KASPERSKY lab

Kaspersky Anti Targeted Attack Platform

Руководство администратора

Версия программы: 3.6

Уважаемый пользователь!

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

Дата редакции документа: 23.05.2019

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

Содержание

Условные обозначения

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

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: ...	Примеры приведены в блоках на голубом фоне под заголовком "Пример".
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком "стрелка".
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

Kaspersky Anti Targeted Attack Platform

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

  KEDR лицензируется отдельно от KATA. Для активации этой функциональности вам нужно использовать отдельный ключ. Вы можете приобрести KEDR вместе с KATA или отдельно от нее.

Программа может получать и обрабатывать данные следующими способами:

- Интегрироваться в локальную сеть, получать и обрабатывать *зеркалированный SPAN-, ERSPAN- и RSPAN-трафик* и извлекать объекты и метаинформацию HTTP-, FTP-, SMTP- и DNS-протоколов.
- Подключаться к прокси-серверу по протоколу ICAP, получать и обрабатывать данные HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- Подключаться к почтовому серверу по протоколам POP3(S) и SMTP, получать и обрабатывать копии сообщений электронной почты.
- Интегрироваться с программами "Лаборатории Касперского" Kaspersky Secure Mail Gateway и Kaspersky Security для Linux® Mail Server, получать и обрабатывать копии сообщений электронной почты.

  Вы можете получить подробную информацию о Kaspersky Secure Mail Gateway и Kaspersky Security для Linux Mail Server из документации к этим программам.
- Интегрироваться с внешними системами с помощью интерфейса REST API и проверять файлы на этих системах.
- Получать данные с отдельных компьютеров, входящих в IT-инфраструктуру организации и работающих под управлением операционной системы Microsoft® Windows®, осуществлять постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.
  - Компонент Kaspersky Anti Targeted Attack Platform Endpoint Sensors может устанавливаться на отдельные компьютеры и получать данные с этих компьютеров.
  - Kaspersky Anti Targeted Attack Platform может интегрироваться с программой "Лаборатории Касперского" Kaspersky Endpoint Security для Windows (далее также "KES").

    Вы можете получить подробную информацию о Kaspersky Endpoint Security для Windows из *Справки Kaspersky Endpoint Security*.

Программа использует следующие средства анализа угроз (Threat Intelligence):

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

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

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

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

- Осуществлять мониторинг работы программы.
- Просматривать таблицу обнаруженных признаков целевых атак и вторжений в IT-инфраструктуру организации, осуществлять фильтрацию и поиск обнаружений, просмотр и работу с каждым обнаружением.
- Просматривать таблицу событий, происходящих на компьютерах и серверах, входящих в IT-инфраструктуру организации, осуществлять поиск угроз, фильтрацию, просмотр и работу с каждым событием.
- Выполнять задачи на хостах с компонентом Endpoint Sensors: запускать программы и останавливать процессы, скачивать и удалять файлы, помещать объекты и их копии в Хранилище и Карантин, а также восстанавливать их из Карантина.
- Настраивать политики запрета запуска файлов и процессов, которые они считают небезопасными, на выбранных хостах с компонентом Endpoint Sensors.
- Изолировать отдельные хосты с компонентом Endpoint Sensors от сети.
- Работать с объектами и их копиями в Хранилище и Карантине.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах с компонентом Endpoint Sensors и в базе обнаружений.
- Работать с индикаторами атак (IOA) для классификации и анализа событий.
- Управлять отчетами о работе программы и отчетами об обнаружениях.

- Настраивать отправку уведомлений об обнаружениях и о проблемах в работе программы на адреса электронной почты пользователей.
- Работать со списком обнаружений со статусом VIP, с белым списком данных, наполнять локальную репутационную базу KPSN.

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

- Настраивать параметры работы программы.
- Настраивать серверы для работы в режиме распределенного решения и multitenancy.
- Производить интеграцию программы с другими программами и системами.
- Управлять учетными записями пользователей программы.
- Осуществлять мониторинг работоспособности программы.

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

- На компьютер локальной сети организации был загружен файл или была предпринята попытка загрузки файла.
- На адрес электронной почты пользователя локальной сети организации был отправлен файл.
- На компьютере локальной сети организации была открыта ссылка на веб-сайт.
- IP-адрес или доменное имя компьютера локальной сети организации были замечены в сетевой активности.
- На компьютере локальной сети организации были запущены процессы.

Kaspersky Anti Targeted Attack Platform оценивает события и рекомендует пользователю обратить внимание на каждое обнаруженное событие (*обнаружение*) в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
Пользователь Kaspersky Anti Targeted Attack Platform самостоятельно принимает решение о дальнейших действиях над обнаружениями.

Что нового

В Kaspersky Anti Targeted Attack Platform появились следующие изменения:

- Реализован режим multitenancy (мультиарендность), при котором Kaspersky Anti Targeted Attack Platform устанавливается в режиме распределенного решения и может использоваться для защиты инфраструктуры нескольких организаций. Поддерживается возможность использования одного или нескольких серверов Central Node для одной организации. Каждая организация может работать с программой независимо от других организаций. Организация-провайдер может работать с данными нескольких организаций.
- Усовершенствована технология Targeted Attack Analyzer: добавлена классификация и автоматический анализ соответствия событий и обнаружений индикаторам атак (далее также "IOA") и матрице MITRE ATT&CK. База IOA-правил сформирована специалистами "Лаборатории Касперского" и постоянно пополняется. Новые события, по которым сработали IOA-правила, помечаются в интерфейсе программы. IOA-правила содержат описание признаков атак, примеры и рекомендации

по противодействию, ссылки на информацию о каждом признаке атаки в базе знаний MITRE ATT&CK..

- Добавлена классификация обнаружений компонентом Sandbox в соответствии с матрицей MITRE ATT&CK. Компонент Sandbox сопоставляет обнаруженные подозрительные активности с фазами атаки, техниками и методами злоумышленников в матрице MITRE ATT&CK.
- Добавлена возможность создания пользовательской базы индикаторов атак (IOA) для классификации и анализа событий.
- Добавлена схема развертывания программы, по которой несколько серверов Central Node могут подключаться к одним и тем же серверам Sandbox.
- Добавлена поддержка чувствительности к регистру символов при поиске, изменении и удалении файлов, каталогов и других объектов в соответствие со стандартами файловой системы NTFS.
- Реализован новый метод анализа APK-файлов операционной системы Android™ современной облачной технологией на базе машинного обучения.
- Добавлен мониторинг новых ключей реестра: анализ данных об изменении веток реестра из разделов HKEY_USERS/HKEY_CURRENT_USER.
- Расширены возможности по подбору паролей к документам Microsoft Office и сообщениям электронной почты. Реализована возможность подбора паролей к вложениям в сообщения электронной почты следующих форматов: ArchiveRAR (RAR v5) и Archive7z (7z). Также добавлена возможность подбора паролей к документам формата PDF, документам Word, Excel® и PowerPoint®. Подбор паролей осуществляется из существующей базы паролей или путем анализа данных в теле сообщения электронной почты.
- Добавлена передача новых типов событий Windows (Windows events logging) со следующими идентификаторами:
  - EventId 4776 – компьютер пытался проверить данные учетной записи.
  - EventId 4648 – попытка входа в систему с использованием учетных данных.
  - EventId 4768 – был запрошен билет проверки подлинности Kerberos (TGT).
  - EventId 4769 – был запрошен билет службы Kerberos.

  Обновление позволяет обнаруживать следующие атаки, использующие эти события Windows:
  - Pass-the-hash (4776, 4624).
  - Keberoast (4769).
  - Mimikatz (4624, 4648, 4768).
- Добавлена поддержка API для передачи информации об обнаружениях Kaspersky Anti Targeted Attack Platform в сторонние решения по запросу от сторонних решений. Передаваемая информация об обнаружении может также содержать дополнительные сведения, например, о сработавших технологиях, типах объектов, важности обнаружения.
- Оптимизирована производительность программы. На 30% снижены требования к аппаратному обеспечению серверов Central Node и Sandbox.

О Kaspersky Threat Intelligence Portal

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

этого файла.

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

Комплект поставки

В комплект поставки программы входят следующие файлы:

1. Образ диска (файл с расширением iso) с установочными файлами операционной системы CentOS 7.4 и компонентов Sensor, Central Node.
2. Образ диска (файл с расширением iso) с установочными файлами операционной системы CentOS 6.9 и компонента Sandbox.
3. Образы дисков (файлы с расширением iso) операционных систем Windows XP SP3, 64-разрядной Windows 7 и Windows 10, в которых компонент Sandbox будет запускать файлы.
4. Установочный файл компонента Endpoint Sensors (файл с расширением msi).
5. Лицензионное соглашение.
6. Политика конфиденциальности.
7. Положение о KSN.
8. Файл с информацией о стороннем коде, используемом в Kaspersky Anti Targeted Attack Platform.

Аппаратные и программные требования

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

- Google Chrome™ для Windows версии 74 или выше.
- Google Chrome для Linux версии 74 или выше.
- Mozilla™ Firefox™ версии 66 или выше.
- Microsoft Edge версии 44 или выше.
- Safari версии 12.0 или выше.

Для развертывания программы на виртуальной платформе должен быть установлен гипервизор VMware ESXi™ версии 5.5.0 или 6.7.0.

Требования к компоненту Endpoint Sensors

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

Если на серверах Central Node установлена программа Kaspersky Anti Targeted Attack Platform версии 3.5, а на компьютерах локальной сети вашей организации установлен компонент Endpoint Sensors версии 3.0, возможны следующие ограничения в работе программы: IOC-проверка файлов на компьютерах с Endpoint Sensors версии 3.0, а также работа с задачами и политиками, созданными на компьютерах с Endpoint Sensors версии 3.0, могут быть недоступны с серверов Central Node.

Программные требования к компьютерам для установки компонента Endpoint Sensors

Одна из следующих операционных систем:

- Windows 7 SP1 Enterprise x86 x64.
- Windows 8.1.1 Enterprise x86 x64.
- Windows 10 RS3 Enterprise x86 x64.
- Windows 10 RS4 Enterprise x86 x64.
- Windows 10 RS5 Enterprise x86 x64.
- Windows 10 RS6 Enterprise x86 x64.
- Windows Server® 2008 R2 Enterprise x64.
- Windows Server 2012 Standard x64.
- Windows Server 2012 R2 Standard x64.
- Windows Server 2016 Standard x64.

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

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

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

Аппаратные требования к компьютерам для установки компонента Endpoint Sensors

Минимальная конфигурация:

- Процессор: 2 ГГц и выше с поддержкой инструкций SSE2.
- Объем оперативной памяти: 2 ГБ.
- Дисковая подсистема: 2 ГБ свободного пространства.
- Один сетевой адаптер со скоростью передачи данных 1 Гбит/с.

Рекомендуемая конфигурация:

- Процессор Intel® Core™ i3 Duo 3.10GHz или эквивалентный (с поддержкой SSE2).
- Объем оперативной памяти: 40 МБ.
- Дисковая подсистема: 100 МБ свободного пространства.

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

Совместимость компонента Endpoint Sensors с другими программами

Совместная работа Kaspersky Anti Targeted Attack Platform с программами, не указанными в этом разделе, не предусмотрена.

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

Вы можете использовать Kaspersky Endpoint Security для Windows версии 10 SP2 MR3 или 11.0 и отдельный компонент Endpoint Sensors версии 3.5 на одном компьютере. Для этого выполните следующие действия:

1. Отключите компонент Endpoint Sensors в составе программы KES.

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

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

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

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

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

Таблица 2. Совместимость компонента Endpoint Sensors и программы KES

Версия программы "Лаборатории Касперского"	Режим совместимости	Установка отдельного компонента Endpoint Sensors после установки другой программы	Установка другой программы после установки отдельного компонента Endpoint Sensors	Поддерживаемые операционные системы
• KES10 SP1 MR3 • KES10 SP1 MR4	Совместная работа.	Стандартная процедура установки.	Стандартная процедура установки.	• Windows 7 SP1 Enterprise x86 x64. • Windows 8.1.1 Enterprise x86 x64. • Windows 10 RS3 Enterprise x86 x64. • Windows 10 RS4 Enterprise x86 x64. • Windows 10 RS5 Enterprise x86 x64. • Windows 10 RS6 Enterprise x86 x64. • Windows Server 2008 R2 Enterprise x64. • Windows Server 2012 Standard x64. • Windows Server 2012 R2 Standard
• KES 10 SP2 • KES 10 SP2 MR1 • KES 10 SP2 MR2 • KES 10 SP2 MR3	Совместная работа. Поддерживается отправка информации об обнаружениях (стр. 277) KES.	Стандартная процедура установки.	Стандартная процедура установки.	
• KES 11.0.0 • KES 11.0.1 • KES 11.1	Возможны следующие сценарии: • Совместная работа KES и отдельного компонента Endpoint Sensors. • Использование встроенного компонента Endpoint Sensors в составе KES.	Для установки отдельного компонента Endpoint Sensors требуется отключить компонент Endpoint Sensors в составе программы KES. Подробнее о том, как отключить компонент Endpoint Sensors в составе программы KES см. в *Справке Kaspersky Endpoint Security* https://help.kaspersky.com/KESWin/11.1.1/ru-RU/132664.htm. Если компонент не отключен, установка прерывается с ошибкой.	Стандартная процедура установки.	

Версия программы "Лаборатории Касперского"	Режим совместимости	Установка отдельного компонента Endpoint Sensors после установки другой программы	Установка другой программы после установки отдельного компонента Endpoint Sensors	Поддерживаемые операционные системы
KES 11.1.1	Доступно только использование компонента Endpoint Sensors в составе KES. Совместная работа отдельного компонента Endpoint Sensors и KES не поддерживается.	Установка прерывается с ошибкой. Вы можете включить использование встроенного компонента Endpoint Sensors https://help.kaspersky.com/KESWin/11.1.1/ru-RU/132664.htm в составе программы KES.	KES удаляет отдельный компонент Endpoint Sensors.	x64. • Windows Server 2016 Standard x64.

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

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

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

Для работы программы KSV в виртуальной инфраструктуре должен быть установлен один из следующих гипервизоров в зависимости от платформы виртуализации:

- Платформа Microsoft Hyper-V®:
  - Гипервизор Microsoft Windows Server 2016 Hyper-V (в полном режиме или в режиме Server Core) со всеми доступными обновлениями.
  - Гипервизор Microsoft Windows Server 2012 R2 Hyper-V (в полном режиме или в режиме Server Core) со всеми доступными обновлениями.
- Платформа Citrix Hypervisor: гипервизор Citrix XenServer 7.1 LTSR.
- Платформа VMware vSphere™:
  - Гипервизор VMware ESXi 6.7.
  - Гипервизор VMware ESXi 6.5.
  - Гипервизор VMware ESXi 6.0 с последними обновлениями.
- Платформа KVM (Kernel-based Virtual Machine): гипервизор KVM на базе одной из следующих

операционных систем:

- Ubuntu Server 18.04 LTS.
- Ubuntu Server 16.04 LTS.
- Red Hat Enterprise Linux® Server 7.5.
- CentOS 7.5.

- Платформа Proxmox VE: гипервизор Proxmox VE 5.2.
- Платформа Скала-Р: гипервизор Р-Виртуализация 7.0.6.
- Платформа HUAWEI FusionSphere: гипервизор HUAWEI FusionCompute CNA 6.3.1.

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

Совместимость компонента Endpoint Sensors с антивирусными программами других производителей

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

- Symantec™ Endpoint Protection.
- Trend Micro™ Maximum Security.
- Sophos Endpoint Protection.
- ESET NOD32 Business Edition Smart Security.
- BitDefender GravityZone Advanced Business Security.

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

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

Требования к компоненту Central Node

Аппаратные требования к серверу для установки компонента Central Node

Конфигурация сервера с компонентом Central Node зависит от объема данных, обрабатываемых программой и от пропускной способности канала связи.

Минимальные аппаратные требования к серверу (пропускная способность канала связи 50 Мбит/сек.; 1000 компьютеров с компонентом Endpoint Sensors):

- Процессор: 12 ядер (24 потока), 2.7 ГГц.
- Объем оперативной памяти: 128 ГБ.
- Дисковая подсистема – два раздела: 2 ТБ свободного пространства для системного раздела и 4 ТБ

свободного пространства для хранения данных компонента Targeted Attack Analyzer.

Рекомендуется использовать дисковый массив уровня RAID 0, 5, 10 или SSD-диск.

- Два сетевых адаптера со скоростью передачи данных по 1 Гбит/сек. каждый.

Требования к компоненту Sensor

Аппаратные требования к серверу для установки компонента Sensor

Конфигурация сервера с компонентом Sensor зависит от объема данных, обрабатываемых программой, а также от пропускной способности канала связи.

Минимальные аппаратные требования к серверу (пропускная способность канала связи 50 Мбит/сек.; компонент обрабатывает зеркалированный трафик и сообщения электронной почты; скорость обработки составляет 120 сообщений в секунду):

- Процессор: 16 ядер, 2.7 ГГц.
- Объем оперативной памяти: 32 ГБ.
- Дисковая подсистема: 500 ГБ свободного пространства.
- Два сетевых адаптера со скоростью передачи данных по 1 Гбит/сек. каждый.

Требования к компоненту Sandbox

Аппаратные требования к серверу для установки компонента Sandbox

Конфигурация сервера с компонентом Sandbox зависит от объема данных, обрабатываемых программой, от количества одновременно запускаемых виртуальных машин с образами операционных систем, а также от пропускной способности канала связи.

Минимальные аппаратные требования к серверу (пропускная способность канала связи 50 Мбит/сек.; 12 одновременно запускаемых виртуальных машин; 3500 файлов, обрабатываемых за одни сутки):

- Процессор Intel с поддержкой VT-x и EPT, 8 ядер, 2.7 ГГц.

  Процессоры AMD™ не поддерживаются.

- Объем оперативной памяти: 32 ГБ.
- Дисковая подсистема: 300 ГБ свободного пространства.
- Два сетевых адаптера со скоростью передачи данных по 1 Гбит/сек. каждый.

Рассчитывайте количество одновременно запускаемых виртуальных машин с образами операционных систем следующим образом: количество ядер процессора нужно умножить на 1,5. Для каждой виртуальной машины необходимо выделить по 1 ГБ оперативной памяти.

Типовые схемы развертывания и установки компонентов программы

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

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

Вы можете установить один или несколько компонентов Central Node. При установке нескольких компонентов Central Node вы можете использовать их независимо друг от друга или объединить для централизованного управления в режиме распределенного решения (стр. 42).

Выбор схемы развертывания зависит от используемой функциональности программы (стр. 91). Все приведенные в данном руководстве схемы применимы также для развертывания программы на виртуальной платформе.

Полная функциональность (KATA и KEDR)

При использовании функциональности KATA и KEDR вы можете проверять сетевой и почтовый трафик, а также данные на компьютерах локальной сети организации.

Если в организации установлено более 5000 компонентов Endpoint Sensors, не рекомендуется использовать компонент Central Node для обработки трафика.

Вы можете использовать компонент Sensor в качестве прокси-сервера для соединения компонентов Endpoint Sensors и Central Node. Один компонент Sensor поддерживает подключение до 1000 компонентов Endpoint Sensors.

Критерии выбора схемы развертывания при использовании функциональности KATA и KEDR представлены в таблице ниже. Алгоритм выбора следующий:

1. В каждой строке таблицы выберите ячейку со значением критерия, соответствующим вашей IT-инфраструктуре.

   Если в строке две ячейки с одинаковым значением, необходимо выбрать левую ячейку.

2. Выберите самую правую колонку, в которой есть отмеченные ячейки.

Таблица 3. Выбор схемы развертывания при использовании функциональности KATA и KEDR

Критерий	Схема на два сервера (стр. 31)	Схема на три сервера (стр. 32)	Схема на четыре и более серверов (стр. 33)	Распределенное решение (стр. 42)
Сетевой и почтовый трафик не может быть принят на одном устройстве	Нет	Да	Да	Да
Количество компонентов Endpoint Sensors	Нет	От 5000 до 10000	От 5000 до 10000	Более 10000
Пропускная способность канала связи	1 Гбит/с	От 1 до 2 Гбит/с	Более 2 Гбит/с	Более 2 Гбит/с
Количество удаленных инфраструктур, в которых требуется анализировать трафик	Нет	Одна	Две и более	Две и более
Мощности одного компонента Sandbox недостаточно для анализа всех объектов в приемлемые сроки	Нет	Нет	Да	Да

В режиме распределенного решения каждый из компонентов программы должен отвечать аппаратным требованиям, указанным в калькуляторе масштабирования (стр. **Error! Bookmark not defined.**).

Обработка сетевого, почтового и веб-трафика (KATA)

Функциональность KATA рекомендуется использовать, если в организации нет необходимости обрабатывать данные на компьютерах локальной сети организации. В этом случае обрабатывается только сетевой и почтовый трафик.

Критерии выбора схемы развертывания при использовании функциональности KATA представлены в таблице ниже. Алгоритм выбора следующий:

1. В каждой строке таблицы выберите ячейку со значением критерия, соответствующим вашей IT-инфраструктуре.

Если в строке две ячейки с одинаковым значением, необходимо выбрать левую ячейку.

2. Выберите самую правую колонку, в которой есть отмеченные ячейки.

Таблица 4. Выбор схемы развертывания при использовании функциональности KATA

Критерий	Схема на два сервера (стр. 31)	Схема на три сервера (стр. 32)	Схема на четыре и более серверов (стр. 33)
Сетевой и почтовый трафик не может быть принят на одном устройстве	Нет	Да	Да
Пропускная способность канала связи	1 Гбит/с	От 1 до 2 Гбит/с	Более 2 Гбит/с
Количество удаленных инфраструктур, в которых требуется анализировать трафик	Нет	Одна	Две и более
Мощности одного компонента Sandbox недостаточно для анализа всех объектов в приемлемые сроки	Нет	Нет	Да

Обработка данных с компьютеров локальной сети организации (KEDR)

Функциональность KEDR рекомендуется использовать, если в организации нет необходимости обрабатывать трафик. В этом случае обрабатываются только данные на компьютерах локальной сети организации.

В зависимости от наличия в организации стороннего решения Sandbox вы можете использовать одну из следующих схем развертывания:

- схема без компонента Sandbox (стр. 34);
- схема с компонентом Sandbox (стр. 35).

