженных в сети Сервером администрирования, выполните следующие действия:

a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Выбранные устройства или импортируемые устройства из списка** и нажмите **Далее**.

b. Добавьте в список устройства по нужным критериям и нажмите **Далее**.

8. Если вы хотите создать задачу для устройств из определенной выборки, выполните следующие действия:

a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Выборка** и нажмите **Далее**.

b. Укажите нужную выборку из списка и нажмите **Далее**.

9. В окне **Выберите лицензионный ключ** выберите нужный лицензионный ключ из списка доступных в хранилище ключей Kaspersky Security Center.

10. Если вы хотите добавить этот лицензионный ключ в качестве дополнительного для автоматического продления срока действия лицензии, установите флажок **Использовать в качестве дополнительного ключа**.

11. Нажмите **Далее**.

12. В окне **Выбор учетной записи для запуска задачи** выберите нужную учетную запись и нажмите **Далее**.

13. Чтобы изменить заданные по умолчанию значения параметров задачи сразу после ее создания, установите флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**.

14. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Настройка параметров задачи обновления баз и модулей программы

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи обновления баз и модулей программы, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры подключения**.
5. Если вы используете Kaspersky Security Center, в блоке параметров **Источник обновлений** выберите один из следующих вариантов:
   - **Сервер администрирования Kaspersky Security Center**.
   - **Серверы обновлений "Лаборатории Касперского"**.
   - **Другие HTTP-, FTP-серверы или сетевые папки**.
6. Если вы используете Kaspersky Security Center Cloud Console, в блоке параметров **Источник обновлений** выберите один из следующих вариантов:
   - **Точки распространения**. Использование в качестве источника обновлений устройства с установленным Агентом администрирования.

     Подробная информация об использовании точек распространения доступна в справке Kaspersky Security Center Cloud Console.
   - **Серверы обновлений "Лаборатории Касперского"**. Использование в качестве источника обновлений серверов обновлений "Лаборатории Касперского".
7. Если вы хотите включить параметр **Использовать серверы обновлений "Лаборатории Касперского", если указанные пользователем серверы недоступны**, установите флажок рядом с названием параметра.

   Недоступно в Kaspersky Security Center Cloud Console.
8. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые папки**, выполните следующие действия:

   Недоступно в Kaspersky Security Center Cloud Console.

   a. Нажмите на ссылку **Параметры**, чтобы открыть окно **Пользовательские источники обновлений**.

   b. Добавьте источники обновлений в список, выполнив следующие действия:

1. Нажмите на кнопку **Добавить**.
2. В открывшемся диалоговом окне в поле **Веб-адрес** введите адрес сервера обновлений (HTTP или FTP), либо путь к сетевой или локальной папке, содержащей файлы обновлений, и нажмите на кнопку **OK**.
3. Если вы хотите использовать этот источник для обновления баз, установите переключатель рядом с его адресом в положение **Включить**.

   Выполняйте аналогичные действия для добавления каждого нового источника.

4. Нажмите на кнопку **OK**.

   Окно **Пользовательские источники обновлений** закроется.

9. Выберите раздел **Параметры обновления**.
10. В блоке параметров **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.
    - **Только проверять наличие важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.
    - **Загружать и устанавливать важные обновления модулей программы**. Kaspersky Endpoint Agent будет проверять доступность обновлений модулей программы и будет загружать и устанавливать критические обновления модулей программы.
11. 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**.
12. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Управление стандартными задачами поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Стандартные задачи поиска IOC – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.

В этом разделе приведены инструкции по управлению стандартными задачами поиска IOC.

Требования к IOC-файлам

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

При создании задач Поиск IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- 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.
- Размер одного IOC-файла не должен превышать 3 МБ. Использование файлов большего размера приводит к завершению задач Поиск IOC с ошибкой. При этом суммарный размер всех добавленных файлов в IOC-коллекции может превышать 3 МБ.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

Особенности и ограничения поддержки стандарта OpenIOC программой приведены в следующей таблице.

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	Полный список поддерживаемых программой IOC-терминов приведен в отдельной таблице.

Поддерживаемые IOC-термины

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC, поддерживаемых программой Kaspersky Endpoint Agent.

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX

Настройка параметров стандартной задачи поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры стандартной задачи поиска IOC выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В разделе **Параметры поиска IOC** настройте IOC-коллекцию, выполнив следующие действия:
   a. В блоке параметров **IOC-файлы** нажмите на кнопку **Переопределить IOC-файлы**.
   b. В открывшемся диалоговом окне нажмите на кнопку **Добавить IOC-файлы** и укажите IOC-файлы, которые вы хотите использовать для задачи.

      Для одной задачи поиска IOC можно выбрать несколько IOC-файлов.
   c. Нажмите на кнопку **OK**, чтобы закрыть диалоговое окно.

      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.
   d. Если вы хотите посмотреть список всех IOC-файлов, которые включены в IOC-коллекцию, а также получить информацию о каждом IOC-файле, выполните следующие действия:
      1. Нажмите на ссылку с именами всех загруженных IOC-файлов в блоке параметров **IOC-файлы**.

         Откроется окно **Содержимое IOC ()**.
      2. Чтобы просмотреть детальную информацию об отдельном IOC-файле, на закладке **IOC-коллекция** в списке файлов нажмите на имя нужного IOC-файла.

         В открывшемся окне отображена информация о выбранном IOC-файле.
      3. Чтобы закрыть окно с информацией о выбранном IOC-файле, нажмите на кнопку **OK** или **Отмена**.

4. Чтобы просмотреть информацию сразу обо всех загруженных IOC-файлах, перейдите на закладку **Данные IOC**.

   В рабочей области окна отображена информация о каждом загруженном IOC-файле.

5. Если вы хотите, чтобы определенный IOC-файл не использовался при запуске задачи поиска IOC, на закладке **IOC-коллекция** переведите переключатель рядом с его именем из положения **Включить** в положение **Исключить**.

6. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Содержимое IOC ()**.

e. Если вы хотите экспортировать созданную IOC-коллекцию, нажмите на кнопку **Экспортировать IOC-коллекцию**.

   В открывшемся окне можно задать имя файла, а также выбрать папку, в которую вы хотите его сохранить.

f. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной папке.

g. В блоке параметров **Ретроспективный поиск IOC** настройте параметры ретроспективного режима поиска IOC:

   1. В блоке параметров **Ретроспективный поиск IOC** включите параметр **Выполнять Ретроспективный поиск IOC в интервале**.

   2. Укажите временной интервал.

      Во время выполнения задачи программа анализирует данные, собранные за указанный вами интервал времени, включая границы указанного интервала (с 00:00 даты начала до 23:59 даты окончания). По умолчанию задан интервал, начинающийся в 00:00 дня, предшествующего дню создания задачи, и заканчивающийся в 23:59 дня создания задачи.

      Если во время выполнения задачи Поиск IOC со включенным параметром **Выполнять Ретроспективный поиск IOC в интервале** программа не обнаруживает данных для анализа за указанный временной интервал, программа не информирует об этом. В этом случае программа сообщает об отсутствии индикаторов компрометации в отчете о выполнении задачи.

h. В блоке параметров **Действия** настройте ответные действия при обнаружении индикатора компрометации:

   1. Установите флажок **Принять ответные действия при обнаружении индикатора компрометации**.

   2. Установите флажок **Изолировать устройство от сети**, чтобы программа Kaspersky Endpoint Agent выполняла сетевую изоляцию устройства, на котором обнаружен индикатор компрометации.

   3. Установите флажок **Поместить на карантин и удалить**, чтобы поместить обнаруженный объект на карантин и удалить его с устройства.

   4. Установите флажок **EPP запустить проверку важных областей на устройстве**, чтобы программа Kaspersky Endpoint Agent отправляла программе EPP команду на выполнение проверки важных областей на всех устройствах группы администрирования, на которых обнаружены индикаторы компрометации.

Если включен параметр **Поместить на карантин и удалить** или **Запустить проверку важных областей**, в качестве ответных действий Kaspersky Endpoint Agent может признать обнаруженные файлы зараженными и удалить их с устройства.

i. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите защитить критические системные файлы от помещения на карантин и удаления при обнаружении индикатора компрометации.