Схема развертывания на два сервера

При использовании функциональности KATA и KEDR вы можете установить компоненты Endpoint Sensors на компьютерах локальной сети организации. При использовании функциональности KATA компоненты Endpoint Sensors не устанавливаются.

При использовании этой схемы развертывания компоненты, необходимые для использования функциональности KATA, устанавливаются на двух серверах.

На одном сервере устанавливаются компоненты Sensor и Central Node. Этот сервер принимает трафик, выполняет первичный анализ трафика и более глубокий анализ извлеченных файлов. По результатам

проверки компоненты выявляют признаки целевых атак на IT-инфраструктуру организации.

На другом сервере устанавливается компонент Sandbox.

Схема работы программы при развертывании на два сервера представлена на рис. ниже.

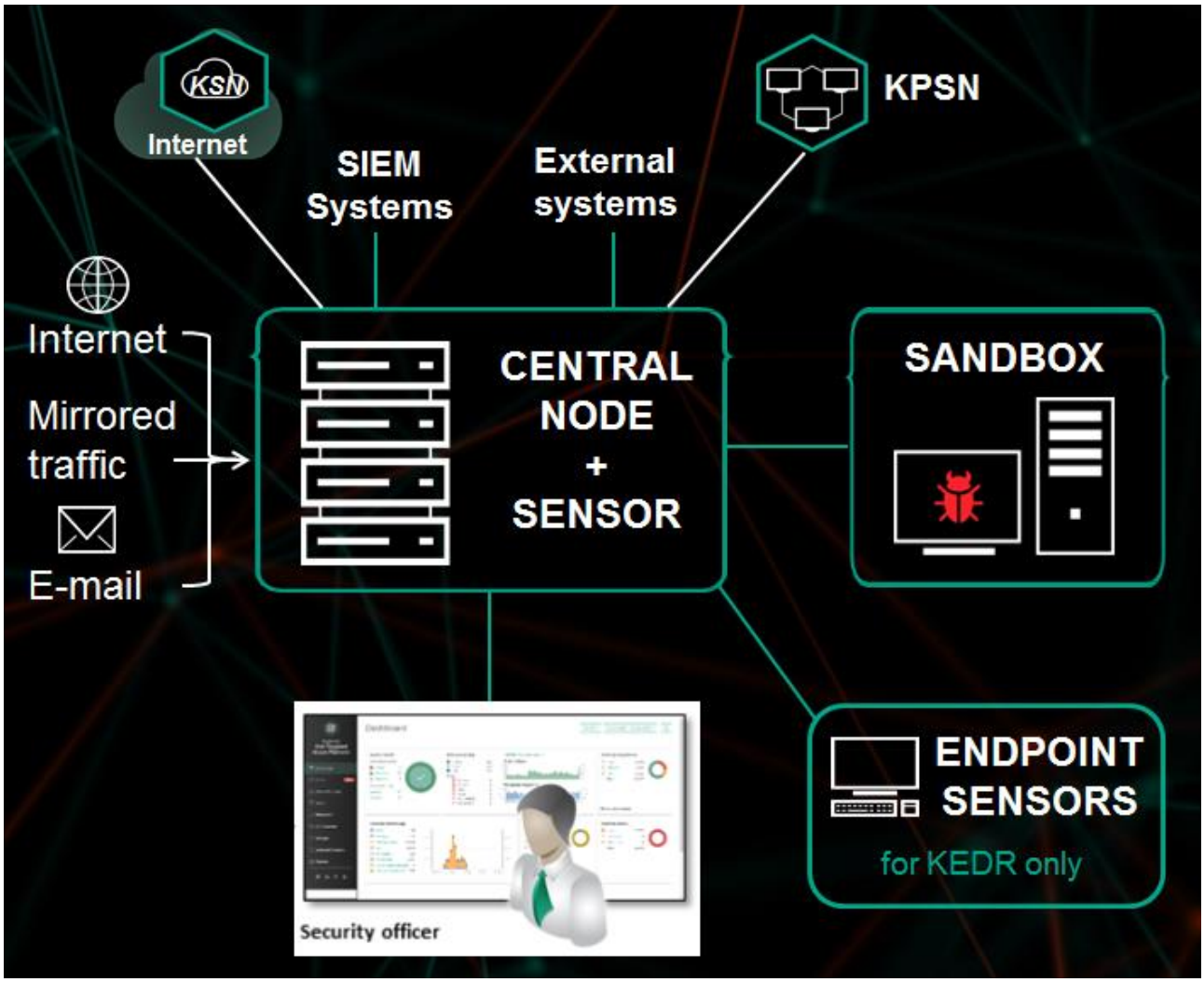


Схема 1: Схема работы программы при развертывании на два сервера

Схема развертывания на три сервера

При использовании функциональности KATA и KEDR вы можете установить компоненты Endpoint Sensors на компьютерах локальной сети организации. При использовании функциональности KATA компоненты Endpoint Sensors не устанавливаются.

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

При использовании этой схемы развертывания компоненты Sensor, Central Node и Sandbox устанавливаются на отдельных серверах. Сервер с компонентом Sensor принимает трафик, выполняет первичный анализ, извлекает файлы и пересылает их на сервер с компонентом Central Node для более глубокого анализа.

При такой схеме развертывания компонент Central Node может принимать трафик и выполнять первичный анализ данных в основной инфраструктуре. В этом случае вы можете установить компонент Sensor на сервере удаленной инфраструктуры, трафик которой требуется анализировать. Если пропускная способность канала в основной инфраструктуре составляет более 2 Гбит/с, то сервер с компонентом Sensor рекомендуется устанавливать в основной инфраструктуре.

Трафик между компонентами Central Node и Sensor составляет до 20% трафика, получаемого компонентом Sensor.

Схема работы программы при развертывании на три сервера представлена на рис. ниже.

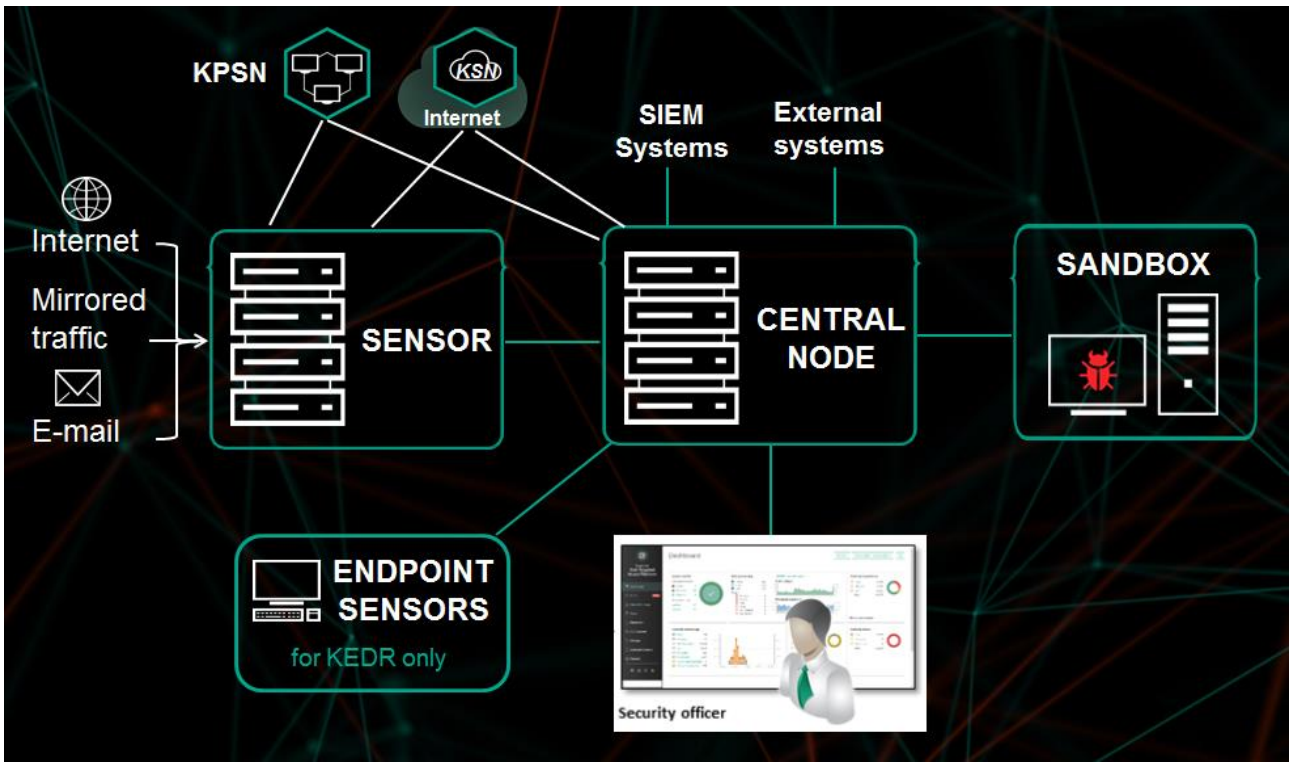


Схема 2: Схема работы программы при развертывании на три сервера

Схема развертывания на четыре и более сервера

При использовании функциональности KATA и KEDR вы можете установить компоненты Endpoint Sensors на компьютерах локальной сети организации. При использовании функциональности KATA компоненты Endpoint Sensors не устанавливаются.

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

При большом объеме трафика вы можете установить несколько компонентов Sensor или несколько компонентов Sandbox на разных серверах. Эта схема рекомендуется для развертывания в крупных организациях.

Вы также можете использовать один компонент Sandbox для подключения к нескольким компонентам Central Node.

Схемы работы программы при развертывании на четыре и более сервера представлены на рис. ниже.

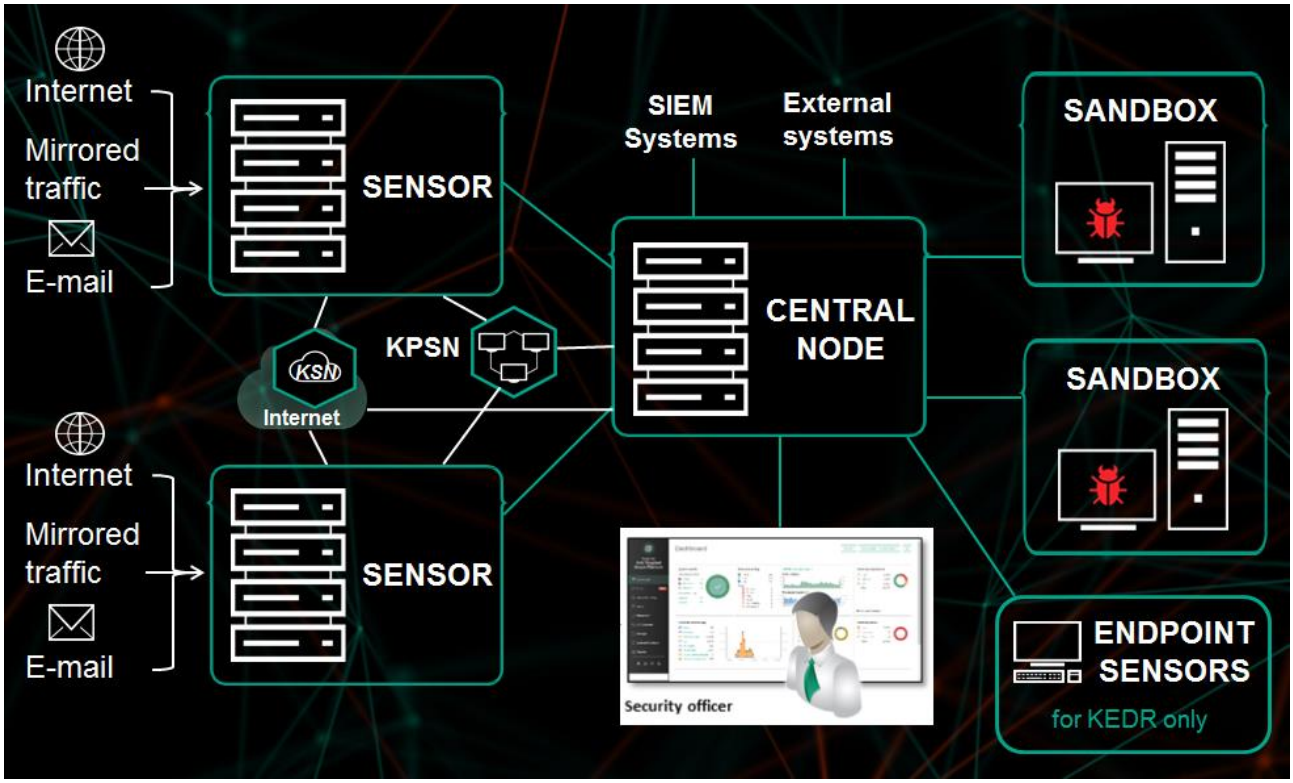


Схема 3: Схема работы программы при развертывании на четыре и более сервера

Схема развертывания функциональности KEDR без компонента Sandbox

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

При такой схеме развертывания компонент Central Node необходим для управления компонентами Endpoint Sensors и анализа данных.

Схема работы программы при развертывании функциональности KEDR без компонента Sandbox представлена на рис. ниже.

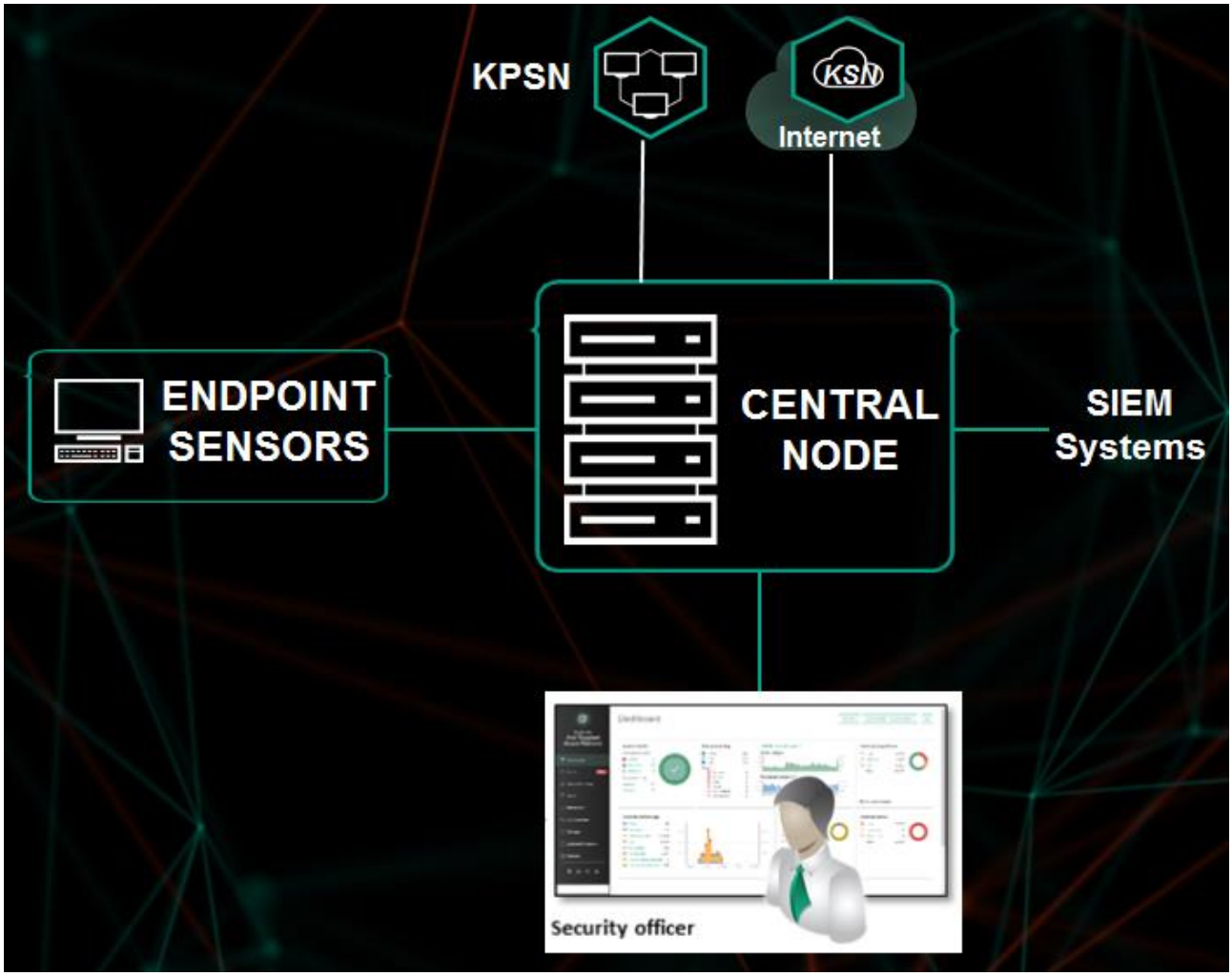


Схема 4: Схема работы программы при развертывании функциональности KEDR без компонента Sandbox

Схема развертывания функциональности KEDR с компонентом Sandbox

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

При такой схеме развертывания компонент Central Node необходим для управления компонентами Endpoint Sensors и анализа данных.

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

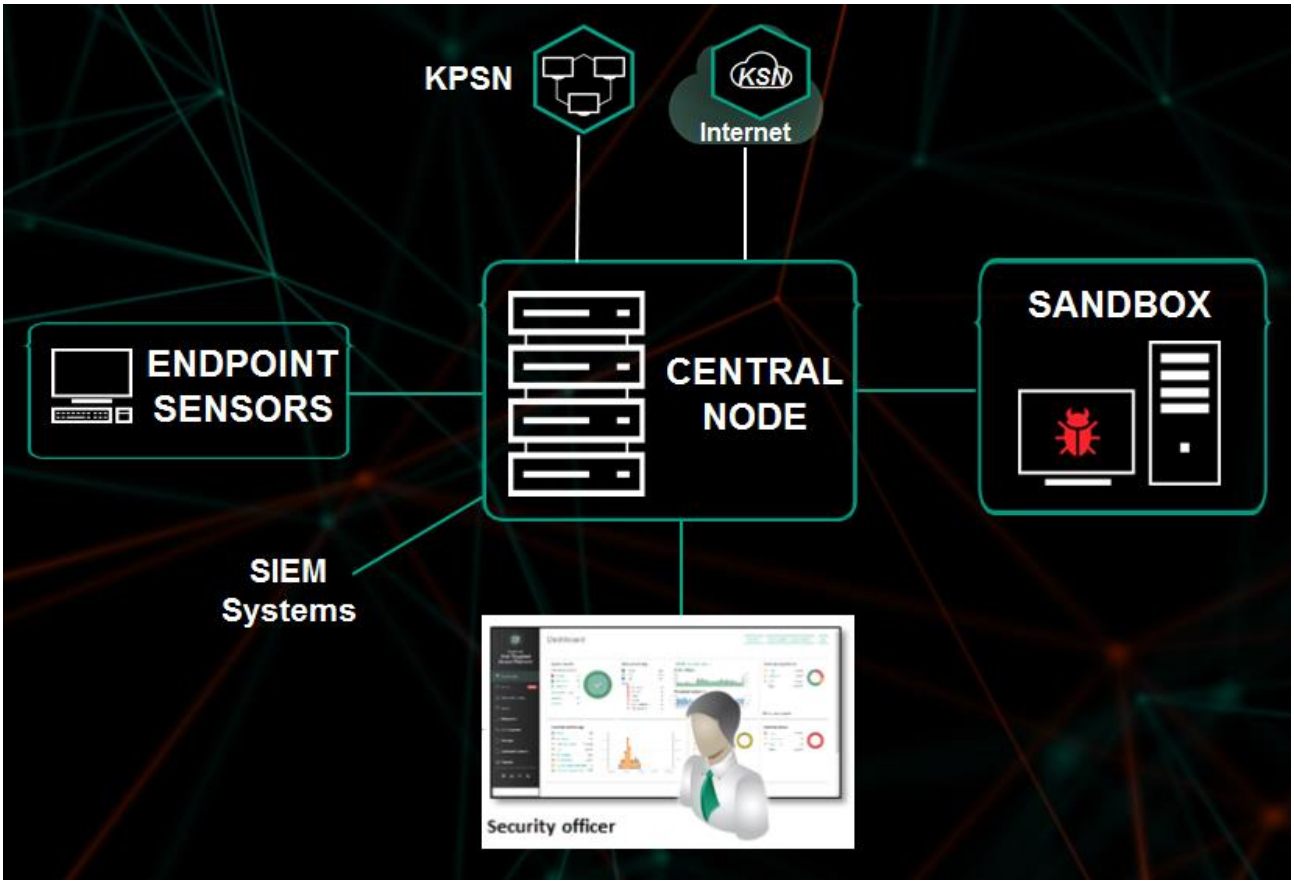


Схема 5: Схема работы программы при развертывании функциональности KEDR с компонентом Sandbox

Архитектура программы

В состав программы входят следующие основные компоненты:

- *Sensor.* Выполняет прием данных.
- *Central Node*. Выполняет проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс программы.
- *Sandbox*. Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации.
- *Endpoint Sensors.* Устанавливается на отдельные компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

Компонент Sensor

На каждом сервере с компонентом Sensor работают следующие модули Kaspersky Anti Targeted Attack Platform:

- *Sensor.* Выполняет прием данных из сетевого и почтового трафика и передает их на обработку на сервер с компонентом Central Node.
- *Intrusion Detection System* (далее также *IDS*). Выполняет проверку интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации.
- *KSN.* Выполняет для Kaspersky Anti Targeted Attack Platform проверку репутации файлов и URL-адресов в базе знаний Kaspersky Security Network и предоставляет сведения о категориях веб-сайтов (например, вредоносный веб-сайт, фишинговый веб-сайт).

  *Kaspersky Security Network (*далее также *KSN)* – инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

  Если вы не хотите участвовать в KSN, вы можете использовать *Kaspersky Private Security Network* (далее также *KPSN*) – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.
- *URL Reputation.* Обнаруживает вредоносные, фишинговые URL-адреса и URL-адреса, которые ранее использовались злоумышленниками для целевых атак и вторжений в IT-инфраструктуру организаций.