Опция доступна, только если в блоке параметров **Действия** выбрано **Поместить на карантин и удалить**.

При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.

5. В разделе **Дополнительно** выберите типы данных (IOC-документы), которые необходимо анализировать во время выполнения задачи, и настройте дополнительные параметры поиска:

a. В блоке параметров **Выберите типы данных (IOC-документы) для анализа во время поиска IOC** установите флажки рядом с нужными IOC-документами.

В зависимости от загруженных IOC-файлов, некоторые флажки могут быть неактивными.

Kaspersky Endpoint Agent автоматически выбирает типы данных (IOC-документы) для задачи Поиск IOC в соответствии с содержанием загруженных IOC-файлов. Не рекомендуется самостоятельно отменять выбор типов данных.

b. Если установлен флажок **Анализировать данные файлов (FileItem)**, нажмите на ссылку **Дополнительно (FileItem)** и в открывшемся окне **Параметры проверки документа FileItem** выберите области на дисках защищаемого устройства, в которых необходимо искать индикаторы компрометации.

Вы можете выбрать одну из предзаданных областей, а также указать пути до нужных областей самостоятельно.

c. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа FileItem**.

d. Если установлен флажок **Анализировать данные WEL (EventLogItem)**, нажмите на ссылку **Дополнительно (EventLogItem)** и в открывшемся окне **Параметры проверки документа EventLogItem** настройте дополнительные параметры анализа событий:

- **Проверять только события, зафиксированные в течение указанного периода**.

  Если флажок установлен, во время выполнения задачи учитываются только те события, которые были зафиксированы в указанный период.

- **Проверять события, относящиеся к следующим каналам**.

  Список каналов, которые анализируются во время выполнения задачи.

e. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры проверки документа FileItem**.

6. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Просмотр результатов выполнения задачи поиска IOC

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы просмотреть результаты выполнения задачи Поиск IOC, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Результаты поиска IOC**.
5. В раскрывающемся списке **Устройство** выберите, для каких устройств вы хотите просмотреть результаты выполнения задачи поиска IOC.

   Отобразится сводная таблица результатов выполнения задачи на выбранных устройствах.

   Если на устройствах обнаружены индикаторы компрометации, в столбце **Результаты** отображается *обнаружены индикаторы компрометации*.
6. Если вы хотите просмотреть подробную информацию об обнаруженных индикаторах компрометации на определенном устройстве, выполните следующие действия:

   a. Нажмите на ссылку **обнаружены индикаторы компрометации** в строке с именем нужного устройства.

      Откроется окно **Результаты поиска IOC** со списком всех IOC-файлов, использованных в рамках задачи. Если на выбранном устройстве присутствует объект, который совпадает с определенным индикатором компрометации, в столбце **Статус** отображается *совпадает*.

   b. Нажмите на ссылку **совпадает** в строке с именем нужного IOC-файла.

      Откроется окно **Карточка инцидента IOC**.

      Карточка инцидента IOC содержит информацию об объектах на устройстве, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.

      Просмотр Карточки инцидента IOC недоступен для IOC-файлов, при проверке которых не было обнаружено совпадений на устройстве.

Настройка параметров задачи Поместить файл на карантин

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы считаете, что на компьютере находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив на карантин.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи Поместить файл на карантин, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В раскрывающемся списке **Укажите файл, который требуется поместить на карантин** выберите одно из следующих значений: **Указать файл по полному пути** или **Задать файл по пути к папке и контрольной сумме**.
5. Если вы выбрали **Указать файл по полному пути**, укажите значение в поле **Полный путь к файлу**.
6. Если вы выбрали **Задать файл по пути к папке и контрольной сумме**, настройте следующие параметры:
   - В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **MD5** или **SHA256**.
   - Укажите значение в поле **Контрольная сумма файла**.
   - Укажите значение в поле **Путь к папке файла**.
7. В блоке параметров **Действия после помещения файла на карантин** выберите, необходимо ли удалять файл с защищаемого устройства после помещения на карантин.