В качестве компонента Sensor также может использоваться почтовый сенсор (стр. 214) – сервер или виртуальная машина, на которой установлена программа "Лаборатории Касперского" Kaspersky Secure Mail Gateway (далее также "KSMG") или Kaspersky Security для Linux Mail Server (далее также "KLMS"). Эти программы отправляют сообщения электронной почты на обработку в Kaspersky Anti Targeted Attack Platform. По результатам обработки сообщений электронной почты в Kaspersky Anti Targeted Attack Platform KSMG и KLMS могут блокировать пересылку сообщений.

Если в качестве компонента Sensor используется программа KSMG или KLMS, то белые списки, настроенные по получателям сообщений и MD5-суммам файлов, не передаются в KSMG и KLMS и не применяются при обработке сообщений программами KSMG и KLMS.

Компонент Central Node

На каждом сервере с компонентом Central Node работают следующие модули, ядра и технологии Kaspersky Anti Targeted Attack Platform:

- *Anti-Malware Engine* (далее также *AM* и *AM Engine*). Выполняет проверку файлов и объектов на вирусы и другие программы, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.
- *Mobile Attack Analyzer* (далее также *MAA*). Выполняет проверку исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения. В результате проверки Kaspersky Anti Targeted Attack Platform получает информацию об обнаруженных угрозах или их отсутствии.
- *YARA*. Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями Kaspersky Anti Targeted Attack Platform.
- *Targeted Attack Analyzer* (далее также *TAA*, *TA Analyzer*). Выполняет статистический анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации. Выполняет поиск признаков сетевой активности, на которую пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание, а также признаков целевых атак на IT-инфраструктуру организации.
- *KSN*. Выполняет для Kaspersky Anti Targeted Attack Platform проверку репутации файлов и URL-адресов в базе знаний Kaspersky Security Network и предоставляет сведения о категориях веб-сайтов (например, вредоносный веб-сайт, фишинговый веб-сайт).

Компонент Sandbox

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

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

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

По умолчанию максимальный размер проверяемого файла составляет 100 Мб. Вы можете настроить параметры проверки в меню администратора консоли управления программой.
Максимальный уровень вложенности проверяемых архивов составляет 32.

Максимальное количество объектов, которое может находиться в очереди на проверку компонентом Sandbox за одни сутки, составляет 10 тысяч объектов. По достижении этого ограничения программа удаляет 10% объектов, поступивших на проверку раньше остальных, и заменяет их новыми объектами, поступившими на проверку. Удаленные объекты сохраняются в программе со статусом NOT_SCANNED (непроверенные).

Компонент Endpoint Sensors

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

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

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

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

Кроме того, Kaspersky Anti Targeted Attack Platform позволяет интегрироваться с программой Kaspersky Security Center и получать статистику работы компонента Endpoint Sensors.

Принцип работы программы

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

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

Принцип работы программы показан на рис. ниже.

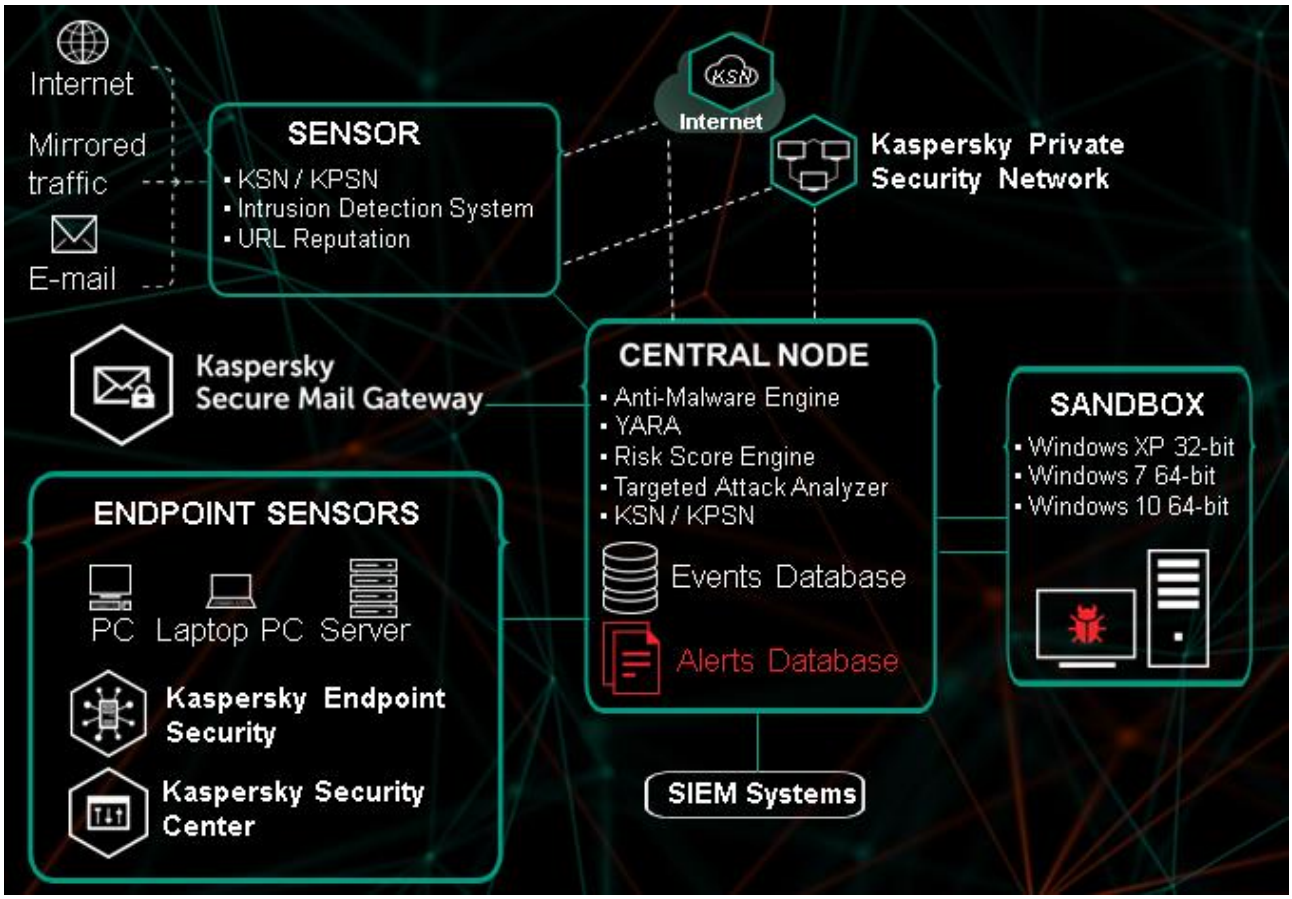


Схема 6: Принцип работы программы в режиме автономного решения

Распределенное решение (стр. 42) представляет собой двухуровневую иерархию серверов Central Node. В этой структуре выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*.

Принцип работы программы в режиме распределенного решения показан на рис. ниже.

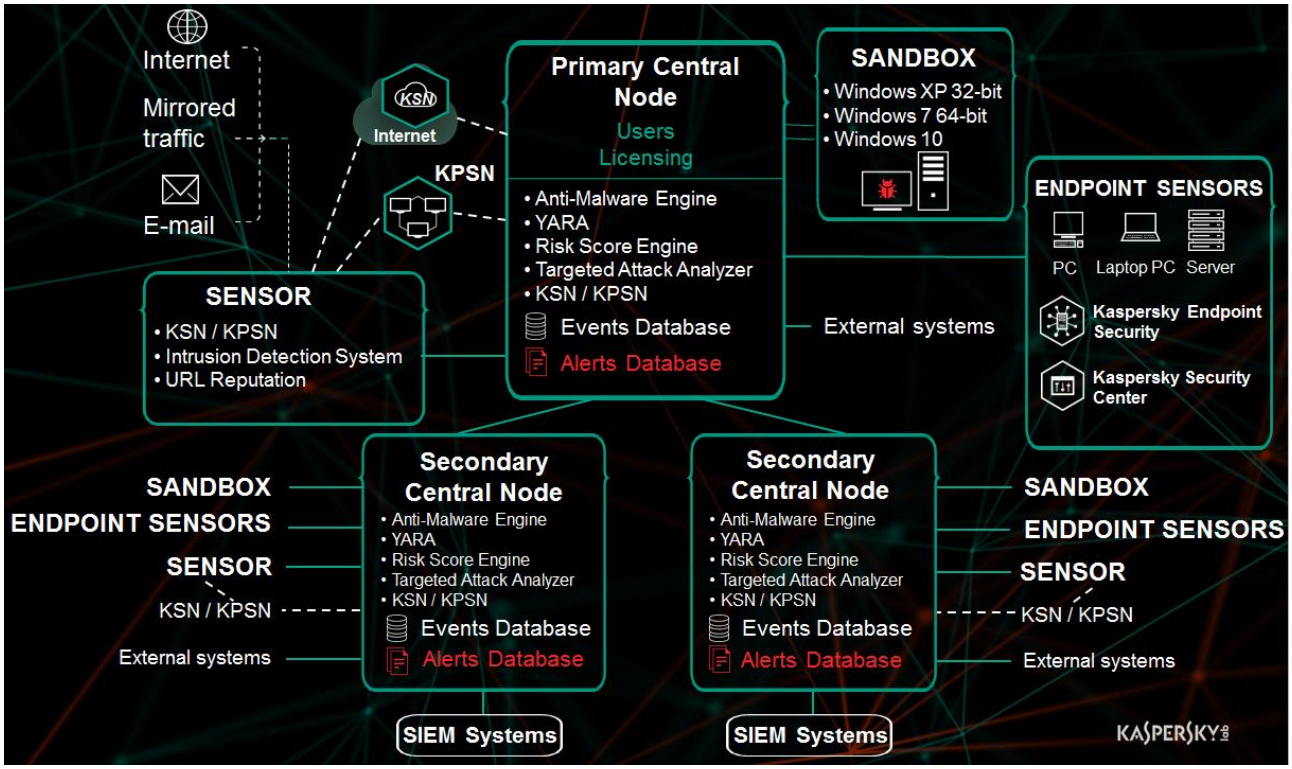


Схема 7: Принцип работы программы в режиме распределенного решения

Распределенное решение и режим multitenancy

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

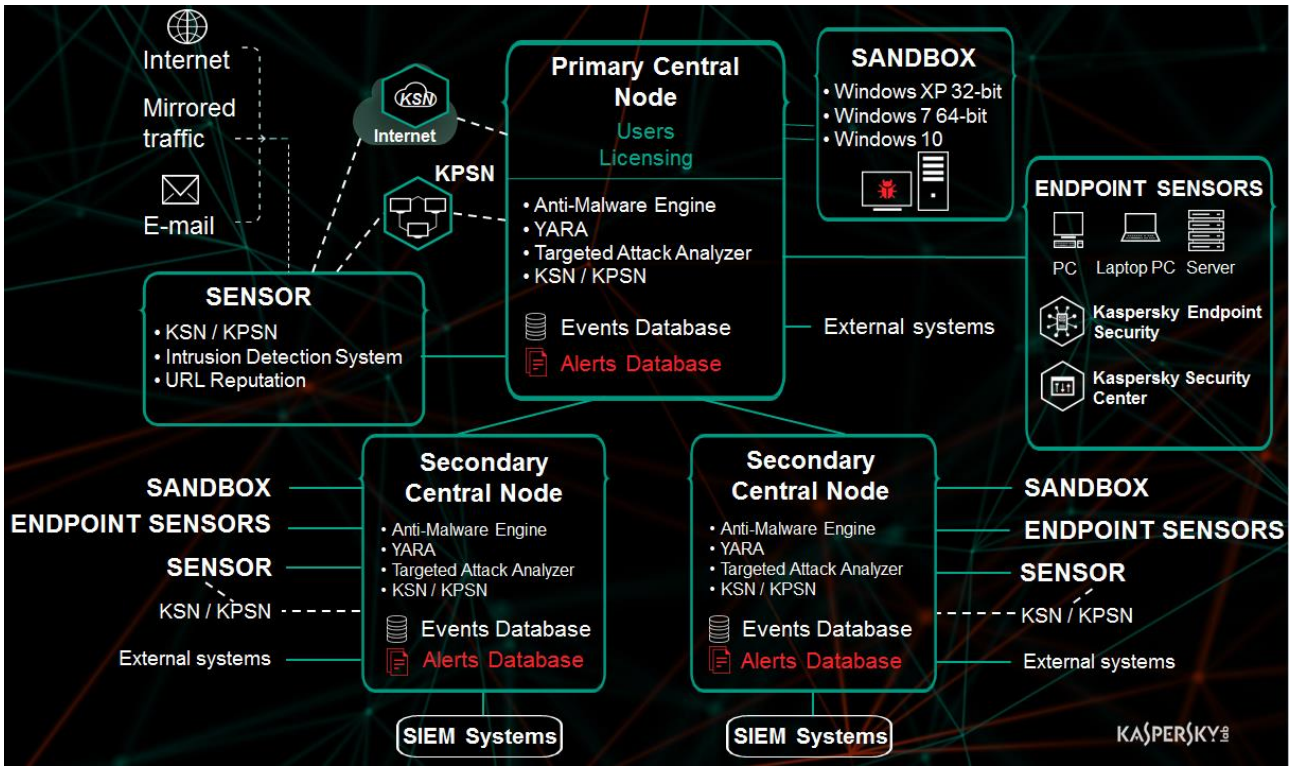
Распределенное решение представляет собой двухуровневую иерархию серверов с установленными компонентами Central Node. В этой структуре выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*. Для взаимодействия серверов необходимо подключить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

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

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

- Пользователи.
- Обнаружения.
- Поиск угроз.
- Задачи.
- Политики.
- IOC/IOA-анализ.
- Хранилище.
- Endpoint Sensors, в том числе сетевая изоляция хостов.
- Отчеты.

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



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

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

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

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

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

  В этом случае вам требуется обновить компонент Central Node до версии 3.6.

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

Сценарий перехода в режим распределенного решения и multitenancy

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

a. **Установка компонентов Central Node (стр. 101)**
b. **Назначение одному из серверов роли PCN (стр. 47)**
c. **Назначение остальным серверам роли SCN и отправка запросов на подключение к PCN (стр. 48)**
d. **Обработка запроса на подключение SCN к PCN (стр. 48)**

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

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

Таблица 5. Изменения в параметрах программы при переключении в режим распределенного решения и multitenancy

Функциональная область	PCN	SCN
Пользователи	Пользователи и назначенные им роли сохраняются. Дополнительно пользователям PCN выдаются права на работу с PCN и всеми подключенными SCN.	Удаляются все пользователи, кроме пользователя, созданного в момент развертывания Central Node. После этого SCN запрашивает у PCN список пользователей и на основе этого списка создает локальных пользователей с такими же параметрами: • имя; • пароль; • роль; • статус. Пользователи, не имеющие прав на доступ к SCN, не отображаются в списке пользователей.

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

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

Функциональная область	PCN	SCN
Резервное копирование программы	При наличии подключенных SCN резервное копирование на PCN становится недоступно.	Резервное копирование программы становится недоступно.

Назначение серверу роли PCN

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

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

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

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

   Откроется окно подтверждения действия.

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

Серверу будет назначена роль PCN и присвоено название организации.

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

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера, необходимый для проверки подлинности при установке соединения с SCN.
- **Организации** – информация об организациях, к которым относится этот сервер, и о подключенных серверах SCN:
  - **IP** – Primary Central Node для этого сервера и IP-адреса серверов SCN (после их подключения).
  - **Сервер** – имя этого сервера и имена серверов SCN (после их подключения).

    Это имя не связано с именем хоста, на котором установлена программа. Вы можете его изменить.
  - **Отпечаток сертификата** – пустое значение для этого сервера и отпечатки сертификатов

серверов SCN (после их подключения).

- **Состояние** – состояние подключения серверов SCN (после их подключения), а также количество серверов организации.

- Таблица **Серверы, ожидающие авторизации** с информацией о подключенных SCN (стр. 49).

Назначение серверу роли SCN

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

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

   Вам нужно войти в веб-интерфейс того сервера, которому вы хотите назначить роль SCN.

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

   В рабочей области отобразится отпечаток сертификата сервера с ролью PCN.

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

   Откроется окно подтверждения действия.

9. Нажмите на кнопку **Да**.

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

Обработка запросов на подключение SCN к PCN

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

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

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

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

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

3. Свяжитесь с администратором SCN, отправившим запрос на подключение, и проверьте отпечаток сертификата в таблице **Серверы, ожидающие авторизации**. Он должен совпадать с отпечатком, отображаемым на SCN в разделе **Режим работы** в поле **Отпечаток сертификата запроса**.
4. Если отпечатки сертификата на PCN и SCN совпадают, выполните одно из следующих действий:

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

     Откроется окно **Принять запрос на подключение**.
  2. В списке **Организация** выберите организацию, которой вы хотите назначить этот сервер SCN. Список формируется из организаций, добавленных ранее (стр. 50).
  3. Нажмите на кнопку **Принять**.

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

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

Просмотр информации об организациях, серверах PCN и SCN

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

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

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

   Вам нужно войти в веб-интерфейс сервера PCN.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.

В рабочей области отобразится следующая информация об организациях и серверах:

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера PCN.
- **Организации** – информация об организациях, к которым относится этот сервер, а также все серверы SCN, подключенные к PCN.
  - **IP** – Primary Central Node для сервера PCN и IP-адреса серверов SCN, подключенных к PCN.
  - **Сервер** – имя этого сервера и имена серверов SCN, подключенных к PCN.

    Это имя не связано с именем хоста, на котором установлена программа. Вы можете его изменить.
  - **Отпечаток сертификата** – пустое значение для сервера PCN и отпечатки сертификатов серверов SCN, которые ожидают подключения к PCN.
  - **Состояние** – состояние подключения, а также количество серверов организации.
- Таблица **Серверы, ожидающие авторизации** со следующей информацией:
  - **IP** – IP-адрес или доменное имя сервера SCN.

- **Сервер** – имя сервера SCN, которое отображается в веб-интерфейсе программы.

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

Добавление организации на сервере PCN

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

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

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

Организация будет добавлена и отобразится в списке.

Удаление организации на сервере PCN

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

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

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите удалить организацию.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. В рабочей области **Организации** выберите организацию, которую вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

   Действие необратимо. Все глобальные объекты, а также отчеты и шаблоны отчетов, связанные с этой организацией, будут потеряны.
5. Нажмите на кнопку **Да**.

Организация будет удалена.

Изменение названия организации на сервере PCN

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

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

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите изменить название организации.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. В списке **Организации** нажмите на значок  справа от названия организации, которое вы хотите изменить.

   Откроется окно изменения названия организации.
4. В поле **Имя** измените название организации.
5. Нажмите на кнопку **Сохранить**.

Название организации будет изменено.

Отключение SCN от PCN

Отключение SCN от PCN может быть односторонним.

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

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

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

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

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

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

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

Откроется окно подтверждения действия.

5. Нажмите на кнопку **Да**.

SCN будет пытаться подключиться к PCN для синхронизации параметров.

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

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

   Войдите в веб-интерфейс того сервера SCN, который вы хотите отключить от PCN.

2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. Нажмите на кнопку **Отключить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

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

Изменения в параметрах программы при отключении SCN от PCN

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

Таблица 6. Изменения параметров программы после отключения SCN от PCN

Функциональная область	PCN	SCN
Пользователи	Отключенный SCN не исключается из списка серверов, на которые распространяются права пользователей. Информация об изменении учетной записи пользователя, имеющего права на отключенный SCN, не передается на SCN.	Учетные записи пользователей, полученные с PCN, не удаляются. Появляется возможность создания новых учетных записей пользователей, а также отключения и смены пароля существующих учетных записей.
Обнаружения	Информация об обнаружениях на отключенном SCN удаляется.	История операций и вся информация об обнаружениях сохраняется.
Задачи	Задачи, созданные на отключенном SCN, удаляются.	Задачи, созданные на PCN, удаляются. Информация о пользователях, создавших задачи на SCN, сохраняется.
Отчеты	Все созданные ранее отчеты об отключенном SCN, а также возможность фильтровать список отчетов по этому серверу, сохраняются.	Шаблоны и отчеты не изменяются.

Функциональная область	PCN	SCN
Политики	Политики, созданные на отключенном SCN, удаляются.	Политики, созданные на PCN, удаляются. Информация о пользователях, создавших политики на SCN, сохраняется.
Хранилище	Из Хранилища удаляются все объекты, относящиеся к отключенному SCN.	Все объекты в Хранилище сохраняются. В информации об объектах, полученных в рамках задач, созданных на PCN, перестает работать ссылка на задачу.
Белый список	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Отправка уведомлений	Изменений нет.	Изменений нет.
Интеграция с почтовыми сенсорами	Изменений нет.	Изменений нет.
Интеграция с Kaspersky Security Center	Настройка интеграции с Kaspersky Security Center остается недоступной.	Настройка интеграции с Kaspersky Security Center становится доступна.
Поиск угроз	В результате обработки поискового запроса события, связанные с отключенным SCN, не отображаются.	Изменений нет.
IOC/IOA-анализ	Индикаторы IOC и IOA отключенного SCN удаляются.	Индикаторы IOC и IOA , созданные на PCN, удаляются.
Резервное копирование программы	Резервное копирование программы остается недоступным.	Резервное копирование программы становится доступным.

Вывод сервера SCN из эксплуатации

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

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

Вывод сервера SCN из эксплуатации программой состоит из следующих этапов:

a. **Удаление всех данных на SCN**
b. **Отключение SCN от PCN через веб-интерфейс PCN (стр. 51)**
c. **Отключение SCN от PCN через веб-интерфейс SCN (стр. 51)**
d. **Удаление SCN через веб-интерфейс PCN**

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

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

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

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

О предоставлении данных

Для работы некоторых компонентов Kaspersky Anti Targeted Attack Platform необходима обработка данных на стороне "Лаборатории Касперского". Компоненты не отправляют данные без согласия администратора Kaspersky Anti Targeted Attack Platform.

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

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

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

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

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

  Перед тем, как данные KSN-статистики отправляются в "Лабораторию Касперского", они накапливаются в кеше на серверах с компонентами Kaspersky Anti Targeted Attack Platform.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского".