   Если файл заблокирован другим процессом, то файл будет удален только после перезагрузки устройства.

8. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

   При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.
9. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки устройства. Рекомендуется проверить успешность выполнения задачи после перезагрузки устройства.

Задача помещения файла на карантин может завершиться с ошибкой *Доступ запрещен*, если вы пытаетесь поместить на карантин исполняемый файл, и он запущен в настоящий момент. Чтобы решить проблему, создайте задачу завершения процесса для этого файла, а затем повторите попытку создания задачи помещения файла на карантин.

Настройка параметров задачи Удалить файл

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи Удалить файл, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В списке **Файл, который нужно удалить** нажмите на кнопку **Добавить**.
5. Откроется диалоговое окно **Файл, который нужно удалить**.
6. В раскрывающемся списке **Укажите файл, который нужно удалить** выберите одно из следующих значений: **Указать файл по полному пути** или **Задать файл по пути к папке и контрольной сумме**.
7. Если вы выбрали **Указать файл по полному пути**, укажите значение в поле **Полный путь к файлу**.
8. Если вы выбрали **Задать файл по пути к папке и контрольной сумме**, настройте следующие параметры:
   - В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **MD5** или **SHA256**.
   - Укажите значение в поле **Контрольная сумма файла**.

- Укажите значение в поле **Путь к папке файла**.
- Установите флажок **Включить подпапки**, чтобы программа удаляла все вхождения объекта не только в указанной папке, но и во всех ее подпапках.

9. Нажмите на кнопку **OK**, чтобы добавить заданный объект в список **Файл, который нужно удалить**.

   Вы можете указать несколько объектов для удаления в рамках одной задачи Удалить файл.

10. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

    При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.

11. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки устройства. Рекомендуется проверить успешность удаления файла после перезагрузки устройства.

Удаление файла с подключенного сетевого диска не поддерживается.

Настройка параметров задачи Запустить процесс

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Задача Запустить процесс позволяет запустить необходимую программу или команду на устройстве.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи Запустить процесс, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.

2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Если вы хотите запустить программу с помощью командной строки (cmd.exe) или выполнить команду, введите необходимую команду в поле **Исполняемая команда**.
5. Если вы хотите запустить программу напрямую, выполните следующие действия:
   a. Укажите путь к исполняемому файлу программы в поле **Рабочая папка**.
   b. Укажите ключи запуска программы в поле **Аргументы**.
6. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Настройка параметров задачи Завершить процесс

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы считаете, что запущенный на устройстве процесс может угрожать безопасности устройства или локальной сети организации, вы можете завершить его.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи Завершить процесс, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В поле **Путь** укажите путь к файлу процесса, который вы хотите завершить.
5. В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **Не задан**, **MD5** или **SHA256**.
6. Если вы выбрали **MD5** или **SHA256**, укажите значение в поле **Контрольная сумма**.

7. Если вы хотите, чтобы программа учитывала регистр символов в пути к файлу процесса, установите флажок **Путь с учетом регистра символов**.

8. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

   При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.

9. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Управление Kaspersky Endpoint Agent через интерфейс командной строки

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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).

Для вызова справки по всем доступным к управлению параметрам программы и их возможным значениям,

выполните команду: `agent.exe --help`

Управление активацией Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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`:

- `-305` – срок действия добавляемого ключа истек.
- `2` – неопределенная программная ошибка.
- `-302` – добавляемый ключ находится в списке запрещенных ключей.
- `-301` – добавляемый ключ не подходит для активации Kaspersky Endpoint Agent.
- `-303` – файл ключа поврежден.
- `4` – синтаксические ошибки.
- `-304` – указан некорректный путь к файлу ключа.

Настройка трассировки

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent не создает папку для сохранения файлов трассировки или файлов дампа на устройстве автоматически. Необходимо указать папку, которая уже доступна на устройстве.

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 для сохранения файлов 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.

     Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе файлы трассировки не будут созданы.