"Лаборатория Касперского" использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

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

Данные компонентов Central Node и Sensor

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

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

Данные в журналах и файлах трассировки

Kaspersky Anti Targeted Attack Platform ведет запись в журналы действий пользователей, а также различных действий компонентов программы. В журналы могут попадать все данные, отображаемые в информации об обнаружениях, политиках, событиях, задачах и результатах их выполнения.

Данные на сервере Central Node хранятся в открытом незашифрованном виде и ротируются при достижении максимально разрешенного размера файла. Данные в журналах хранятся за последние 7 дней и безвозвратно удаляются при удалении программы.

Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность этих данных самостоятельно.

Kaspersky Anti Targeted Attack Platform записывает данные в следующие журналы:

1. Журнал истории обработки. Хранится в файле /var/log/kaspersky/apt-history/apt-history.log на серверах Central Node и Sensor. В журнал ведется запись этапов обработки объектов, фактов внесения изменений в параметры, информации о выполнении задач и запретов для последующего использования в разборе проблем и улучшения качества программы. Ниже перечислены данные, которые записываются в журнал истории обработки.
    a. Факт отправки файла на проверку:
        - MD5-хеш проверяемого файла.
        - Дата обработки файла.
        - Результат проверки.
        - Версия баз, с помощью которых проверялся файл.
        - Ядро, которое участвовало в проверке файла.
    b. Факт обработки файла или URL-адреса по белому списку:
        - Имя, тип, размер файла, путь к файлу, MD5-, SHA256-хеш файла, URL-адрес, с которого был скачан файл.
        - URL-адрес.
        - Правило белого списка.
        - IP-адрес и порт компьютера, который установил соединение (клиент).

- IP-адрес и порт компьютера, с которым было установлено соединение (сервер).
- Тип HTTP-запроса (GET, POST).
- Дата и время запроса (с точностью до секунды).
- User Agent (данные о браузере) клиента.
- Referrer.
- Тип DNS-сообщения (request, response).
- Тип DNS-запроса (A, MX).
- Дата и время DNS-сообщения (с точностью до секунды).
- Список всех IP-серверов (для DNS-ответа A-записи).
- Список всех доменных имен почтовых серверов, а также все IP-адреса, относящиеся к A-записи (для DNS-ответа MX записи).
- Значение сработавшего правила белого списка: адрес электронной почты, IP-адрес, домен, тип файла, MD5-хеш файла.

c. Факт обработки сообщения электронной почты по белому списку:
   - Информация о сообщении: адреса электронной почты отправителя и получателей сообщения.
   - Тема сообщения.

d. Факт создания обнаружения:
   - Важность обнаружения.
   - Дата и время, когда обнаружено событие.
   - Модули и технологии, которыми проверялся файл.
   - Результаты проверки модулями и технологиями.
   - MD5-хеш проверенного файла.
   - Проверенный URL-адрес.

e. Создание задач для компьютеров с компонентом Endpoint Sensors:
   - Идентификатор задачи, время создания, время ожидания (таймаут) выполнения задачи, тип задачи.
   - IP-адрес, имя хоста, которому назначена задача.
   - Имя, путь к запрашиваемому файлу, MD5-хеш запрашиваемого файла.
   - Приоритет выполнения задачи.

f. Обработка результатов выполнения задач для компьютеров с компонентом Endpoint Sensors:
   - Путь временного файла пакета от компьютера с компонентом Endpoint Sensors, размер пакета.
   - Имя хоста и IP-адрес компьютера с компонентом Endpoint Sensors.
   - Версия отчета от компьютера с компонентом Endpoint Sensors.
   - Информация о результатах проверки файла.

- Идентификатор процесса, количество областей памяти.
- Признак успешной обработки задачи.
- Описание ошибки, возникшей при обработке задач компьютера с компонентом Endpoint Sensors. В описании ошибки, помимо технической информации, могут содержаться следующие данные пользователя:
  - Пути к файлам, которые находятся на компьютере с компонентом Endpoint Sensors.
  - Сообщения электронной почты: тело сообщения, вложения, адреса электронной почты отправителя и получателей сообщения, IP-адрес отправителя сообщения, информация, содержащаяся в служебных заголовках сообщения, идентификатор сообщения электронной почты.
  - Содержимое файлов.
  - URL-адреса, извлеченные из сообщения электронной почты, с которых был скачан файл или по которым пользователь совершил переход.
  - Имя учетной записи пользователя, IP-адрес и имя компьютера пользователя.
  - MachineID компьютера пользователя.
  - UID компьютера пользователя в KSC.
  - Уникальный идентификатор компьютера от компонента Endpoint Sensors.
  - MAC-адрес компьютера пользователя.

g. Работа с политиками:

- Идентификатор запрета, дата и время внесения изменений в запрет.
- MD5- или SHA256-хеш файла.
- Уникальный идентификатор компьютера от компонента Endpoint Sensors.
- Имя запрета.
- MachineID хоста.

2. Журнал аудита. Хранится в файле /var/log/kaspersky/apt-audit.log на серверах Central Node и Sensor. В журнал ведется запись действий с учетными записями, параметрами, запись изменений статусов работоспособности компонентов программы для последующего использования в разборе проблем. Ниже перечислены данные, которые записываются в журнал аудита.

a. Факт внесения изменений в белый список:

- Имя учетной записи пользователя.
- Значение элемента белого списка: MD5-хеш, формат, маска URL-адреса, подсеть, User Agent (данные о браузере), адрес электронной почты.

b. Статусы компонентов программы:

- Время, название компонента, IP-адрес, статус, описание ошибки.
- Статус обновления баз.

c. Действия с учетными записями пользователей:

- Тип события (создание, изменение, удаление).
- Дата и время.

- Имя учетной записи пользователя.
- IP-адрес компьютера пользователя.
- Роль пользователя.
- Статус пользователя (активный / работа пользователя приостановлена).
- Имя учетной записи пользователя, внесшего изменения.

d. Изменение записей группы VIP:

- Тип события.
- Дата и время.
- Имя пользователя, создавшего или изменившего запись группы VIP.
- IP-адрес, FQDN-имя компьютера, адрес электронной почты.

e. Действия с обнаружениями:

- Идентификатор обнаружения.
- Имя учетной записи пользователя, выполнившего действие с обнаружением.

3. Системный журнал и файлы трассировки хранятся на серверах Central Node и Sensor. Системный журнал хранится в директории /var/log. Файлы трассировки хранятся в директории /var/log/kaspersky.

В файлах трассировки в открытом (незашифрованном) виде могут сохраняться те же данные, которые входят в состав данных об обнаружениях, политиках, событиях, задачах и результатах их выполнения. Вы можете настроить запись файлов трассировки в syslog (в режиме Technical Support Mode).

В системный журнал пишется общая информация о состоянии программы, а также возникших ошибках и исключениях в работе различных компонентов программы (в том числе стороннего производителя) и операционной системы.

Помимо данных об обнаружениях, политиках, событиях, задачах и результатах их выполнения, в файлах трассировки и в системных журналах могут содержаться следующие данные пользователя:

a. Пути к файлам, которые находятся на локальном компьютере.

b. Сообщения электронной почты: тело сообщения, вложения, адреса электронной почты отправителя и получателей сообщения, IP-адрес отправителя сообщения, информация, содержащаяся в служебных заголовках сообщения, идентификатор сообщения.

c. Содержимое файлов.

d. URL-адрес:

- извлеченный из сообщения электронной почты;
- с которого был скачан файл;
- по которому пользователь совершил переход.

e. Имя учетной записи пользователя, IP-адрес и имя компьютера пользователя.

f. MachineID компьютера пользователя.

g. UID компьютера пользователя в KSC.

h. Уникальный идентификатор компьютера от компонента Endpoint Sensors.

i. MAC-адрес компьютера пользователя.

Данные в обнаружениях

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

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

Во всех обнаружениях хранится следующая информация:

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

Если обнаружен файл в сетевом или почтовом трафике, на сервере может храниться следующая информация:

- Имя, размер, тип файла.
- MD5-, SHA256-хеш файла.
- Категория обнаруженного объекта (например, название вируса), важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
- Версии баз компонентов Kaspersky Anti Targeted Attack Platform, с помощью которых было выполнено обнаружение.
- Для каждой виртуальной машины компонента Sandbox: имя виртуальной машины, версия баз компонента Sandbox, с помощью которых был проверен файл, журнал исследования поведения файла.
- Названия YARA-правил, с помощью которых было выполнено обнаружение.
- Статус проверки объекта технологиями и время проверки каждой технологией.
- IP-адрес и тип интеграции сервера, на котором произошло обнаружение.
- Для IDS-обнаружения: адрес источника, адрес назначения, URL-адрес, User Agent, метод.
- Если файл получен от компонента Endpoint Sensors: IP-адрес, имя, домен хоста (в формате FQDN), полный путь к файлу на компьютере с компонентом Endpoint Sensors и имя файла.
- Принадлежность группе VIP.

- DNS-запрос, ответ на этот запрос и список хостов из запроса.
- URL-адрес FTP-запроса.

Если обнаружено сообщение электронной почты, на сервере может храниться следующая информация:

- Адреса электронной почты отправителя и получателей сообщения (включая получателей копии и скрытой копии сообщения).
- Тема сообщения электронной почты.
- Дата и время поступления сообщения в Kaspersky Anti Targeted Attack Platform, с точностью до секунд.
- Уникальный идентификатор сообщения электронной почты.
- Все служебные заголовки сообщения (так, как они выглядят в сообщении).
- IP-адрес, имя и тип интеграции сервера, на котором обнаружено сообщение электронной почты.
- URL-адреса, извлеченные из сообщения электронной почты.

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

- URL-адрес, к которому обращался компьютер локальной сети организации, или доменное имя из DNS-запроса.
- URL-адрес, извлеченный из сообщения электронной почты, до нормализации.
- IP-адрес отправителя пакета данных.
- IP-адрес получателя пакета данных.
- Категория обнаруженного объекта (например, вредоносный или фишинговый URL-адрес), важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это событие может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского", имена обнаруженных APT-атак.
- Принадлежность группе VIP.
- Информация о прокси-сервере.
- Уникальный идентификатор сообщения электронной почты.
- Адреса электронной почты отправителя и получателей сообщения (включая получателей копии и скрытой копии сообщения).
- Тема сообщения электронной почты.
- Дата и время поступления сообщения в Kaspersky Anti Targeted Attack Platform, с точностью до секунд.
- Список обнаруженных объектов.
- Время сетевого соединения.
- URL-адрес сетевого соединения.

Если обнаружение выполнено технологией Intrusion Detection System, на сервере может храниться следующая информация:

- Идентификатор правила IDS.
- Категория обнаруженного объекта по версии баз Intrusion Detection System.

- Категория обнаруженного объекта по классификации "Лаборатории Касперского".
- Версия баз Intrusion Detection System, с помощью которых было выполнено обнаружение.
- Важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
- Файл с трафиком, в котором произошло обнаружение.
- URL-адрес, извлеченный из файла с трафиком, User Agent, метод.
- IP-адрес и тип интеграции сервера, на котором произошло обнаружение.
- Принадлежность группе VIP.
- Время передачи данных.
- IP-адрес отправителя пакета данных.
- IP-адрес получателя пакета данных.

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

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

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

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

Если обнаружение выполнено в результате IOC-проверки, на сервере может храниться следующая информация:

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

Данные в событиях

Данные пользователя могут содержаться в событиях. Информация о произошедших событиях хранится на

сервере с компонентом Central Node в директории /data/var/lib/kaspersky/storage/fastsearch/elasticsearch/data/ в течение 30 дней.

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

Данные о событиях могут содержать следующую информацию:

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

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

Данные Targeted Attack Analyzer

Данные пользователя могут содержаться в обнаружениях. Информация об обнаружениях, выполненных с помощью технологии Targeted Attack Analyzer, хранится на сервере с компонентом Central Node в директории /data/var/lib/kaspersky/storage/fastsearch/detector/data/ бессрочно. Файлы, по результатам проверки которых возникло обнаружение, накапливаются на сервере с компонентом Central Node и ротируются по мере заполнения дискового пространства.

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

Если обнаружение выполнено Targeted Attack Analyzer, в Хранилище может содержаться следующая информация:

- Имя хоста.
- Имя пользователя.
- Время выполнения обнаружения.
- Имя обнаруженного объекта.
- Полное имя и путь к файлу, в котором обнаружен объект.
- MD5-, SHA256-хеш файла.
- VHS файла.

- Описание файла.
- Время создания файла.
- Время изменения файла.
- Компания, выпустившая программу, к которой относится файл.
- Версия файла.
- Автор файла.
- Параметры командной строки.
- Имя, владелец домена, дата регистрации домена, название организации, зарегистрировавшей домен.
- Популярность домена в мире.
- Дата и время обнаружения хоста.
- Количество обращений к хосту.
- Объем данных, загруженных с компьютера локальной сети на этот хост.
- IP-адрес, имя хоста и порт, с которого были отправлены данные.
- Локальный IP-адрес и порт сетевого адаптера.
- Версия баз программы, с помощью которых было выполнено обнаружение.
- URL-адреса посещенных веб-сайтов.
- Тип и описание обнаружения.
- Информация о файле процесса: путь к файлу процесса; компания, выпустившая программу, к которой относится процесс; версия программы; размер и версия файла, MD5-, SHA256-хеш файла; автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу, действительна ли подпись.
- Дата и время обнаружения процесса в локальной сети.
- Количество раз, которое процесс был обнаружен в локальной сети.
- Количество компьютеров, на которых был обнаружен подобный процесс.
- Популярность файла, запустившего процесс, в мире.
- Популярность пути, по которому был загружен процесс, в мире.
- Имена DLL-библиотек, на которые пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание, журнал DLL-активности.
- Тип учетной записи, тип входа в компьютер; дата и время, когда учетная запись была впервые обнаружена в локальной сети; дата и время, когда учетная запись была впервые обнаружена на компьютере; количество компьютеров, на которых была обнаружена учетная запись.
- Журнал HTTP-запросов и ответов для обнаруженных процессов и доменов: каждый час данные по каждой паре процесс – домен (время, удаленный хост, путь к файлу процесса, количество запросов, объем запросов, объем ответов); в рамках каждого часа точный журнал (индивидуальные HTTP-запросы и ответы (IP-адрес и порт источника; IP-адрес, порт, название адресата, длина тела и заголовка запроса, длина тела и заголовка ответа, время запроса, URI, имя удаленного хоста, User Agent, метод); заголовок и тело запроса и ответа для конкретной пары запрос – ответ).
- Журнал Process Activity для процессов, участвовавших в обнаружении: каждый час данные о

количестве запусков в час по каждому из процессов, перечисленных в блоке **Процессы**; в рамках каждого часа информация о времени каждого запуска и связанной команде; для каждого запуска путь к файлу, MD5-, SHA256-хеш файла; путь к родительскому файлу, MD5-, SHA256-хеш родительского файла, имя, роль и домен учетной записи, тип входа в компьютер, команда, время запуска и завершения процесса.

- Информация об обнаружении.
- Принадлежность группе VIP.
- Уникальный идентификатор компьютера, на котором выполнено обнаружение.
- DNS-запрос и ответ на него.

Данные в отчетах

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

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

В отчетах может содержаться следующая информация:

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

Данные об объектах в Хранилище

Объекты в Хранилище могут содержать данные пользователя. Информация об объектах в Хранилище хранится на сервере с компонентом Central Node в директории /data/var/lib/kaspersky/storage/pgsql/10/data/ бессрочно.

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

Данные об объектах в Хранилище могут содержать следующую информацию:

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

Данные о параметрах программы

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

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

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

Данные о политиках

Данные о политиках могут содержать следующую информацию:

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

Данные о задачах

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

Данные о задачах могут содержать следующую информацию:

- Идентификатор задачи.
- Время создания задачи.
- Имя и IP-адрес хоста, которому назначена задача.
- Максимальное время выполнения задачи.
- Приоритет выполнения задачи.
- Путь к файлу (для задач получения и удаления файла, помещения файла в Хранилище, завершения

процесса).

- От чьего имени требуется выполнить программу.
- Тип задачи (выполнение команды или запуск файла).
- Путь к файлу, аргументы или командная строка.
- Рабочая директория.
- Путь к ключу реестра.
- Отчет о выполнении задачи.
- Комментарии пользователя к задаче.
- Идентификатор учетной записи пользователя, создавшего задачу.

Данные об ученых записях пользователей

Данные об учетных записях пользователей программы могут содержать следующую информацию:

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

Данные о компонентах Endpoint Sensors

Данные о компонентах Endpoint Sensors могут содержать следующую информацию:

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

Данные о параметрах IOC-проверки

Данные о параметрах IOC-проверки могут содержать следующую информацию:

- Имя IOC-файла.
- Запросы IOC-проверки.
- Время последнего выполнения IOC-проверки.
- Состояние IOC-файла.
- Дата загрузки IOC-файла.
- Уровень важности создаваемых обнаружений.

Данные о правилах сетевой изоляции

Данные о правилах сетевой изоляции могут содержать следующую информацию:

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

Данные о шаблонах отчетов

Данные о шаблонах отчетов могут содержать следующую информацию:

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

Данные об общих параметрах программы

Данные об общих параметрах программы могут содержать следующую информацию:

- Параметры схем расположения графиков в разделе **Мониторинг**.
- Параметры IOC-проверки.
- Параметры интеграции с SIEM-системой.
- Параметры интеграции с почтовым сенсором.
- Показатели активности компонентов Endpoint Sensors.
- Адреса группы VIP.

Служебные данные, необходимые для работы программы

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

Таблица 7. Служебные данные, необходимые для работы программы

Тип данных	Место хранения	Доступ к данным	Срок хранения
Журнал событий операционной системы.	• /var/log	Доступ для пользователей с правами root.	Бессрочно.

Тип данных	Место хранения	Доступ к данным	Срок хранения
Кеш данных программы (redis).	• /var/log	Доступ пользователей определяется администратором с помощью средств операционной системы. Доступ осуществляется только по шифрованному каналу IPSec.	Бессрочно.
Файлы экспорта	• /var/log	Доступ	Бессрочно.
Артефакты компонента Sandbox, файлы PCAP перехваченного трафика.	• /var/opt/kaspersky/apt-agents/sb_storage	Доступ пользователей определяется администратором с помощью средств операционной системы.	Файлы ротируются при заполнении отведенного места хранения.
Очередь объектов на проверку.	• /var/opt/kaspersky/apt-collector/spool	Доступ пользователей определяется администратором с помощью средств операционной системы.	До выполнения проверки.
Объекты в Карантине, а также объекты, полученные от компонента Endpoint Sensors.	• /var/opt/kaspersky/apt/edr_quarantine • /var/opt/kaspersky/apt/edr_storage	Доступ пользователей определяется администратором с помощью средств операционной системы.	Файлы ротируются при заполнении отведенного места хранения.
YARA-правила.	• /var/opt/kaspersky/apt-agents/yara_rules	Доступ пользователей определяется администратором с помощью средств операционной системы.	Бессрочно.

Тип данных	Место хранения	Доступ к данным	Срок хранения
Сертификаты серверов, используемые для интеграции компонентов программы.	• /etc/ssl/certs	Доступ пользователей определяется администратором с помощью средств операционной системы. Информация о действиях с сертификатами сохраняется в журнале событий программы.	Бессрочно.
Ключи шифрования, передаваемые между компонентами программы.	• /etc/opt/kaspersky/apt-base/ipsec.d	Доступ пользователей определяется администратором с помощью средств операционной системы. Информация об изменениях ключей шифрования сохраняется в журнале событий программы.	Бессрочно.

Данные компонента Endpoint Sensors

Если вы используете компонент Endpoint Sensors, на сервер с компонентом Central Node могут передаваться файлы, связанные с обнаруженными событиями.

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

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

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

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

Файлы, подготовленные к отправке компонентом Endpoint Sensors на сервер с компонентом Central Node, хранятся на компьютерах с компонентом Endpoint Sensors в открытом незашифрованном виде в той

директории, которая по умолчанию используется для хранения файлов перед отправкой на каждом компьютере с компонентом Endpoint Sensors.

Файлы с компьютеров с компонентом Endpoint Sensors отправляются только на сервер с компонентом Central Node по защищенному SSL-соединению (стр. 132).

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

Kaspersky Anti Targeted Attack Platform поддерживает возможность изменения параметров локального компьютера с компонентом Endpoint Sensors, влияющих на производительность компьютера при взаимодействии с компонентом Central Node.
Изменение параметров следует производить исключительно по рекомендации Службы технической поддержки "Лаборатории Касперского".
Самостоятельное изменение параметров может ухудшить производительность локального компьютера.

Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность компьютеров с компонентом Endpoint Sensors и серверов Kaspersky Anti Targeted Attack Platform с перечисленными выше данными самостоятельно. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за доступ к данной информации.

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

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

Данные, получаемые от компонента Central Node

Компонент Endpoint Sensors сохраняет на жестком диске компьютера значения параметров, получаемые от компонента Central Node. Данные сохраняются в открытом незашифрованном виде в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\data.

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

Данные удаляются при удалении компонента Endpoint Sensors.

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

- О сетевых соединениях.

- Об операционной системе, установленной на сервере с компонентом Central Node.
- Об учетных записях пользователей операционной системы.
- О пользовательских сессиях в операционной системе.
- О журнале событий Windows.
- О ресурсе типа RT_VERSION.
- О содержимом PE-файла.
- О службах операционной системы.
- Сертификат сервера с компонентом Central Node.
- URL- и IP-адреса посещенных веб-сайтов.
- Заголовки протокола HTTP.
- Имя компьютера.
- MD5-хеши файлов.
- Уникальный идентификатор компьютера с компонентом Endpoint Sensors.
- Имена и значения ключей реестра Windows.
- Пути к ключам реестра Windows.
- Имена переменных реестра Windows.
- Имя записи локального DNS-кеша.
- Адрес из записи локального DNS-кеша в формате IPv4.
- IP-адрес или имя запрашиваемого хоста из локального DNS-кеша.
- Хост элемента локального DNS-кеша.
- Доменное имя элемента локального DNS-кеша.
- Адрес элемента ARP-кеша в формате IPv4.
- Физический адрес элемента APR-кеша.
- Серийный номер логического диска.
- Домашняя директория локального пользователя.
- Имя учетной записи пользователя, запустившего процесс.
- Путь к скрипту, запускаемому при входе пользователя в систему.
- Имя пользователя, под учетной записью которого произошло событие.
- Имя компьютера, на котором произошло событие.
- Полные пути к файлам компьютеров с компонентом Endpoint Sensors.
- Имена файлов компьютеров с компонентом Endpoint Sensors.
- Маски файлов компьютеров с компонентом Endpoint Sensors.
- Полные имена папок компьютеров с компонентом Endpoint Sensors.
- Комментарии поставщика файла.
- Маска файла-образа процесса.

- Путь к файлу-образу процесса, открывшего порт.
- Имя процесса, открывшего порт.
- Локальный IP-адрес порта.
- Доверенный публичный ключ цифровой подписи исполняемых модулей.
- Имя процесса.
- Имя сегмента процесса.
- Параметры командной строки.

Данные в журналах и файлах трассировки

Компонент Endpoint Sensors может выполнять запись отладочной информации компонента и драйверов компонента в соответствии с заданными параметрами в файлы трассировки. По умолчанию компонент Endpoint Sensors не записывает отладочную информацию. Автоматическая отправка файлов трассировки за пределы хоста, на котором они были сформированы, не производится. Содержимое файлов трассировки можно просмотреть с помощью стандартных средств просмотра текстовых файлов. Файлы трассировки полностью удаляются при удалении компонента Endpoint Sensors.

Файлы трассировки хранятся в открытом незашифрованном виде в следующих папках:

- Файлы трассировки сервисной части и драйверов компонента Endpoint Sensors в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\logs\system.

  Пользователи с правами учетной записи операционной системы System и Administrator могут удалять файлы, изменять их содержимое и изменять права доступа к ним.

- Файлы трассировки оболочки Shell и графического интерфейса компонента Endpoint Sensors в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\logs\user.

  Пользователи с правами учетной записи операционной системы User, System и Administrator могут удалять файлы и изменять их содержимое. Пользователи с правами учетной записи операционной системы System и Administrator могут также изменять права доступа к файлам.

Компонент Endpoint Sensors не управляет правами доступа к этим папкам и их файлам. По умолчанию доступ к файлам на чтение имеют только пользователи с правами System и Administrator.

Данные в файлах трассировки могут содержать следующую информацию:

- Время события.
- Номер потока выполнения.
- Компонент программы, в результате работы которого произошло обнаружение.
- Важности события.
- Об исполняемых модулях.
- Об открытых портах.
- О сетевых соединениях.
- Об операционной системе, установленной на компьютере с компонентом Endpoint Sensors.
- Об учетных записях пользователей операционной системы.
- О пользовательских сессиях в операционной системе.

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

- Исходное имя файла (OriginalFileName) для ресурса RT_VERSION.

Данные в обнаружениях и событиях

Данные о событиях хранятся в бинарном виде в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\kata в открытом незашифрованном виде.

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

Данные о событиях могут содержать следующую информацию:

- Об исполняемых модулях.
- О сетевых соединениях.
- Об операционной системе, установленной на компьютере с компонентом Endpoint Sensors.
- О пользовательских сессиях в операционной системе.
- Об учетных записях пользователей операционной системы.
- О журнале событий Windows.
- Об обнаружениях Kaspersky Endpoint Security для Windows.
- Об организационных подразделениях (OU) Active Directory.
- Заголовки протокола HTTP.
- Полное доменное имя компьютера.
- MD5-, SHA256-хеш файлов и их фрагментов.
- Уникальный идентификатор компьютера с компонентом Endpoint Sensors.
- Уникальные идентификаторы сертификатов.
- Издатель сертификата.
- Субъект сертификата.
- Название алгоритма, при помощи которого выполнен отпечаток сертификата.
- Адрес и порт локального сетевого интерфейса.
- Адрес и порт удаленного сетевого интерфейса.
- Поставщик программы.
- Название программы.
- Имя переменной реестра Windows.
- Путь к ключу реестра Windows.
- Данные переменной реестра Windows.
- Имя обнаруженного объекта.
- Идентификатор Агента администрирования Kasersky Security Center.

- Содержимое файла hosts.
- Командная строка запуска процесса.

Данные в отчетах о выполнении задач

Перед отправкой на компонент Central Node отчеты, а также сопутствующие файлы временно сохраняются на жестком диске компьютера с компонентом Endpoint Sensors. Отчеты о выполнении задач сохраняются в архивированном незашифрованном виде в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\kata\data_queue.

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

Отчеты о выполнении задач содержат следующую информацию:

- О результатах выполнения задач.
- Об исполняемых модулях.
- О процессах операционной системы.
- Об учетных записях пользователей.
- О пользовательских сессиях.
- Полное доменное имя компьютера.
- Уникальный идентификатор компьютера с компонентом Endpoint Sensors.
- Файлы компьютера с компонентом Endpoint Sensors.
- Имена альтернативных потоков NTFS.
- Полные пути к файлам компьютера с компонентом Endpoint Sensors.
- Полные имена папок компьютера с компонентом Endpoint Sensors.
- Содержимое стандартного потока вывода процесса.
- Содержимое стандартного потока ошибок процесса.

Данные в журнале установки

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

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

Данные о файлах, запрещенных к запуску

Данные о файлах, запрещенных к запуску, хранятся в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor

3.6\protected\kata в открытом незашифрованном виде.

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

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

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

Данные, связанные с выполнением задач

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

- для компонента Endpoint Sensors, входящего в состав программы Kaspersky Endpoint Security, в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\kata\temp;
- для компонента Endpoint Sensors, установленного из пакета Kaspersky Anti Targeted Attack Platform, в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\data\kata\temp.

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

- для компонента Endpoint Sensors, входящего в состав программы Kaspersky Endpoint Security, в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\kata\temp;
- для компонента Endpoint Sensors, установленного из пакета Kaspersky Anti Targeted Attack Platform, в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\data\kata\temp.

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

Данные в файлах дампов

При выполнении запроса о предоставлении дампов процесса компонент Endpoint Sensors локально хранит содержимое дампов процесса в открытом незашифрованном виде в следующих папках:

- Файлы дампов сервисной части и драйверов компонента Endpoint Sensors в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\logs\system.

  Пользователи с правами учетной записи операционной системы System и Administrator могут удалять файлы, изменять их содержимое и изменять права доступа к ним.

- Файлы дампов и оболочки Shell компонента Endpoint Sensors в папке C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\logs\user.

  Пользователи с правами учетной записи операционной системы User, System и Administrator могут удалять файлы и изменять их содержимое. Пользователи с правами учетной записи операционной системы System и Administrator могут также изменять права доступа к файлам.

Данные хранятся до тех пор, пока отчет о выполнении запроса не будет отправлен на компонент Central Node. Компонент Endpoint Sensors не управляет правами доступа к данной папке и ее файлам. Доступ определяет системный администратор. По умолчанию доступ к файлам на чтение имеют только пользователи с правами System и Administrator.

Файлы дампов компонента Endpoint Sensors формируются операционной системой при сбоях программы, хранятся в папке, заданной параметрами операционной системы, и перезаписываются при каждом сбое. В файлы дампов могут попасть любые персональные данные пользователя или конфиденциальные данные вашей организации.

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

Данные в файлах дампов могут содержать следующую информацию:

- Время события.
- Номер потока выполнения.
- Компонент программы, в результате работы которого произошло обнаружение.
- Важность события.
- Об исполняемых модулях.
- Об открытых портах.
- О сетевых соединениях.
- Об операционной системе, установленной на компьютере с компонентом Endpoint Sensors.
- Об учетных записях пользователей операционной системы.
- О пользовательских сессиях в операционной системе.
- О журнале событий Windows.
- Об обнаружениях Kaspersky Endpoint Security для Windows.
- Об организационных подразделениях (OU) Active Directory.
- Уникальный идентификатор компьютера с компонентом Endpoint Sensors.
- Полное доменное имя компьютера.
- Серийный номер логического диска.
- Заголовки протокола HTTP.
- Полные пути к файлам компьютера с компонентом Endpoint Sensors.
- Имена файлов компьютера с компонентом Endpoint Sensors.
- Полные имена папок компьютера с компонентом Endpoint Sensors.

- Домашняя директория локального пользователя.
- Имя учетной записи пользователя, запустившего процесс.
- Путь к скрипту, запускаемому при входе пользователя в систему.
- Имя пользователя, под учетной записью которого произошло событие.
- URL- и IP-адреса посещенных веб-сайтов, а также ссылки с этих веб-сайтов.
- При использовании прокси-сервера: IP-адрес прокси-сервера, имя компьютера, порт, имя пользователя прокси-сервера.
- Внешние IP-адреса, с которыми было установлено соединение с локального компьютера.
- Команды запуска процесса.
- Параметры командной строки.
- Идентификатор Агента администрирования Kaspersky Security Center.
- Пути к ключам в реестре Windows.
- Имена переменных реестра Windows.
- Значения переменных реестра Windows.
- Разделы реестра Windows.
- Имена обнаруженных объектов.
- Имя записи локального DNS-кеша.
- Адрес из записи локального DNS-кеша в формате IPv4.
- IP-адрес или имя запрашиваемого хоста из локального DNS-кеша.
- Хост элемента локального DNS-кеша.
- Доменное имя элемента локального DNS-кеша.
- Адрес элемента ARP-кеша в формате IPv4.
- Физический адрес элемента APR-кеша.
- Имя учетной записи пользователя, запустившего сервис операционной системы.
- Параметры, с которыми запущен сервис операционной системы.
- Исходное имя файла (OriginalFileName) для ресурса RT_VERSION.

Данные компонента Sandbox

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

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

Таблица 8. Данные, хранящиеся на сервере с компонентом Sandbox

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

Данные, пересылаемые между компонентами программы

Central Node и Endpoint Sensors

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

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

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

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

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

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

MD5-, SHA256-хеш файла, размер файла.

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

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

- PID процесса, отображаемый в диспетчере задач Windows.
- Командная срока запуска процесса.
- Причина ошибки при обработке объекта.

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

Central Node и Sandbox

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

Central Node и Sensor

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

- Файлы и сообщения электронной почты.
- Данные об обнаружениях, выполненных технологиями Intrusion Detection System и URL Reputation.
- Информацию о лицензии.
- Белые списки.
- Данные компонента Endpoint Sensors, если настроена интеграция с прокси-сервером (стр. 197).
- Базы программы, если настроено получение обновления баз от компонента Central Node.

Серверы с ролями PCN и SCN

Если программа работает в режиме распределенного решения (стр. 42), то между PCN и подключенными SCN передаются следующие данные:

- Об обнаружениях.
- О событиях.
- О задачах.
- О политиках.
- Об IOC-проверке.
- О файлах в Хранилище.
- Об учетных записях пользователей.
- О лицензии.
- Список компьютеров с установленным компонентом Endpoint Sensors.
- Объекты, помещенные в Хранилище.
- Файлы, прикрепленные к обнаружениям.
- IOC-файлы.

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 Anti Targeted Attack Platform.
- Прочитав документ /EULA/License.<язык>.

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

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

О лицензии

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

Лицензия включает в себя право на получение следующих видов услуг:

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

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

В Kaspersky Anti Targeted Attack Platform предусмотрены следующие типы лицензий:

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

По истечении срока действия лицензии программа продолжает работу, но с ограниченной функциональностью (стр. 91). Чтобы использовать программу в режиме полной функциональности, вам

нужно приобрести коммерческую лицензию или продлить срок действия коммерческой лицензии.

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность программы также зависит от типа установленного ключа.

О лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

О ключе

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

► *Чтобы добавить ключ в программу,*

загрузите файл ключа.

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

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность программы зависит от типа установленного ключа:

- **Ключи KATA и KEDR**. Полная функциональность программы.
- **Ключ KEDR**. Ограничен прием и обработка данных из сетевого и почтового трафика.
- **Ключ KATA**. Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **IOC-проверка**, **Хранилище**, **Endpoint Sensors**.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл

ключа предназначен для добавления ключа, активирующего программу.

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

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

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

Для восстановления файла ключа обратитесь к продавцу лицензии.

Просмотр информации о лицензии и добавленных ключах

В режиме распределенного решения (стр. 42) и multitenancy вы можете просматривать информацию о лицензии и добавленных ключах в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса программы.

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

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

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

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

За 30 дней до окончания срока действия лицензии в разделе **Мониторинг** появляется уведомление о необходимости продлить лицензию. Это уведомление отображается на всех серверах с компонентом Central Node (в режиме распределенного решения и multitenancy – на PCN и всех подключенных SCN) для всех пользователей независимо от их роли.

Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node

В режиме распределенного решения (стр. 42) и multitenancy вы можете просматривать текст Лицензионного соглашения в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса программы.

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

1. Выберите раздел **Параметры**, подраздел **Лицензия**.
2. Нажмите на кнопку **Лицензионное соглашение** в правом верхнем углу рабочей области.

3. В открывшемся окне просмотрите текст Лицензионного соглашения.
4. По окончании просмотра нажмите на кнопку **Закрыть**.

Просмотр текста Политики конфиденциальности в веб-интерфейсе Central Node

В режиме распределенного решения и multitenancy вы можете просматривать текст Политики конфиденциальности в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса программы.

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

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

Просмотр информации о стороннем коде, используемом в программе

В режиме распределенного решения и multitenancy вы можете просматривать информацию о стороннем коде, используемом в Kaspersky Anti Targeted Attack Platform, в веб-интерфейсе серверов PCN и всех подключенных SCN под учетной записью локального администратора, администратора или пользователей веб-интерфейса программы.

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

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

Просмотр текста Лицензионного соглашения в веб-интерфейсе Sandbox

► *Чтобы просмотреть текст Лицензионного соглашения в веб-интерфейсе сервера с компонентом Sandbox (стр. 164), выполните следующие действия:*

1. Войдите в веб-интерфейс Sandbox под учетными данными, которые вы задали при установке компонента Sandbox (стр. 98).

2. Нажмите на кнопку  в левой нижней части окна веб-интерфейса.
3. Откроется окно с информацией о компоненте Sandbox.
4. По ссылке **Лицензионное соглашение** раскройте окно с текстом Лицензионного соглашения программы.
5. Просмотрите текст Лицензионного соглашения.
6. По окончании просмотра нажмите на кнопку ✕.

Просмотр текста Лицензионного соглашения на компьютере с компонентом Endpoint Sensors

На каждом компьютере, на котором установлен отдельный компонент Endoint Sensors, файл с Лицензионным соглашением Kaspersky Anti Targeted Attack Platform находится в папке EULA в той директории, в которой установлен компонент Endpoint Sensors (стр. 131).

Добавление ключа

В режиме распределенного решения (стр. 42) добавление ключа доступно только на сервере PCN.

► *Чтобы добавить ключ, выполните следующие действия:*

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

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

   Окно выбора файлов закроется.

Ключ будет добавлен в программу.

Замена ключа

В режиме распределенного решения (стр. 42) замена ключа доступна только на сервере PCN.

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

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Лицензия**.

2. Выберите тип ключа: **KATA** или **KEDR**.
3. В разделе с выбранным типом ключа нажмите на кнопку **Заменить**.

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

   Окно выбора файлов закроется.

Загруженный ключ заменит активный ключ программы.

Удаление ключа

> В режиме распределенного решения (стр. 42) удаление ключа доступно только на сервере PCN.

► *Чтобы удалить ключ, выполните следующие действия:*

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

   Откроется окно подтверждения удаления ключа.
4. Нажмите на кнопку **Да**.

   Окно подтверждения удаления ключа закроется.

Ключ будет удален.

Режимы работы программы в соответствии с лицензией

В Kaspersky Anti Targeted Attack Platform предусмотрены различные режимы работы программы в зависимости от добавленных ключей.

Без лицензии

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

В режиме Без лицензии действуют следующие ограничения:

- Не обновляются базы программы.
- Отсутствует подключение к базе знаний Kaspersky Security Network.
- Ограничен прием и обработка данных из сетевого и почтового трафика.
- Ограничена функциональность разделов веб интерфейса **Поиск угроз**, **Задачи**, **Политики**, **IOC-проверка**, **Хранилище**, **Endpoint Sensors**.

Коммерческая лицензия

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

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

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

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность программы также зависит от типа установленного ключа:

- **Ключи KATA и KEDR**. Полная функциональность программы.
- **Ключ KEDR**. Ограничен прием и обработка данных из сетевого и почтового трафика.
- **Ключ KATA**. Ограничена функциональность разделов веб-интерфейса **Поиск угроз**, **Задачи**, **Политики**, **IOC-проверка**, **Хранилище**, **Endpoint Sensors**.

Установка и первоначальная настройка программы

В этом разделе содержатся инструкции по установке и первоначальной настройке программы.

Подготовка к установке компонентов программы

В этом разделе представлена информация о том, как подготовить IT-инфраструктуру вашей организации к установке компонентов Kaspersky Anti Targeted Attack Platform.

Подготовка IT-инфраструктуры к установке компонентов программы

► *Перед установкой программы подготовьте IT-инфраструктуру вашей организации к установке компонентов Kaspersky Anti Targeted Attack Platform:*

1. Убедитесь, что серверы, а также компьютер, предназначенный для работы с веб-интерфейсом программы, и компьютеры, на которых устанавливается компонент Endpoint Sensors, удовлетворяют аппаратным и программным требованиям (стр. 22).
2. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Sandbox:
   a. Для обоих сетевых интерфейсов запретите доступ сервера с компонентом Sandbox в локальную сеть организации для обеспечения безопасности сети от анализируемых объектов.
   b. Для первого сетевого интерфейса разрешите доступ сервера с компонентом Sandbox в интернет для обновления баз и анализа поведения объектов.
   c. Для второго сетевого интерфейса разрешите входящее соединение сервера с компонентом Sandbox на следующие порты:
      - TCP 22 для подключения к серверу по протоколу SSH.
      - TCP 443 для получения объектов на проверку от компонента Central Node.
      - TCP 8443 для использования веб-интерфейса программы.
3. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Central Node:
   a. Разрешите входящее соединение сервера с компонентом Central Node на следующие порты:
      - TCP 22 для подключения к серверу по SSH.
      - TCP 8081 для получения данных от сервера с компонентом Sensor.
      - TCP 9092 для добавления метаданных в базу данных Targeted Attack Analyzer (если компонент Sensor устанавливается на отдельный сервер).
      - TCP 443 для получения данных от компьютеров с компонентом Endpoint Sensors.
      - TCP 6379 для синхронизации с базой данных Redis на сервере с компонентом Sensor.
      - TCP 8443 для просмотра результатов проверки в веб-интерфейсе программы.
   b. Разрешите исходящее соединение сервера с компонентом Central Node на следующие порты:
      - UDP 161 для получения данных о состоянии компонента Sensor (если компонент Sensor

устанавливается на отдельный сервер).

- TCP 80 и 443 для связи с серверами службы KSN и серверами обновлений "Лаборатории Касперского".
- TCP 443 для передачи объектов на проверку компоненту Sandbox.
- TCP 601 для отправки сообщений в SIEM-систему.
- TCP 13299 для интеграции с Kaspersky Security Center.

4. Произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонента Sensor:

   a. Для сетевого интерфейса, используемого для интеграции с прокси-сервером и почтовым сервером, разрешите входящее соединение сервера с компонентом Sensor на следующие порты:

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

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

   - TCP 8081 для передачи объектов на сервер с компонентом Central Node.
   - TCP 80 и 443 для связи с серверами службы KSN и серверами обновлений "Лаборатории Касперского".
   - TCP 6379 для синхронизации с базой данных Redis на сервере с компонентом Central Node.
   - TCP 9092 для передачи метаданных из зеркалированного трафика на сервер с компонентом Central Node.
   - TCP 995 (или TCP 110 для незащищенных соединений) для интеграции с почтовым сервером.

   При установке второго сетевого интерфейса, принимающего только зеркалированный трафик, в виртуальной среде VMware ESXi используйте сетевой адаптер E1000 или отключите опцию LRO (large receive offload) на сетевом адаптере VMXNET3.

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

   Соединение между серверами с компонентами Central Node и Sensor происходит внутри шифрованного канала связи на базе IPSec с использованием протокола ESP.

7. Если вы используете режим распределенного решения и multitenancy, произведите следующую предварительную подготовку IT-инфраструктуры организации к установке компонентов Central Node:

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

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

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

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

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

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

Если в качестве почтового сервера вы используете почтовый сервер Microsoft Exchange и отправитель настроил запрос уведомления о прочтении сообщения электронной почты, то необходимо отключить отправку уведомлений о прочтении. В противном случае уведомления о прочтении будут отправляться с того адреса электронной почты, который вы настроили в качестве адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform. Также необходимо отключить автоматическую обработку приглашений на встречи для предотвращения заполнения почтового ящика для приема сообщений Kaspersky Anti Targeted Attack Platform.

► *Чтобы отключить отправку уведомлений о прочтении с адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform, выполните следующие действия:*

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

   ```
   Get-MailboxMessageConfiguration -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> | fl
   ```

2. Если отправка уведомлений включена, выполните команду:

   ```
   Set-MailboxMessageConfiguration -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> -ReadReceiptResponse NeverSend
   ```

Отправка уведомлений о прочтении с адреса электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform будет отключена.

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

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

   ```
   Get-CalendarProcessing -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> | fl
   ```

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

   ```
   Set-CalendarProcessing -Identity <адрес электронной почты для приема сообщений Kaspersky Anti Targeted Attack Platform> -AutomateProcessing:None
   ```

Автоматическая обработка приглашений на встречи будет отключена.

Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP

► *Чтобы подготовить IT-инфраструктуру вашей организации к интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP, выполните следующие действия:*

1. На внешнем почтовом сервере настройте правила пересылки копий тех сообщений, которые вы хотите отправлять на проверку Kaspersky Anti Targeted Attack Platform на адреса, указанные в Kaspersky Anti Targeted Attack Platform.
2. Укажите маршрут для пересылки сообщений электронной почты на сервер с компонентом Sensor.

   Рекомендуется указать статический маршрут – IP-адрес сервера с компонентом Sensor.
3. На сетевом экране вашей организации разрешите входящие соединения сервера с компонентом Sensor на порт 25 от почтовых серверов, пересылающих копии сообщений электронной почты.

Вы также можете увеличить безопасность интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP.