   - `agent.exe --trace=enable --folder <путь к папке для сохранения файлов трассировки> --rotation=yes --rotate-file-size=<максимальный размер файла в МБ> --rotate-files-count=<максимальное количество файлов>`, чтобы включить трассировку в режиме перезаписи старых файлов трассировки при достижении указанных значений размера и количества файлов.

     Указанное ограничение по количеству файлов применяется для каждого отлаживаемого процесса Kaspersky Endpoint Agent отдельно, поэтому суммарное количество файлов для всех процессов может превышать заданное значение. Если с параметром `--rotation=yes` не указать параметры `--rotate-file-size` или `--rotate-files-count` (один из, или оба), то программа использует значения по умолчанию. По умолчанию задан 1 файл размером в 50 МБ.

   - `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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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.

     Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе файлы дампа не будут созданы.

   - `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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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.

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 `>]`.

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=<контрольная сумма файла>`	Обязательный параметр, если передан параметр `--hashalg`. Параметр задает контрольную сумму объекта, который вы хотите поместить на карантин.
`--file=<папка с файлом>`	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 Kaspersky Sandbox

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы управлять параметрами интеграции программы Kaspersky Endpoint Agent с Kaspersky Sandbox 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**:

   ```
   --sync-period=<sync period>--sandbox=<enable|disable|show> [--tls=<yes|no>] --servers=<адрес>:<порт> [--timeout=<максимальное время ожидания ответа от сервера Kaspersky Sandbox>] [--pinned-certificate=<полный путь к файлу TLS-сертификата соединения Kaspersky Endpoint Agent с Kaspersky Sandbox>] --pwd=<текущий пароль пользователя>
   ```

Параметры команды `--sandbox` при управлении параметрами интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox

Параметр	Описание
`--sandbox=<enable|disable|show>`	Обязательный параметр. Позволяет включить, отключить и просмотреть состояние интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox. • `--sandbox=<enable>` включает интеграцию. • `--sandbox=<disable>` отключает интеграцию. • `--sandbox=<show>` отображает состояние интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox.

`--tls=<yes|no>`	Необязательный параметр. Позволяет включить или отключить использование доверенного соединения Kaspersky Sandbox с Kaspersky Endpoint Agent. • `--tls=<yes>` включает использование доверенного соединения. • `--tls=<no>` отключает использование доверенного соединения.
`--servers=<адрес>:<порт>`	Обязательный параметр. Позволяет добавить серверы Kaspersky Sandbox в список Kaspersky Endpoint Agent.
`--timeout=<максимальное время ожидания ответа от сервера Kaspersky Sandbox>`	Необязательный параметр. Позволяет задать максимальное время ожидания ответа от сервера Kaspersky Sandbox в миллисекундах.
`--pinned-certificate=<полный путь к файлу TLS-сертификата соединения Kaspersky Endpoint Agent с Kaspersky Sandbox>`	Обязательный параметр, если передан параметр `--tls` со значением `<yes>`. Позволяет добавить TLS-сертификат соединения Kaspersky Endpoint Agent с Kaspersky Sandbox.
`--pwd=<текущий пароль пользователя>`	Позволяет ввести пароль пользователя, с правами учетной записи которого выполняется команда.

Управление параметрами интеграции с компонентом KATA Central Node

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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>`

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.
`--compression=<yes|no>`	Необязательный параметр. Позволяет включить или отключить сжатие данных, передаваемых между Kaspersky Endpoint Agent и компонентом KATA Central Node. По умолчанию включено.
`---tls=<yes|no>`	Необязательный параметр. Позволяет включить или 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 KATA>`	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.
`--client-password=<пароль к архиву формата PFX>`	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.
`--throttling=<yes|no>`	Позволяет включить или выключить регулирование количества запросов. Функция регулирования количества запросов позволяет ограничить поток событий низкой важности от Kaspersky Endpoint Agent к компоненту Central Node.
`--event-limit=<количество событий в час>`	Позволяет задать максимальное количество событий в час. Программа анализирует поток данных телеметрии и ограничивает передачу событий низкой важности, если поток передаваемых событий стремится превысить заданную величину.
`--exceed-limit=<величина порога>`	Позволяет задать порог превышения лимита событий. Если поток однотипных событий низкой важности превысит заданный порог в процентах от общего количества событий, то именно этот тип событий будет ограничен. Можно задать величину от 5 до 100 (без символа %).