► *Чтобы увеличить безопасность интеграции Kaspersky Anti Targeted Attack Platform с почтовым сервером по протоколу SMTP, выполните следующие действия:*

1. Настройте аутентификацию сервера Kaspersky Anti Targeted Attack Platform на стороне почтовых серверов, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform.
2. Настройте обязательное шифрование трафика на почтовых серверах, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform.
3. Настройте аутентификацию почтовых серверов, передающих сообщения электронной почты для Kaspersky Anti Targeted Attack Platform, на стороне Kaspersky Anti Targeted Attack Platform.

Подготовка виртуальной машины к установке компонента Sandbox

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

4. Откройте консоль для управления виртуальными машинами.
5. В контекстном меню виртуальной машины, на которой вы хотите установить компонент Sandbox, выберите пункт **Edit Settings**.

   Откроется окно свойств виртуальной машины.
6. На закладке **Virtual Hardware** раскройте блок параметров **CPU** и установите флажок **Expose hardware-assisted virtualization to guest OS**.
7. На закладке **VM Options** в раскрывающемся списке **Latency Sensitivity** выберите **High**.
8. Нажмите на кнопку **OK**.

Виртуальная машина будет готова к установке компонента Sandbox.

Порядок установки и настройки компонентов программы

Выполняйте действия по установке и настройке программы в следующем порядке:

1. Установите образ диска с компонентом Sandbox.
2. Настройте компонент Sandbox через веб-интерфейс Sandbox.
3. Установите образы дисков операционных систем Microsoft Windows и программ для работы компонента Sandbox.
4. Установите образ диска с компонентами Central Node и Sensor. Настройте компоненты Central Node и Sensor.

   При наличии нескольких компонентов Central Node вы можете использовать программу в режиме распределенного решения и multitenancy (стр. 42).

   При наличии нескольких компонентов Sensor вы можете установить и настроить компонент Sensor (стр. 116) на необходимом количестве серверов.

   При необходимости использования компонента Central Node отдельно от компонента Sensor пропускайте шаги по настройке компонента Sensor при установке компонентов Central Node и Sensor (стр. 101).
5. Установите компонент Endpoint Sensors на компьютерах, входящих в IT-инфраструктуру организации.

Установка компонента Sandbox

Этот раздел представляет собой пошаговую инструкцию по установке компонента Sandbox.

► *Чтобы приступить к установке компонента Sandbox,*

запустите образ диска с компонентом Sandbox.

Запустится мастер установки.

Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

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

Также вам нужно просмотреть Политику конфиденциальности и принять ее условия.

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

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

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

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

Откроется окно с текстом Политики конфиденциальности.

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

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор диска для установки компонента Sandbox

На этом шаге выберите физический диск для установки компонента Sandbox.

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

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

   Архив с установочными файлами распакуется на диск. Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 3. Создание учетной записи администратора Sandbox

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

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

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

   Пароль должен удовлетворять следующим требованиям:

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

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор управляющего сетевого интерфейса в списке

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

- Управляющий сетевой интерфейс. Этот интерфейс предназначен для доступа к серверу с компонентом Sandbox по протоколу SSH, а также через этот интерфейс сервер с компонентом Sandbox будет принимать объекты с сервера с компонентом Central Node.

- Сетевой интерфейс для доступа обрабатываемых объектов в интернет. Через этот интерфейс объекты, которые обрабатывает компонент Sandbox, смогут предпринимать попытки действий в интернете, а компонент Sandbox сможет анализировать их поведение. Если вы запретите доступ в интернет, компонент Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

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

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

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

1. В списке сетевых интерфейсов выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.

2. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Назначение адреса и маски сети управляющего интерфейса

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

1. В поле **Address** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.

2. В поле **Netmask** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.

3. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Настройка статического сетевого маршрута

► *Чтобы настроить статические сетевые маршруты, выполните следующие действия для каждого сетевого маршрута:*

1. В окне **IPv4 Routes** выберите **New**.
2. Нажмите на клавишу **ENTER**.

   Откроется окно **IPv4 Static Route**.
3. В поле **Address/Mask** введите IP-адрес и маску подсети, для которой вы хотите настроить сетевой маршрут.
4. В поле **Gateway** введите IP-адрес шлюза.
5. Нажмите на кнопку **Ok**.

Перейдите к настройке компонента Sandbox через веб-интерфейс (стр. 164).

Установка и настройка компонентов Central Node и Sensor на одном сервере

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

Если вы устанавливаете Kaspersky Anti Targeted Attack Platform в гипервизоре VMware ESXi и планируете, что программа будет получать зеркалированный трафик от нескольких виртуальных сетей, вам нужно произвести предварительную настройку ESX-сервера, на котором вы хотите установить программу.

► *Чтобы произвести предварительную настройку ESX-сервера, выполните следующие действия в гипервизоре VMware ESXi:*

1. Запустите программу VMware vSphere Client.
2. В списке ESX-серверов выберите ESX-сервер, предварительную настройку которого вы хотите произвести.
3. Нажатием правой кнопки мыши раскройте меню.
4. Выберите пункт меню **Configuration**.

   Откроется окно изменения конфигурации ESX-сервера.
5. В разделе **Hardware** выберите пункт **Networking**.

   Откроется окно изменения параметров.
6. На закладке **Ports** выберите раздел **VM Network**.

   Откроется окно **VM Network Properties**.
7. На закладке **General** в списке **VLAN ID (Optional)** выберите значение **All**.
8. Нажмите на кнопку **Ok**.

Программа сможет получать зеркалированный трафик от нескольких виртуальных сетей.

Шаг 1. Начало установки компонентов Central Node и Sensor и выбор роли сервера

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

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

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

   Откроется окно начала установки программы.
3. Нажмите на кнопку **OK**.

   Откроется окно выбора роли сервера.
4. Выберите **Act as Central Node**.

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

При необходимости использования компонента Central Node отдельно от компонента Sensor пропускайте шаги по настройке компонента Sensor при установке компонентов Central Node и Sensor (стр. 101).

5. Откроется окно подтверждения выбора роли сервера.

   Нажмите на кнопку **Confirm role**.

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

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности

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

Также вам нужно просмотреть Политику конфиденциальности и принять ее условия.

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

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

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

2. Нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения.

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

   Откроется окно с текстом Политики конфиденциальности.

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

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонентов Central Node и Sensor

► *Чтобы выбрать диск для установки компонентов Central Node и Sensor, выполните следующие действия:*

1. В окне **Select device** в списке дисков выберите диск, на который вы хотите установить компоненты Central Node и Sensor.
2. Нажмите на клавишу **ENTER**.
3. Откроется окно **Select action**.
4. Выберите **Install**.

5. Нажмите на клавишу **ENTER**.

   Откроется окно с предупреждением о том, что диск будет отформатирован.

6. Нажмите на кнопку **Install**.

Произойдет форматирование диска. Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 4. Создание учетной записи для работы в меню администратора и в консоли управления сервером

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

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

   Пароль должен удовлетворять следующим требованиям:

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

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

Мастер установки перейдет к следующему шагу.

Шаг 5. Назначение имени хоста

► *Чтобы назначить имя хоста программы для использования DNS-серверами, выполните следующие действия:*

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

   Указывайте имя сервера в формате FQDN (например, host.domain.com или host.domain.subdomain.com).

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Первоначальное включение сетевого интерфейса

Необходимо включить сетевые интерфейсы для последующей настройки их параметров.

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

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

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

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

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

Мастер установки перейдет к следующему шагу.

Шаг 7. Настройка сетевого маршрута для использования по умолчанию

На этом шаге настройте сетевой маршрут, который программа будет использовать по умолчанию. Вы можете настроить сетевой маршрут с помощью DHCP-сервера или настроить статический сетевой маршрут.

Настройка сетевого маршрута с помощью DHCP-сервера

► *Чтобы настроить сетевой маршрут с помощью DHCP-сервера, выполните следующие действия:*

1. В списке **Default route** выберите **Interface**.
2. Нажмите на клавишу **ENTER**.

   Откроется список сетевых интерфейсов.
3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
4. Нажмите на клавишу **ENTER**.

   Мастер установки вернется к окну настройки сетевого маршрута.

   Напротив названия параметра **Gateway** отобразится значение **dhcp**.
5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Настройка статического сетевого маршрута

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

1. В списке **Default route** выберите **Interface**.
2. Нажмите на клавишу **ENTER**.

Откроется список сетевых интерфейсов.

3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
4. Нажмите на клавишу **ENTER**.

   Мастер установки вернется к окну настройки сетевого маршрута.
5. Выберите параметр **Gateway**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения настройки статического сетевого маршрута.
7. Нажмите на кнопку **Yes**.

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

   Мастер установки вернется к окну настройки сетевого маршрута.

   Напротив названия параметра **Gateway** отобразится статический адрес шлюза, который вы назначили.
10. Выберите **Continue**.
11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка параметров DNS

На этом шаге настройте параметры DNS для работы серверов с компонентами программы. Вы можете настроить назначение DNS-адресов с помощью DHCP-сервера или настроить назначение статических DNS-адресов.

Назначение DNS-адресов с помощью DHCP-сервера

Вам может понадобиться использовать DHCP-сервер для назначения DNS-адресов, если вы настраиваете Kaspersky Anti Targeted Attack Platform в тестовом режиме.

► *Чтобы назначить DNS-адреса с помощью DHCP-сервера, выполните следующие действия:*

1. В окне **Obtain DNS addresses over DHCP** выберите имя вашего сетевого интерфейса.
2. Нажмите на клавишу **ENTER**.

   Отобразится окно настройки параметров DNS.
3. Убедитесь, что параметры **Search list**, **Primary DNS**, **Secondary DNS** имеют значение **dhcp**.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Назначение статических DNS-адресов

Рекомендуется назначить статические DNS-адреса, если вы настраиваете Kaspersky Anti Targeted Attack

Platform не в тестовом режиме.

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

1. В окне **Select action - Resolver** выберите **no**.
2. Нажмите на клавишу **ENTER**.

   Отобразится окно настройки параметров DNS.
3. Выберите любой параметр.

   Например, параметр **Search list**.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно ввода статических DNS-адресов.
5. В поле **Search list** введите DNS-суффикс, который вы хотите использовать в Kaspersky Anti Targeted Attack Platform.

   Например, example.com.
6. В поле **Primary** введите IP-адрес основного DNS-сервера в формате IPv4.
7. В поле **Secondary** введите IP-адрес дополнительного DNS-сервера в формате IPv4.
8. Нажмите на кнопку **Ok**.

   Отобразится окно настройки параметров DNS с установленными статическими параметрами DNS.
9. Проверьте правильность установленных параметров DNS.
10. Выберите **Continue**.
11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Настройка параметров соединения с прокси-сервером

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

Включение и отключение использования прокси-сервера

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

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

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

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

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

Настройка параметров соединения с прокси-сервером

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

1. В окне **Select Action - Proxy** выберите любой параметр.

   Например, выберите параметр **Host**.

2. Нажмите на клавишу **ENTER**.

   Отобразится окно настройки параметров соединения с прокси-сервером.

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

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

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

4. Нажмите на кнопку **Ok**.

   Окно настройки параметров соединения с прокси-сервером закроется.

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

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

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

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

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

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

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

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

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

Мастер установки перейдет к следующему шагу.

Шаг 10. Установка часового пояса

► *Чтобы установить часовой пояс для Kaspersky Anti Targeted Attack Platform, выполните следующие действия:*

1. В окне **Select Timezone - Select Country** выберите страну из списка.

   Например, выберите **Russia**.
2. Нажмите на клавишу **ENTER**.

   Отобразится список часовых поясов, доступных для выбранной страны.
3. Выберите часовой пояс.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения выбора часового пояса.
5. Если часовой пояс выбран верно, нажмите на кнопку **Yes**.

Мастер установки перейдет к следующему шагу.

Шаг 11. Настройка синхронизации времени с NTP-сервером

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

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

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

   Откроется окно **Set the system clock manually**.
2. Нажмите на одну из следующих кнопок:

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

   Мастер установки программы сразу перейдет к следующему шагу.

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

   Откроется окно **Set the system clock**, в котором вы можете настроить время.
3. По окончании настройки времени выберите **Continue**.
4. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

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

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

   Откроется окно **ConСхема NTP servers**.
2. В окне **ConСхема NTP servers** выберите **New**.

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

Окно **Add NTP server** закроется.

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

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

Мастер установки перейдет к следующему шагу.

Шаг 12. Подключение к серверу с компонентом Sandbox

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

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

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

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

Мастер установки перейдет к следующему шагу.

Шаг 13. Выделение диска для базы данных компонента Targeted Attack Analyzer

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

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

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

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

Мастер установки перейдет к следующему шагу.

► *Чтобы выделить диск, выполните следующие действия:*

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

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

Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 14. Создание учетной записи локального администратора веб-интерфейса

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

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

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

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

Мастер установки перейдет к следующему шагу.

Шаг 15. Настройка получения зеркалированного трафика со SPAN-портов

На этом шаге вы можете настроить получение зеркалированного трафика со SPAN-портов.

► *Чтобы отказаться от получения зеркалированного трафика со SPAN-портов,*

в окне **Enable SPAN traffic processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

► *Чтобы настроить получение зеркалированного трафика со SPAN-портов, выполните следующие действия:*

1. В окне **Enable SPAN traffic processing** нажмите на кнопку **Yes**.

   Откроется окно выбора сетевых интерфейсов.

   По умолчанию получение зеркалированного трафика со SPAN-портов всех интерфейсов отключено. Справа от названия сетевого интерфейса отображается значение **skip**.

2. Выберите сетевой интерфейс, с которого вы хотите настроить получение зеркалированного трафика.

   > Не настраивайте получение зеркалированного трафика с управляющего сетевого интерфейса сервера с компонентом Central Node.

3. Нажмите на клавишу **ENTER**.

   Получение зеркалированного трафика со SPAN-портов выбранного интерфейса включится. Справа от названия сетевого интерфейса отобразится значение **capture**.

4. Если вы хотите настроить получение зеркалированного трафика для других сетевых интерфейсов, повторите действия 2–3 для каждого из них.
5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 16. Настройка интеграции с прокси-сервером по протоколу ICAP

На этом шаге вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с прокси-сервером, использующимся в вашей организации, по протоколу ICAP.

► *Чтобы отказаться от интеграции Kaspersky Anti Targeted Attack Platform с прокси-сервером,*

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

Мастер установки перейдет к следующему шагу.

► *Чтобы включить интеграцию Kaspersky Anti Targeted Attack Platform с прокси-сервером, выполните следующие действия:*

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

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

Используйте этот URI-адрес для настройки интеграции с Kaspersky Anti Targeted Attack Platform по протоколу ICAP на прокси-сервере, использующемся в вашей организации.

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 17. Настройка интеграции с почтовым сервером по протоколу POP3

На этом шаге вы можете настроить интеграцию с почтовым сервером по протоколу POP3 после предварительной подготовки IT-инфраструктуры вашей организации (стр. 95).

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

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

Мастер установки перейдет к следующему шагу.

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

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

   Откроется окно настройки интеграции с почтовым сервером по протоколу POP3.

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

   Откроется окно **POP3 server**.

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

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

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

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

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

   Откроется окно **POP3 access**.

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

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

13. Выберите параметр **Check interval**.

14. Нажмите на клавишу **ENTER**.

    Откроется окно **Check interval**.

15. В поле **Check interval** введите частоту соединения с почтовым сервером в секундах.

16. Нажмите на кнопку **Ok**.

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

17. В разделе **Accepts certificates** настройте параметры TLS-шифрования соединения Kaspersky Anti Targeted Attack Platform с внешними почтовыми серверами по протоколу POP3.

    - Если вы хотите, чтобы программа принимала любые TLS-сертификаты при соединении с внешними почтовыми серверами, выполните следующие действия:

      a. Выберите вариант **any certificate**.

      b. Нажмите на клавишу **ENTER**, чтобы напротив варианта **any certificate** отобразилось значение **yes**.

    - Если вы хотите, чтобы программа принимала недоверенные самоподписанные TLS-сертификаты при соединении с внешними почтовыми серверами, выполните следующие действия:

      1. Выберите вариант **untrusted self-signed**.

      2. Нажмите на клавишу **ENTER**, чтобы напротив варианта **untrusted self-signed** отобразилось значение **yes**.

    - Если вы хотите, чтобы программа принимала только доверенные TLS-сертификаты при соединении с внешними почтовыми серверами, выполните следующие действия:

      a. Выберите вариант **any certificate**.

      b. Нажмите на клавишу **ENTER**, чтобы напротив варианта **any certificate** отобразилось значение **no**.

      c. Выберите вариант **untrusted self-signed**.

      d. Нажмите на клавишу **ENTER**, чтобы напротив варианта **untrusted self-signed** отобразилось значение **no**.

    При установке соединения с внешним почтовым сервером рекомендуется настроить прием только доверенных TLS-сертификатов. Прием недоверенных TLS-сертификатов не гарантирует защиту соединения от MITM-атак. Прием доверенных TLS-сертификатов также не полностью гарантирует защиту соединения от MITM-атак, но является самым безопасным из поддерживаемых способов интеграции с почтовым сервером по протоколу POP3.

18. При необходимости в разделе **Cipher list** измените параметры OpenSSL, используемые при установке соединения с почтовым сервером по протоколу POP3. Выполните действия:

    a. Выберите **edit**.

    b. Нажмите на клавишу **ENTER**.

       Откроется окно **Cipher list**.

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

19. Нажмите на кнопку **Ok**.

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

20. Выберите **Continue**.

21. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 18. Настройка интеграции с почтовым сервером по протоколу SMTP

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

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

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

Мастер установки перейдет к следующему шагу.

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

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

   Откроется окно настройки интеграции с почтовым сервером по протоколу SMTP.
2. Выберите параметр **Clients**.
3. Нажмите на клавишу **ENTER**.

   Откроется окно **ConСхема Networks**.
4. Выберите параметр **New**.
5. Нажмите на клавишу **ENTER**.
6. В поле **Network address** введите адрес почтового сервера, с которым Kaspersky Anti Targeted Attack Platform разрешено взаимодействовать по протоколу SMTP.

   Если вы оставите адрес почтового сервера пустым, Kaspersky Anti Targeted Attack Platform будет принимать сообщения от всех серверов.
7. Нажмите на кнопку **Ok**.
8. Выберите параметр **Domains**.
9. Нажмите на клавишу **ENTER**.

   Откроется окно **ConСхема domains**.
10. Выберите параметр **New**.
11. Нажмите на клавишу **ENTER**.
12. В поле **Domain** введите имя почтового домена или поддомена, на который администратор почтового сервера должен настроить отправку скрытой копии сообщений.

    Если вы оставите имя почтового домена пустым, Kaspersky Anti Targeted Attack Platform будет принимать сообщения, отправленные на любые адреса электронной почты.
13. Нажмите на кнопку **Ok**.
14. Выберите параметр **TLS encryption**.
15. Нажмите на клавишу **ENTER**.

    Откроется окно **Select TLS encryption level**.
16. Выберите один из следующих вариантов TLS-шифрования соединения с почтовым сервером по

протоколу SMTP:

- **none**, если вы не хотите устанавливать TLS-шифрование соединения.
- **optional**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform поддерживал TLS-шифрование соединения.
- **mandatory**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform требовал TLS-шифрования соединения от почтового сервера.

17. Нажмите на клавишу **ENTER**.
18. Выберите параметр **Client certs**.
19. Нажмите на клавишу **ENTER**.

    Откроется окно **Select TLS client certificates use**.
20. Выберите один из следующих вариантов проверки TLS-сертификата клиента при соединении с почтовым сервером по протоколу SMTP:
    - **ignore**, если вы не хотите проверять TLS-сертификат клиента.
    - **optional**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform поддерживал проверку TLS-сертификата клиента.
    - **mandatory**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform требовал TLS-сертификат клиента.
21. Выберите параметр **Message size**.
22. Нажмите на клавишу **ENTER**.

    Откроется окно **Message size limit**.
23. В поле **Message size limit** задайте максимальный размер принимаемого сообщения. Максимальный размер принимаемого сообщения не может быть больше 10 МБ.
24. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Установка и настройка компонента Sensor на отдельном сервере

Этот раздел представляет собой пошаговую инструкцию по установке и предварительной настройке компонента Sensor на отдельном сервере.

Если вы устанавливаете Kaspersky Anti Targeted Attack Platform в гипервизоре VMware ESXi и планируете, что программа будет получать зеркалированный трафик от нескольких виртуальных сетей, вам нужно произвести предварительную настройку ESX-сервера, на котором вы хотите установить программу.

► *Чтобы произвести предварительную настройку ESX-сервера, выполните следующие действия в гипервизоре VMware ESXi:*

1. Запустите программу VMware vSphere Client.
2. В списке ESX-серверов выберите ESX-сервер, предварительную настройку которого вы хотите произвести.
3. Нажатием правой кнопки мыши раскройте меню.
4. Выберите пункт меню **Configuration**.

   Откроется окно изменения конфигурации ESX-сервера.
5. В разделе **Hardware** выберите пункт **Networking**.

   Откроется окно изменения параметров.
6. На закладке **Ports** выберите раздел **VM Network**.

   Откроется окно **VM Network Properties**.
7. На закладке **General** в списке **VLAN ID (Optional)** выберите значение **All**.
8. Нажмите на кнопку **Ok**.

Программа сможет получать зеркалированный трафик от нескольких виртуальных сетей.

Шаг 1. Начало установки компонента Sensor и выбор роли сервера

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

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

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

   Откроется окно начала установки программы.
3. Нажмите на кнопку **OK**.

   Откроется окно выбора роли сервера.
4. Выберите **Act as Sensor**.

   Откроется окно подтверждения выбора роли сервера.
5. Нажмите на кнопку **Confirm role**.

Запустится мастер установки компонента Sensor на отдельном сервере.

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности

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

Также вам нужно просмотреть Политику конфиденциальности и принять ее условия.

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

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

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

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

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

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента Sensor

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

1. В окне **Select device** в списке дисков выберите диск, на который вы хотите установить компонент Sensor.
2. Нажмите на клавишу **ENTER**.
3. Откроется окно **Select action**.
4. Выберите **Install**.
5. Нажмите на клавишу **ENTER**.

   Откроется окно с предупреждением о том, что диск будет отформатирован.
6. Нажмите на кнопку **Install**.

Произойдет форматирование диска. Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 4. Создание учетной записи для работы в меню администратора и в консоли управления сервером

► *Чтобы создать учетную запись администратора для работы в меню администратора и в*

консоли управления сервером, выполните следующие действия:

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

   Пароль должен удовлетворять следующим требованиям:

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

Мастер установки перейдет к следующему шагу.