Управление параметрами интеграции с KICS for Networks

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Описанный здесь функционал станет доступен после выпуска программы Kaspersky Industrial CyberSecurity for Nodes версии 3.0.

Чтобы управлять параметрами интеграции программы Kaspersky Endpoint Agent с программой KICS for Networks через интерфейс командной строки Kaspersky Endpoint Agent:

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=<kics> --compression=<yes|no> --tls=<yes|no> --servers=<адрес>:<порт> [--pinned-certificate=<полный путь к файлу TLS-сертификата>] [--client-certificate=<полный путь к файлу сертификата>] --client-password=<пароль к архиву формата PFX>`

Параметры команды `--message-broker` при управлении параметрами интеграции Kaspersky Endpoint Agent с программой KICS for Networks

Параметр	Описание
`--message-broker=<enable|disable|show>`	Обязательный параметр. Позволяет включить, отключить и просмотреть состояние программы Kaspersky Endpoint Agent с программой KICS for Networks. • `--message-broker=<enable>` включает интеграцию. • `--message-broker=<disable>` отключает интеграцию. • `--message-broker=<show>` отображает состояние интеграции Kaspersky Endpoint Agent с программой KICS for Networks.
`--type=<kics>`	Обязательный параметр. Позволяет указать KICS for Networks в качестве программы, с которой выполняется интеграция.
`--compression=<yes|no>`	Необязательный параметр. Позволяет включить или отключить сжатие данных, передаваемых между Kaspersky Endpoint Agent и сервером KICS for Networks. По умолчанию включено.
`---tls=<yes|no>`	Необязательный параметр. Позволяет включить или отключить использование доверенного соединения Kaspersky Endpoint Agent с программой KICS for Networks. • `--tls=<yes>` включает использование доверенного соединения. • `--tls=<no>` отключает использование доверенного соединения.
`--servers=<адрес>:<порт>`	Обязательный параметр. Позволяет указать данные сервера KICS for Networks.
`--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 KICS for Networks.
`--client-certificate=<полный путь к файлу сертификата>`	Позволяет добавить пользовательский сертификат соединения Kaspersky Endpoint Agent с сервером KICS for Networks.
`--client-password=<пароль к архиву формата PFX>`	Позволяет ввести пароль к архиву формата PFX, содержащему пользовательский сертификат соединения Kaspersky Endpoint Agent с сервером KICS for Networks.

Запуск обновления баз или модулей Kaspersky Endpoint Agent

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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]
   ```

   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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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>]
   ```

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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`
- `--selfdefense`
- `--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.

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=state`, 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В Kaspersky Endpoint Agent реализована защита служб программы 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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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 --selfdefense=<enable|disable>`