Шаг 5. Назначение имени хоста

► *Чтобы назначить имя хоста программы для использования DNS-серверами, выполните следующие действия:*

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

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

Мастер установки перейдет к следующему шагу.

Шаг 6. Первоначальное включение сетевого интерфейса

Необходимо включить сетевые интерфейсы для последующей настройки их параметров.

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

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

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

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

   Сетевой интерфейс будет включен.

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

Мастер установки перейдет к следующему шагу.

Шаг 7. Настройка сетевого маршрута для использования по умолчанию

На этом шаге настройте сетевой маршрут, который программа будет использовать по умолчанию. Вы можете настроить сетевой маршрут с помощью DHCP-сервера или настроить статический сетевой маршрут.

Настройка сетевого маршрута с помощью DHCP-сервера

► *Чтобы настроить сетевой маршрут с помощью DHCP-сервера, выполните следующие действия:*

1. В списке **Default route** выберите **Interface**.
2. Нажмите на клавишу **ENTER**.

   Откроется список сетевых интерфейсов.
3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
4. Нажмите на клавишу **ENTER**.

   Мастер установки вернется к окну настройки сетевого маршрута.

   Напротив названия параметра **Gateway** отобразится значение **dhcp**.
5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Настройка статического сетевого маршрута

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

1. В списке **Default route** выберите **Interface**.
2. Нажмите на клавишу **ENTER**.

   Откроется список сетевых интерфейсов.
3. Выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
4. Нажмите на клавишу **ENTER**.

   Мастер установки вернется к окну настройки сетевого маршрута.
5. Выберите параметр **Gateway**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно подтверждения настройки статического сетевого маршрута.
7. Нажмите на кнопку **Yes**.

Откроется окно ввода статического адреса шлюза.

8. В поле **Gateway** введите статический адрес шлюза.
9. Нажмите на кнопку **Ok**.

   Мастер установки вернется к окну настройки сетевого маршрута.

   Напротив названия параметра **Gateway** отобразится статический адрес шлюза, который вы назначили.
10. Выберите **Continue**.
11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка параметров DNS

На этом шаге настройте параметры DNS для работы серверов с компонентами программы. Вы можете настроить назначение DNS-адресов с помощью DHCP-сервера или настроить назначение статических DNS-адресов.

Назначение DNS-адресов с помощью DHCP-сервера

Вам может понадобиться использовать DHCP-сервер для назначения DNS-адресов, если вы настраиваете Kaspersky Anti Targeted Attack Platform в тестовом режиме.

► *Чтобы назначить DNS-адреса с помощью DHCP-сервера, выполните следующие действия:*

1. В окне **Obtain DNS addresses over DHCP** выберите имя вашего сетевого интерфейса.
2. Нажмите на клавишу **ENTER**.

   Отобразится окно настройки параметров DNS.
3. Убедитесь, что параметры **Search list**, **Primary DNS**, **Secondary DNS** имеют значение **dhcp**.
4. Выберите **Continue**.
5. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Назначение статических DNS-адресов

Рекомендуется назначить статические DNS-адреса, если вы настраиваете Kaspersky Anti Targeted Attack Platform не в тестовом режиме.

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

1. В окне **Select action - Resolver** выберите **no**.
2. Нажмите на клавишу **ENTER**.

   Отобразится окно настройки параметров DNS.
3. Выберите любой параметр.

Например, параметр **Search list**.

4. Нажмите на клавишу **ENTER**.

   Отобразится окно ввода статических DNS-адресов.

5. В поле **Search list** введите DNS-суффикс, который вы хотите использовать в Kaspersky Anti Targeted Attack Platform.

   Например, example.com.

6. В поле **Primary** введите IP-адрес основного DNS-сервера в формате IPv4.
7. В поле **Secondary** введите IP-адрес дополнительного DNS-сервера в формате IPv4.
8. Нажмите на кнопку **Ok**.

   Отобразится окно настройки параметров DNS с установленными статическими параметрами DNS.

9. Проверьте правильность установленных параметров DNS.
10. Выберите **Continue**.
11. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Настройка параметров соединения с прокси-сервером

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

Включение и отключение использования прокси-сервера

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

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

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

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

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

Настройка параметров соединения с прокси-сервером

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

1. В окне **Select Action - Proxy** выберите любой параметр.

   Например, выберите параметр **Host**.

2. Нажмите на клавишу **ENTER**.

   Отобразится окно настройки параметров соединения с прокси-сервером.

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

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

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

4. Нажмите на кнопку **Ok**.

   Окно настройки параметров соединения с прокси-сервером закроется.

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

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

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

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

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

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

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

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

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

Мастер установки перейдет к следующему шагу.

Шаг 10. Установка часового пояса

► *Чтобы установить часовой пояс для Kaspersky Anti Targeted Attack Platform, выполните следующие действия:*

1. В окне **Select Timezone - Select Country** выберите страну из списка.

   Например, выберите **Russia**.

2. Нажмите на клавишу **ENTER**.

   Отобразится список часовых поясов, доступных для выбранной страны.

3. Выберите часовой пояс.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения выбора часового пояса.

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

Мастер установки перейдет к следующему шагу.

Шаг 11. Настройка синхронизации времени с NTP-сервером

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

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

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

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

2. Нажмите на одну из следующих кнопок:

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

   Мастер установки программы сразу перейдет к следующему шагу.

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

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

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

Мастер установки перейдет к следующему шагу.

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

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

   Откроется окно **ConCхема NTP servers**.

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

   Откроется окно **Add NTP server**.

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

   Окно **Add NTP server** закроется.

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

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

Мастер установки перейдет к следующему шагу.

Шаг 12. Подключение к серверу с компонентом Central Node

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

1. В поле **Central Node** введите IP-адрес или URL-адрес сервера с компонентом Central Node.
2. Нажмите на кнопку **Ok**.

   Откроется окно **Central Node certificate**.
3. Сверьте отпечаток сертификата с отпечатком сертификата на сервере с компонентом Central Node.
4. Если отпечатки сертификатов совпадают, нажмите на кнопку **Accept**.

   Откроется окно **Central Node connection**.

   Убедитесь, что значения параметров подключения к серверу Central Node верны.
5. Нажмите на кнопку **Ok**.

> Для завершения подключения компонента Sensor к серверу с компонентом Central Node вам потребуется принять запрос на подключение от этого компонента Sensor в веб-интерфейсе сервера с компонентом Central Node (стр. 215). Вы можете сделать это в любое время независимо от хода установки и настройки компонента Sensor в мастере установки.

Мастер установки перейдет к следующему шагу.

Шаг 13. Выбор сервера Central Node в качестве источника обновления баз компонента Sensor

► *Чтобы выбрать сервер Central Node в качестве источника обновления баз компонента Sensor,*

в окне **Update source** нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 14. Настройка получения зеркалированного трафика со SPAN-портов

На этом шаге вы можете настроить получение зеркалированного трафика со SPAN-портов.

► *Чтобы отказаться от получения зеркалированного трафика со SPAN-портов,*

в окне **Enable SPAN traffic processing** нажмите на кнопку **No**.

Мастер установки перейдет к следующему шагу.

► *Чтобы настроить получение зеркалированного трафика со SPAN-портов, выполните*

следующие действия:

1. В окне **Enable SPAN traffic processing** нажмите на кнопку **Yes**.

   Откроется окно выбора сетевых интерфейсов.

   По умолчанию получение зеркалированного трафика со SPAN-портов всех интерфейсов отключено. Справа от названия сетевого интерфейса отображается значение **skip**.

2. Выберите сетевой интерфейс, с которого вы хотите настроить получение зеркалированного трафика.

   > Не настраивайте получение зеркалированного трафика с управляющего сетевого интерфейса сервера с компонентом Central Node.

3. Нажмите на клавишу **ENTER**.

   Получение зеркалированного трафика со SPAN-портов выбранного интерфейса включится. Справа от названия сетевого интерфейса отобразится значение **capture**.

4. Если вы хотите настроить получение зеркалированного трафика для других сетевых интерфейсов, повторите действия 2–3 для каждого из них.
5. Выберите **Continue**.
6. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 15. Настройка интеграции с прокси-сервером по протоколу ICAP

На этом шаге вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с прокси-сервером, использующимся в вашей организации, по протоколу ICAP.

► *Чтобы отказаться от интеграции Kaspersky Anti Targeted Attack Platform с прокси-сервером,*

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

Мастер установки перейдет к следующему шагу.

► *Чтобы включить интеграцию Kaspersky Anti Targeted Attack Platform с прокси-сервером, выполните следующие действия:*

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

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

   Используйте этот URI-адрес для настройки интеграции с Kaspersky Anti Targeted Attack Platform по протоколу ICAP на прокси-сервере, использующемся в вашей организации.

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 16. Настройка интеграции с почтовым сервером по протоколу POP3

На этом шаге вы можете настроить интеграцию с почтовым сервером по протоколу POP3 после

предварительной подготовки IT-инфраструктуры вашей организации (стр. 95).

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

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

Мастер установки перейдет к следующему шагу.

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

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

   Откроется окно настройки интеграции с почтовым сервером по протоколу POP3.
2. Выберите параметр **Server**.
3. Нажмите на клавишу **ENTER**.

   Откроется окно **POP3 server**.
4. В поле **Server** введите IP-адрес почтового сервера, с которым вы хотите настроить интеграцию.
5. Нажмите на кнопку **Ok**.

   Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.
6. Выберите параметр **Encrypted**.
7. Нажмите на клавишу **ENTER**.
   - Если шифрованное соединение с почтовым сервером было отключено, оно включится. Напротив названия параметра **Encrypted** отобразится значение **yes**.
   - Если шифрованное соединение с почтовым сервером было включено, оно отключится. Напротив названия параметра **Encrypted** отобразится значение **no**.
8. Выберите параметр **Username**.
9. Нажмите на клавишу **ENTER**.

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

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

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

    Мастер установки вернется к окну настройки интеграции с почтовым сервером по протоколу POP3.
17. В разделе **Accepts certificates** настройте параметры TLS-шифрования соединения Kaspersky Anti Targeted Attack Platform с внешними почтовыми серверами по протоколу POP3.
    - Если вы хотите, чтобы программа принимала любые TLS-сертификаты при соединении с

внешними почтовыми серверами, выполните следующие действия:

a. Выберите вариант **any certificate**.

b. Нажмите на клавишу **ENTER**, чтобы напротив варианта **any certificate** отобразилось значение **yes**.

- Если вы хотите, чтобы программа принимала недоверенные самоподписанные TLS-сертификаты при соединении с внешними почтовыми серверами, выполните следующие действия:

  1. Выберите вариант **untrusted self-signed**.
  2. Нажмите на клавишу **ENTER**, чтобы напротив варианта **untrusted self-signed** отобразилось значение **yes**.

- Если вы хотите, чтобы программа принимала только доверенные TLS-сертификаты при соединении с внешними почтовыми серверами, выполните следующие действия:

  a. Выберите вариант **any certificate**.

  b. Нажмите на клавишу **ENTER**, чтобы напротив варианта **any certificate** отобразилось значение **no**.

  c. Выберите вариант **untrusted self-signed**.

  d. Нажмите на клавишу **ENTER**, чтобы напротив варианта **untrusted self-signed** отобразилось значение **no**.

При установке соединения с внешним почтовым сервером рекомендуется настроить прием только доверенных TLS-сертификатов. Прием недоверенных TLS-сертификатов не гарантирует защиту соединения от MITM-атак. Прием доверенных TLS-сертификатов также не полностью гарантирует защиту соединения от MITM-атак, но является самым безопасным из поддерживаемых способов интеграции с почтовым сервером по протоколу POP3.

18. При необходимости в разделе **Cipher list** измените параметры OpenSSL, используемые при установке соединения с почтовым сервером по протоколу POP3. Выполните действия:

    a. Выберите **edit**.

    b. Нажмите на клавишу **ENTER**.

    Откроется окно **Cipher list**.

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

19. Нажмите на кнопку **Ok**.

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

20. Выберите **Continue**.

21. Нажмите на клавишу **ENTER**.

Мастер установки перейдет к следующему шагу.

Шаг 17. Настройка интеграции с почтовым сервером по протоколу SMTP

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

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

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

Мастер установки перейдет к следующему шагу.

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

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

   Откроется окно настройки интеграции с почтовым сервером по протоколу SMTP.
2. Выберите параметр **Clients**.
3. Нажмите на клавишу **ENTER**.

   Откроется окно **ConСхема Networks**.
4. Выберите параметр **New**.
5. Нажмите на клавишу **ENTER**.
6. В поле **Network address** введите адрес почтового сервера, с которым Kaspersky Anti Targeted Attack Platform разрешено взаимодействовать по протоколу SMTP.

   Если вы оставите адрес почтового сервера пустым, Kaspersky Anti Targeted Attack Platform будет принимать сообщения от всех серверов.
7. Нажмите на кнопку **Ok**.
8. Выберите параметр **Domains**.
9. Нажмите на клавишу **ENTER**.

   Откроется окно **ConСхема domains**.
10. Выберите параметр **New**.
11. Нажмите на клавишу **ENTER**.
12. В поле **Domain** введите имя почтового домена или поддомена, на который администратор почтового сервера должен настроить отправку скрытой копии сообщений.

    Если вы оставите имя почтового домена пустым, Kaspersky Anti Targeted Attack Platform будет принимать сообщения, отправленные на любые адреса электронной почты.
13. Нажмите на кнопку **Ok**.
14. Выберите параметр **TLS encryption**.
15. Нажмите на клавишу **ENTER**.

    Откроется окно **Select TLS encryption level**.
16. Выберите один из следующих вариантов TLS-шифрования соединения с почтовым сервером по протоколу SMTP:

    - **none**, если вы не хотите устанавливать TLS-шифрование соединения.
    - **optional**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform поддерживал TLS-шифрование соединения.
    - **mandatory**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform требовал TLS-шифрования соединения от почтового сервера.

17. Нажмите на клавишу **ENTER**.
18. Выберите параметр **Client certs**.
19. Нажмите на клавишу **ENTER**.

    Откроется окно **Select TLS client certificates use**.
20. Выберите один из следующих вариантов проверки TLS-сертификата клиента при соединении с почтовым сервером по протоколу SMTP:
    - **ignore**, если вы не хотите проверять TLS-сертификат клиента.
    - **optional**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform поддерживал проверку TLS-сертификата клиента.
    - **mandatory**, если вы хотите, чтобы сервер Kaspersky Anti Targeted Attack Platform требовал TLS-сертификат клиента.
21. Выберите параметр **Message size**.
22. Нажмите на клавишу **ENTER**.

    Откроется окно **Message size limit**.
23. В поле **Message size limit** задайте максимальный размер принимаемого сообщения. Максимальный размер принимаемого сообщения не может быть больше 10 МБ.
24. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Установка и удаление компонента Endpoint Sensors

Этот раздел представляет собой инструкцию по установке и удалению компонента Endpoint Sensors.

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

Особенности установки компонента Endpoint Sensors при совместной работе программы с KES

Совместимость KES и компонента Endpoint Sensors версии 3.5

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

1. Отключите компонент Endpoint Sensors в составе программы KES.

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

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

Совместимость KES и отдельного компонента Endpoint Sensors версии 3.6

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

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

Таблица 9. Сценарии установки KES и отдельного компонента Endpoint Sensors

Версия KES	Установка отдельного компонента Endpoint Sensors после установки KES	Установка KES после установки отдельного компонента Endpoint Sensors
• KES10 SP1 MR3 • KES10 SP1 MR4 • KES 10 SP2 • KES 10 SP2 MR1 • KES 10 SP2 MR2 • KES 10 SP2 MR3	Стандартная процедура установки.	Стандартная процедура установки.

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

Установка компонента Endpoint Sensors

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

► *Чтобы установить компонент Endpoint Sensors на компьютеры локальной сети организации, с которых Kaspersky Anti Targeted Attack Platform получает и обрабатывает данные, выполните следующие действия:*

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

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

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

4. Нажмите на клавишу **ENTER**.

Установка компонента Endpoint Sensors завершится.

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

Подготовка SSL-соединения к обмену данными между компонентами Endpoint Sensors и Central Node

Компонент Endpoint Sensors наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами на компьютерах, на которых он установлен, и отправляет данные наблюдения на сервер с компонентом Central Node. По результатам проверки этих данных компонентом Central Node компонент Endpoint Sensors также может отправить файлы, связанные с обнаруженными событиями, на сервер с компонентом Central Node.

Чтобы компонент Endpoint Sensors мог отправлять файлы на сервер с компонентом Central Node, вам нужно усилить безопасность SSL-соединения компонента Endpoint Sensors с сервером Central Node.

Вы можете усилить безопасность SSL-соединения компьютеров с компонентом Endpoint Sensors с сервером Central Node при соблюдении следующих условий конфигурации локальной сети вашей организации:

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

Выполняйте действия по усилению безопасности SSL-соединения компьютеров с компонентом Endpoint Sensors с сервером Central Node в следующем порядке:

1. Скачайте SSL-сертификат с сервера с компонентом Central Node (стр. 132).

   Вы можете скачать сертификат, автоматически созданный на сервере с компонентом Central Node в процессе установки программы, созданный на сервере с компонентом Central Node вручную (стр. 133) или созданный самостоятельно и загруженный на сервер с компонентом Central Node (стр. 133).

2. Подготовьте SSL-сертификат и загрузите его в Active Directory (стр. 135).

Скачивание SSL-сертификата с сервера с компонентом Central Node

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

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

1. Выполните команду `scp admin@<IP-адрес сервера с компонентом Central Node>:ssl/kata.crt .`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Central Node, заданный при установке компонента Central Node.

SSL-сертификат будет загружен с сервера с компонентом Central Node в текущую директорию.

Создание SSL-сертификата на сервере с компонентом Central Node

► *Чтобы создать SSL-сертификат на сервере с компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Central Node (стр. 151):*

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

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

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

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

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

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

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

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

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

Загрузка самостоятельно подготовленного SSL-сертификата на сервер с компонентом Central Node

Вы можете самостоятельно подготовить SSL-сертификат и загрузить его на сервер с компонентом Central Node по протоколу SCP. Подробнее о способах загрузки файлов по протоколу SCP см. в документации к операционной системе, установленной на том компьютере, с которого вы хотите загрузить SSL-сертификат.

Файл SSL-сертификата, предназначенный для загрузки на сервер с компонентом Central Node, должен удовлетворять следующим требованиям:

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

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

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

1. Выполните команду `scp kata.pem admin@<IP-адрес сервера с компонентом Central Node>:`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Central Node, заданный при установке компонента Central Node.

SSL-сертификат будет загружен на сервер с компонентом Central Node.

► *Чтобы применить загруженный SSL-сертификат на сервере с компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Central Node (стр. 151):*

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

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

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

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

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

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

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

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

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

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

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

Подготовка и загрузка SSL-сертификата в Active Directory

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

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

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

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

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

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

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

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

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

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

Удаление компонента Endpoint Sensors

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

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

При удалении компонента Endpoint Sensors удаляются следующие данные:

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

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

Настройка перенаправления трафика с компонентов Endpoint Sensors на компонент Sensor

Вы можете использовать сервер с компонентом Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Sensors и компонентом Central Node, чтобы снизить нагрузку на компонент Central Node.

При настройке перенаправления трафика учитывайте следующие ограничения:

- Максимальный объем входящего трафика для компонента Sensor не должен превышать 1 Гбит/с.
- Максимальное количество компьютеров с компонентом Endpoint Sensors составляет 1000 шт.
- Рекомендуемая ширина канала между серверами с компонентами Central Node и Sensor составляет 15% от трафика на SPAN-порте.
- Максимально допустимые потери пакетов, пересылаемых между серверами с компонентами Sensor и Central Node, составляют 10% при задержке отправки пакетов до 100 мс.

Выполняйте действия по усилению безопасности SSL-соединения сервера с компонентом Sensor с сервером Central Node аналогично действиям с компонентом Endpoint Sensors и компонентом Central Node в следующем порядке:

1. Используйте сертификат, автоматически созданный в процессе установки программы, созданный на сервере с компонентом Sensor вручную (стр. 133) или созданный самостоятельно и загруженный на сервер с компонентом Sensor (стр. 133).
2. Подготовьте SSL-сертификат и загрузите его в Active Directory (стр. 135).

Вы можете использовать компонент Sensor в качестве прокси-сервера, только если компоненты Sensor и Central Node расположены на разных серверах.
Если вы используете компонент Sensor в качестве прокси-сервера, убедитесь, что при настройке параметров компонента Endpoint Sensors вместо IP-адреса Central Node вы указали IP-адрес компонента Sensor.

Включение и отключение перенаправления трафика с компонентов Endpoint Sensors

► *Чтобы включить или отключить использование компонента Sensor в качестве прокси-сервера при обмене данными между компонентами Endpoint Sensors и компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Sensor (стр. 151):*

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

   Откроется следующее окно меню администратора.
3. Выберите пункт **ConСхема Central Node**.
4. Нажмите на клавишу **ENTER**.
5. В открывшемся окне укажите IP-адрес сервера с компонентом Central Node.
6. Нажмите на кнопку **Ok**.

Откроется окно с информацией о сертификате компонента Central Node.

7. Убедитесь, что отображаемый сертификат совпадает с сертификатом компонента Central Node, который вы скачали.
8. Нажмите на кнопку **Accept**.
9. Если соединение с компонентом Central Node уже установлено или запрос на авторизацию отправлен, в открывшемся окне подтверждения действия нажмите на кнопку **Yes**.
10. В открывшемся окне **Update source** выполните одно из следующих действий:
    - Если вы хотите использовать сервер с компонентом Central Node в качестве источника обновления баз программы, нажмите на кнопку **Yes**.
    - Если вы не хотите использовать сервер с компонентом Central Node в качестве источника обновления баз программы, нажмите на кнопку **No**.
11. Если вы хотите использовать компонент Sensor в качестве прокси-сервера, в открывшемся окне **Enable Proxy to Central Node** нажмите на кнопку **Yes**.

    Использование компонента Sensor в качестве прокси-сервера будет включено после подтверждения авторизации на сервере с компонентом Central Node.
12. Если вы уже используете компонент Sensor в качестве прокси-сервера и хотите отключить его, в открывшемся окне **Proxy to Central Node** нажмите на кнопку **Yes**.