Управление фильтрацией событий

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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|accountloggon|codeinjecti
--action=<enable|disable|show>
```

Управление сетевой изоляцией

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы управлять сетевой изоляцией через интерфейс командной строки, выполните следующие действия:

Включение сетевой изоляции, а также настройка параметров сетевой изоляции недоступны через интерфейс командной строки.

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:

   - `agent.exe --isolation=show`

     Команда выводит в консоль текущие параметры сетевой изоляции на устройстве, включая список заданных сетевых профилей исключений, а также список правил, заданных в сетевых профилях.

   - `agent.exe --isolation=disable`

     Команда отключает сетевую изоляцию на устройстве.
4. Нажмите на клавишу **ENTER**.

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

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Стандартные задачи поиска IOC – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.

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] [--network=no] [--url=no] [--drives=<all|system|critical|custom>] [--excludes=<список исключений>][--scope=<настраиваемый список папок>] [--retro]`

   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.

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.
--network=no	Необязательный параметр. Параметр включает поиск угроз на основе IOC-документа Network при поиске IOC. Если параметр передан со значением <no>, Kaspersky Endpoint Agent не выполняет поиск угроз на основе IOC-документа Network. Если в IOC-файле указаны термины IOC-документа Network, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent включает поиск угроз на основе IOC-документа Network, только если IOC-документ Network описан в переданном на проверку IOC-файле.
--url=no	Необязательный параметр. Параметр включает поиск угроз на основе IOC-документа UrlHistoryItem при поиске IOC. Если параметр передан со значением <no>, Kaspersky Endpoint Agent не выполняет поиск угроз на основе IOC-документа UrlHistoryItem. Если в IOC-файле указаны термины IOC-документа UrlHistoryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent включает поиск угроз на основе IOC-документа UrlHistoryItem, только если IOC-документ UrlHistoryItem 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	Необязательный параметр.

`исключений>`	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.
`--retro`	Необязательный параметр. Параметр передается для запуска задачи в режиме **Ретроспективный поиск IOC**. Дополнительно с этим параметром можно передать временной интервал, в рамках которого программа должна выполнять ретроспективный поиск IOC при помощи параметров: • `--start-time=<дата и время начала интервала>` • `--end-time=<время окончания интервала>` Пример: `agent.exe --scan-ioc --path=<путь к папке с IOC-файлами> --retro --start-time=2021-05-21T10:30:00Z --end-time=2021-05-24T10:30:00Z` Если временной интервал не передан, то используется интервал, начинающийся за сутки от момента запуска задачи и заканчивающийся датой и временем в момент запуска задачи.

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:

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.

Управление Запретом запуска

Здесь приведена информация для Kaspersky Endpoint Agent для Windows. Эта информация может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Полную информацию о Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы управлять Запретом запуска 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 --prevention=disable`, чтобы отключить запрет запуска.
- `agent.exe --prevention=show`, чтобы вывести в командную строку текущие параметры Запрета запуска.

Коды возврата команды `--prevention`:

- -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 Запрет запуска, если Запрет запуска уже отключен).

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

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

Kaspersky предоставляет поддержку программного решения, в состав которого входит Kaspersky Endpoint Agent, в течение жизненного цикла (см. страницу жизненного цикла программ). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки, отправив запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. 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.

Глоссарий

End User License Agreement

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

Endpoint Protection Platform (EPP)

Интегрированная система комплексной защиты конечных устройств (например, мобильных устройств, компьютеров или ноутбуков) с помощью различных технологий безопасности. Пример Endpoint Protection Platform – программа Kaspersky Endpoint Security для бизнеса.

EPP-программа

Программа, входящая в состав системы защиты конечных устройств (англ. Endpoint Protection Platform, EPP). EPP-программы устанавливаются на конечные устройства внутри IT-инфраструктуры организации (например, мобильные устройства, компьютеры или ноутбуки). Примером EPP-программы является Kaspersky Endpoint Security для Windows в составе EPP-решения Kaspersky Endpoint Security для бизнеса.

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.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent - программа, которая устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации. Программа осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами. Kaspersky Endpoint Agent взаимодействует с другими решениями "Лаборатории Касперского" для обнаружения комплексных угроз (таких как таргетированные атаки).

OpenIOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

Сервер сбора телеметрии

Тип сервера, с которым Kaspersky Endpoint Agent поддерживает интеграцию. В рамках интеграции Kaspersky Endpoint Agent отправляет *телеметрию* на сервер, получает задачи от сервера, а также готовит отчеты о выполнении этих задач.

Телеметрия

Данные, которые Kaspersky Endpoint Agent анализирует на защищаемом устройстве и отправляет на *Сервер сбора телеметрии*. Телеметрия представляет собой список событий, которые произошли на защищаемом устройстве.

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

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.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

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.

Microsoft, Active Directory, Excel, Word, PowerPoint, PowerShell, Hyper-V, Win32, Windows, Windows Vista и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Adobe Acrobat – товарный знак или зарегистрированный в Соединенных Штатах Америки и/или в других странах товарный знак Adobe Systems Incorporated.

Java – зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.

McAfee – товарный знак или зарегистрированный в США и других странах товарный знак McAfee, Inc.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

ESET и ESET NOD32 – товарные знаки или зарегистрированные товарные знаки ESET, spol. s r.o.

Trend Micro – товарный знак компании Trend Micro.