    Использование компонента Sensor в качестве прокси-сервера будет отключено после подтверждения авторизации на сервере с компонентом Central Node.

Авторизация компонента Sensor на сервере с компонентом Central Node

► *Чтобы авторизовать компонент Sensor на сервере с компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Central Node (стр. 151):*

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

   Откроется следующее окно меню администратора.
3. Выберите пункт **ConСхема Sensor connections**.

   Откроется окно со списком запросов на авторизацию от серверов с компонентом Sensor.
4. В нижней части окна выберите IP-адрес сервера с компонентом Sensor, запрос на авторизацию от которого вы хотите подтвердить или отклонить.

   Откроется окно подтверждения авторизации.
5. Если вы хотите авторизовать выбранный сервер с компонентом Sensor, выберите пункт **Accept Sensor**.

   Запрос на авторизацию будет подтвержден.
6. Если вы хотите отклонить авторизацию выбранного сервера с компонентом Sensor, выберите пункт **Reject Sensor**.

   Запрос на авторизацию будет отклонен.

Управление компонентами Endpoint Sensors в Kaspersky Security Center

Вы можете устанавливать, удалять и удаленно управлять компонентами Endpoint Sensors из консоли Kaspersky Security Center (далее также "консоль KSC").

В Kaspersky Security Center версии 11 также есть возможность работать в веб-консоли.

Подробную информацию о работе в консоли и в веб-консоли KSC см. в *Справке Kaspersky Security Center*.

Если у вас установлен компонент Endpoint Sensors в составе Kaspersky Endpoint Security, вам не нужно создавать установочный пакет, устанавливать или удалять компонент Endpoint Sensors.

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

Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Справки Kaspersky Endpoint Security*.

Создание установочного пакета Endpoint Sensors

Для создания установочного пакета используйте дистрибутив компонента Endpoint Sensors (файл с расширением msi, входящий в комплект поставки).

Если у вас установлен компонент Endpoint Sensors в составе KES, вам не нужно дополнительно создавать установочный пакет и устанавливать или удалять компонент Endpoint Sensors.
Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Справки Kaspersky Endpoint Security*.

► *Чтобы создать установочный пакет для удаленной установки компонента Endpoint Sensors, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе с дополнительными параметрами выберите подраздел с установочными пакетами.
4. Запустите создание установочного пакета.

   Откроется окно мастера создания установочного пакета.
5. Если вы используете программу Kaspersky Security Center версии 10 SP3 и позже, выполните следующие действия:

   a. В окне мастера создания установочного пакета выберите установочный пакет программы "Лаборатории Касперского".

> Не рекомендуется выбирать создание установочного пакета сторонней программы, так как в этом случае некоторые функции удаленного управления компонентом Endpoint Sensors будут недоступны.

b. Укажите путь к файлу в формате KUD и имя нового установочного пакета.

c. Ознакомьтесь с Лицензионным соглашением на этот компонент.

Внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми его пунктами, примите условия Лицензионного соглашения.

После этого создание установочного пакета будет продолжено. В процессе создания установочного пакета в программу Kaspersky Security Center будет установлен плагин для управления компонентом Endpoint Sensors, если вы не установили его ранее.

d. Укажите адрес и порт сервера с компонентом Central Node, а также статус самозащиты.

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

Значения по умолчанию: порт 443, адрес сервера не задан, самозащита включена.

> Самозащита запускает механизм защиты компонента Endpoint Sensors от изменения или удаления собственных файлов на диске, процессов в памяти и записей в системном реестре. Изменить статус самозащиты компонента Endpoint Sensors в дальнейшем можно только при переустановке компонента.

6. Если вы используете программу Kaspersky Security Center версии 10 SP2 MR1 или 10 SP2, в окне мастера создания установочного пакета выберите создание установочного пакета сторонней программы и укажите следующие параметры в командной строке:

- `SELFDEFENSE=On/Off` – статус самозащиты.

  По умолчанию самозащита включена.

  > Самозащита запускает механизм защиты компонента Endpoint Sensors от изменения или удаления собственных файлов на диске, процессов в памяти и записей в системном реестре. Изменить статус самозащиты компонента Endpoint Sensors в дальнейшем можно только при переустановке компонента.

- `SERVER=<адрес сервера>` – адрес сервера с компонентом Central Node.

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

  По умолчанию адрес сервера не задан.

- `acceptEULA=1` – принятие условий Лицензионного соглашения.

Вы можете ознакомиться с условиями Лицензионного соглашения, прочитав документ license.txt. Этот документ включен в комплект поставки программы. Если вы согласны со всеми пунктами Лицензионного соглашения, примите условия Лицензионного соглашения.

- `MESSAGEQUEUEPRINTMESSAGESTOLOG=1` – запись событий в журнал на сервере с компонентом Central Node.

  Необязательный параметр.

  Постоянное использование записи событий в журнал приводит к быстрому заполнению свободного места на диске. Используйте запись событий в журнал только в случае необходимости.

  Также вы можете указать следующие параметры записи событий в журнал:

  - `TRACELEVEL=500`, если вы хотите записывать в журнал только ошибки.
  - `TRACELEVEL=800`, если вы хотите использовать запись событий в журнал в режиме отладки.

О настройке дополнительных параметров вы можете узнать, обратившись в Службу технической поддержки.

После завершения работы мастера созданный установочный пакет будет отображаться в рабочей области папки с установочными пакетами.

Удаленная установка компонента Endpoint Sensors

Если у вас установлен компонент Endpoint Sensors в составе KES, вам не нужно дополнительно создавать установочный пакет и устанавливать или удалять компонент Endpoint Sensors.
Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Справки Kaspersky Endpoint Security*.
Перед установкой новой версии компонента Endpoint Sensors убедитесь, что на локальном компьютере не установлена предыдущая версия этого компонента.

Вы можете удаленно установить компонент Endpoint Sensors на компьютер с помощью программы Kaspersky Security Center 11, Kaspersky Security Center 10 SP3, Kaspersky Security Center 10 SP2 MR1 или Kaspersky Security Center 10 SP2.

Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Справки Kaspersky Endpoint Security*.

► *Чтобы удаленно установить компонент Endpoint Sensors на компьютеры локальной сети организации, выполните следующие действия:*

1. Откройте консоль KSC.

2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC выберите раздел с задачами.
4. В рабочей области выберите создание задачи.

   Запустится мастер создания задачи.
5. В мастере создания задачи выберите создание задачи удаленной установки приложения.
6. Выберите группу администрирования или отдельные компьютеры, на которые вы хотите установить компонент Endpoint Sensors.
7. Оставьте без изменений значения параметров по умолчанию.

В результате работы мастера создания задачи будет создана задача удаленной установки. Созданная задача разместится в папке с задачами или добавится к задачам группы администрирования, для которой она была создана.

Удаленное изменение параметров компонента Endpoint Sensors

Вы можете удаленно изменить параметры компонента Endpoint Sensors, переустановив его на компьютерах локальной сети организации.

► *Чтобы удаленно изменить параметры компонента Endpoint Sensors на компьютерах локальной сети организации, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе с дополнительными параметрами выберите подраздел с установочными пакетами.
4. Запустите создание установочного пакета.

   Откроется окно мастера создания установочного пакета.
5. Если вы используете программу Kaspersky Security Center 11 или Kaspersky Security Center 10 SP3, выполните следующие действия:
   a. В окне мастера создания установочного пакета выберите установочный пакет программы "Лаборатории Касперского".
   b. Укажите путь к файлу в формате KUD и имя нового установочного пакета.
   c. Ознакомьтесь с Лицензионным соглашением на этот компонент.

      Внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми его пунктами, примите условия Лицензионного соглашения.

      После этого создание установочного пакета будет продолжено. В процессе создания установочного пакета в программу Kaspersky Security Center будет установлен плагин для управления компонентом Endpoint Sensors, если вы не установили его ранее.
   d. Укажите адрес и порт сервера с компонентом Central Node, а также статус самозащиты.

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

Значения по умолчанию: порт 443, адрес сервера не задан, самозащита включена.

> Самозащита запускает механизм защиты компонента Endpoint Sensors от изменения или удаления собственных файлов на диске, процессов в памяти и записей в системном реестре. Изменить статус самозащиты компонента Endpoint Sensors в дальнейшем можно только при переустановке компонента.

6. Если вы используете программу Kaspersky Security Center 10 SP2 MR1 или Kaspersky Security Center 10 SP2, в окне мастера создания установочного пакета выберите создание установочного пакета сторонней программы и укажите следующие параметры в командной строке:

   - `SELFDEFENSE=On/Off` – статус самозащиты.

     По умолчанию самозащита включена.

     > Самозащита запускает механизм защиты компонента Endpoint Sensors от изменения или удаления собственных файлов на диске, процессов в памяти и записей в системном реестре. Изменить статус самозащиты компонента Endpoint Sensors в дальнейшем можно только при переустановке компонента.

   - `SERVER=<адрес сервера>` – адрес сервера с компонентом Central Node.

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

     По умолчанию адрес сервера не задан.

   - `acceptEULA=1` – принятие условий Лицензионного соглашения.

     > Внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми его пунктами, примите условия Лицензионного соглашения.

   - `MESSAGEQUEUEPRINTMESSAGESTOLOG=1` – запись событий в журнал на сервере с компонентом Central Node.

     Необязательный параметр.

     > Постоянное использование записи событий в журнал приводит к быстрому заполнению свободного места на диске. Используйте запись событий в журнал только в случае необходимости.

     Также вы можете указать следующие параметры записи событий в журнал:

     - `TRACELEVEL=500`, если вы хотите записывать в журнал только ошибки.
     - `TRACELEVEL=800`, если вы хотите использовать запись событий в журнал в режиме отладки.

О настройке дополнительных параметров вы можете узнать, обратившись в Службу технической поддержки.

7. В рабочей области выберите установочный пакет компонента Endpoint Sensors.
8. В блоке работы с выбранным объектом запустите установку программы.

   Запустится мастер удаленной установки.
9. Выберите компьютеры, на которые вы хотите установить компонент Endpoint Sensors.

   Вы можете выбрать группу администрирования или отдельные устройства.
10. Оставьте без изменений значения параметров по умолчанию.

В результате работы мастера будет создана и запущена задача удаленной установки компонента Endpoint Sensors с новыми значениями параметров. Созданная задача разместится в папке с задачами или добавится к задачам группы администрирования, для которой она была создана.

Удаленная деинсталляция компонента Endpoint Sensors

Если у вас установлен компонент Endpoint Sensors в составе KES, вам не нужно дополнительно создавать установочный пакет и устанавливать или удалять компонент Endpoint Sensors.
Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Справки Kaspersky Endpoint Security*.

Вы можете удаленно деинсталлировать компонент Endpoint Sensors с компьютера с помощью программы Kaspersky Security Center 11 или Kaspersky Security Center 10 SP3. Удаленная деинсталляция компонента Endpoint Sensors с компьютера с помощью программ Kaspersky Security Center 10 SP2 MR1 или Kaspersky Security Center 10 SP2 не поддерживается.

► *Чтобы удаленно деинсталлировать компонент Endpoint Sensors на компьютерах локальной сети организации, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC выберите папку с задачами.
4. Запустите процесс создания задачи.

   Откроется окно мастера создания задачи.
5. Выберите задачу удаленной деинсталляции.
6. В списке программ Kaspersky Security Center выберите компонент Endpoint Sensors.
7. Выберите группу администрирования или набор устройств, с которых вы хотите удалить компонент Endpoint Sensors.
8. Укажите имя задачи и время запуска.

Созданная задача отображается в рабочей области папки с задачами. В результате выполнения задачи удаленной деинсталляции компонент Endpoint Sensors будет удален с выбранных устройств.

Удаленный запуск и остановка компонента Endpoint Sensors

Вы можете временно отключить компонент Endpoint Sensors, если он мешает работе пользователя, а затем включить его. Не рекомендуется отключать компонент надолго, так как это снижает безопасность локальной сети организации.

► *Чтобы запустить или остановить компонент Endpoint Sensors на компьютере локальной сети организации, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC выберите устройство, на котором вы хотите остановить или запустить компонент Endpoint Sensors.
4. С помощью контекстного меню перейдите в окно свойств компонента.
5. Если вы хотите остановить или запустить компонент Endpoint Sensors, использующийся в составе KES, выберите закладку с задачами.
6. Если вы хотите остановить или запустить компонент Endpoint Sensors, не входящий в состав KES, выберите закладку с приложениями.
7. На открывшейся закладке выберите компонент Endpoint Sensors.
8. Остановите или запустите компонент Endpoint Sensors.

После остановки компонент Endpoint Sensors прекратит наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также отправку данных наблюдения на сервер с компонентом Central Node.

Создание политики для удаленного управления компонентом Endpoint Sensors

Вы можете создать политику для удаленного управления компонентом Endpoint Sensors на компьютере с помощью программы Kaspersky Security Center 11 или Kaspersky Security Center 10 SP3.

Если у вас установлен компонент Endpoint Sensors в составе KES, вам не нужно дополнительно создавать политику.

Вы можете получить подробную информацию об установке компонента Endpoint Sensors в Kaspersky Endpoint Security из *Справки Kaspersky Endpoint Security*.

Для работы с политиками в программе Kaspersky Security Center должен быть установлен плагин управления компонентом Endpoint Sensors. Подробную информацию об установке плагина управления в Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

► *Чтобы создать политику для удаленного управления компонентом Endpoint Sensors, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.

3. В дереве консоли KSC выберите раздел с политиками.
4. Запустите мастер создания политики.

   Откроется окно мастера создания политики.
5. Укажите имя политики.
6. Укажите адрес и порт сервера с компонентом Central Node.

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

   Значения по умолчанию: порт 443, адрес сервера не задан.
7. Выберите группу компьютеров, к которой будет применена политика.
8. Сделайте новую политику активной.

После завершения работы мастера будет создана новая политика. Список всех политик отображается в папке политик дерева консоли KSC.

Изменение параметров политики для удаленного управления компонентом Endpoint Sensors

Вы можете изменить параметры политики для удаленного управления компонентом Endpoint Sensors на компьютере с помощью программы Kaspersky Security Center 11 или Kaspersky Security Center 10 SP3.

► *Чтобы изменить параметры политики для удаленного управления компонентом Endpoint Sensors, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе с политиками выберите политику, параметры которой вы хотите изменить.
4. С помощью контекстного меню перейдите в окно свойств политики.
5. Внесите необходимые изменения.

   Вы можете изменить:

   - параметры отображения компонентов Endpoint Sensors разных типов в журнале состояний;
   - время хранения компонентов Endpoint Sensors разных типов в журнале состояний;
   - адрес и порт сервера с компонентом Central Node.

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

Изменения политики будут сохранены.

Получение данных от компонента Endpoint Sensors в консоли администрирования Kaspersky Security Center

Вы можете получать данные о состоянии компонента Endpoint Sensors из Консоли администрирования Kaspersky Security Center.

Подробную информацию о работе в консоли KSC см. в *Справке Kaspersky Security Center*.

Создание выборки компьютеров по наличию на них или свойствам компонентов Endpoint Sensors

► *Чтобы создать выборку компьютеров по свойствам компонентов Endpoint Sensors или наличию на компьютерах компонентов Endpoint Sensors, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе выбора устройств создайте новую выборку.
4. В свойствах выборки добавьте условие, созданное по умолчанию.
5. Откройте свойства нового условия.
6. Дополните условие по умолчанию в соответствии с желаемым результатом с помощью тегов. Также вы можете переходить в другие разделы для совершения дополнительных действий по поиску необходимой информации о компонентах Endpoint Sensors.

   Например, если вы хотите получить список компьютеров, на которых компонент Endpoint Sensors остановлен, включите в условие по умолчанию регулярное выражение `KATA:server address*` и статус компонента Endpoint Sensors `Stopped` в разделе статусов компонентов.

Таблица 10. Параметры создания выборки компьютеров с компонентом Endpoint Sensors

Список компьютеров, на которых…	Регулярное выражение	Необходимое действие	Дополнительные действия
…установлен компонент Endpoint Sensors.	`KATA:*`	Включить	Нет значения.
…не установлен компонент Endpoint Sensors.	`KATA:*`	Исключить	Нет значения.
…установлен компонент Endpoint Sensors, настроенный на соединение с любым компонентом Central Node.	`KATA:server address*`	Включить	Нет значения.
…установлен компонент Endpoint Sensors, настроенный на соединение с определенным компонентом Central Node.	`KATA:server address:<имя сервера>:443`	Включить	Нет значения.

Список компьютеров, на которых…	Регулярное выражение	Необходимое действие	Дополнительные действия
…установлен компонент Endpoint Sensors определенной версии.	Нет значения	Нет значения	В новом условии в разделе с названиями программ выберите компонент Endpoint Sensors и укажите номер версии.
…установлен компонент Endpoint Sensors в составе KES определенной версии.	`KATA:agent version:<номер версии>`	Включить	Нет значения.
…установлена программа KES, но отсутствует Endpoint Sensors в составе KES.	`KATA:*`	Исключить	В разделе с названиями программ выберите Kaspersky Endpoint Security.
…компонент Endpoint Sensors в составе KES установлен, но не включен.	`KATA:agent version*`	Включить	Нет значения.
	`KATA:server address*`	Исключить	Нет значения.
…остановлен компонент Endpoint Sensors.	`KATA:server address*`	Включить	В разделе статусов компонентов добавьте в условие статус компонента Endpoint Sensors: Stopped.
…установлен компонент Endpoint Sensors, но отсутствует соединение с компонентом Central Node.	Нет значения	Нет значения	В разделе статусов компонентов добавьте в условие статус компонента Endpoint Sensors: Connection to server is failed.
			В разделе статусов компонентов добавьте в условие статус Kaspersky Endpoint Security 11: Connection to server is failed.
…компонент Endpoint Sensors установлен, но не выполняет задачи.	Нет значения	Нет значения	В разделе статусов компонентов добавьте в условие статус компонента Endpoint Sensors: Tasks don’t work.

Список компьютеров, на которых…	Регулярное выражение	Необходимое действие	Дополнительные действия
			В разделе статусов компонентов добавьте в условие статус Kaspersky Endpoint Security: Tasks don't work.
…отключена самозащита компонента Endpoint Sensors.	Нет значения	Нет значения	В разделе описания статусов компонентов выберите значение статус компонента Endpoint Sensors: Self-defense is off.

Получение данных о состоянии компонента Endpoint Sensors на определенном компьютере

► *Чтобы получить данные о состоянии компонента Endpoint Sensors на определенном компьютере, выполните следующие действия:*

1. Откройте консоль KSC.
2. Выберите нужный Сервер администрирования.
3. В дереве консоли KSC в разделе с управляемыми устройствами выберите нужный вам компьютер.

   В рабочей области отобразятся данные о текущем состоянии компонента Endpoint Sensors на этом компьютере.
4. Выберите закладку с событиями в свойствах компьютера.

   Откроется журнал событий. События, связанные с работой компонента Endpoint Sensors, содержат строку "Endpoint Sensor" в графе задач.

Начало работы с программой

Этот раздел содержит информацию о том, как начать работу с программой в веб-интерфейсе, в меню администратора и в режиме Technical Support Mode.

Начало работы в веб-интерфейсе программы

Веб-интерфейс Kaspersky Anti Targeted Attack Platform расположен на сервере с компонентом Central Node.

Веб-интерфейс Kaspersky Anti Targeted Attack Platform защищен от *CSRF-атак* и работает только в том случае, если браузер пользователя веб-интерфейса программы предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Kaspersky Anti Targeted Attack Platform, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом Kaspersky Anti Targeted Attack Platform осуществляется через прокси-сервер вашей организации, убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

► *Чтобы начать работу в веб-интерфейсе, выполните следующие действия:*

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, введите IP-адрес сервера с компонентом Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. Введите имя пользователя и пароль доступа к веб-интерфейсу программы, которые вы задали на этапе установки и настройки компонента Central Node.

Откроется страница **Мониторинг** веб-интерфейса программы.

Вы можете начать работу в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Начало работы в меню администратора программы

Вы можете работать с параметрами каждого из компонентов программы Sensor, Central Node и Sandbox в меню администратора в консоли управления каждого сервера, на котором установлен компонент программы.

► *Чтобы начать работу в меню администратора компонента Sandbox, Sensor или Central Node в консоли управления сервером с компонентом Sandbox, Sensor или Central Node, выполните следующие действия:*

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы (стр. 93).

   Отобразится меню администратора компонента программы.

Вы можете начать работу в меню администратора компонента программы.

Начало работы с программой в режиме Technical Support Mode

Не рекомендуется выполнять действия с Kaspersky Anti Targeted Attack Platform в режиме Technical Support Mode без консультации или указания сотрудников Службы технической поддержки.

Вы можете работать с компонентами программы Sensor, Central Node и Sandbox в режиме Technical Support Mode.

Режим Technical Support Mode предоставляет администратору Kaspersky Anti Targeted Attack Platform неограниченные права (root) доступа к программе и всем данным (в том числе персональным), которые в ней хранятся.

Работа с Kaspersky Anti Targeted Attack Platform из консоли управления в режиме Technical Support Mode (стр. 152) с правами учетной записи суперпользователя позволяет выполнять следующие действия:

- Управлять параметрами работы программы с помощью конфигурационных файлов.

  При этом могут быть изменены параметры шифрования данных при передаче между узлами программы, параметры хранения и обработки объектов проверки.

  В этом случае данные передаются в открытом виде. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность серверов с этими данными самостоятельно. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за изменение конфигурационных файлов программы.

- Управлять параметрами журнала трассировки.

  Файлы трассировки могут содержать конфиденциальные данные пользователя.

► *Чтобы начать работу с программой в режиме Technical Support Mode, выполните следующие действия:*

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы (стр. 93).

   Отобразится меню администратора компонента программы.
3. В меню администратора программы выберите режим **Technical Support Mode**.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Если вы действительно хотите выполнять действия с программой в режиме Technical Support Mode, выберите **Yes** и нажмите на клавишу **ENTER**.

Управление учетными записями администраторов и пользователей программы

В Kaspersky Anti Targeted Attack Platform предусмотрены учетные записи для серверов со следующими компонентами:

- Sensor. Учетная запись администратора для работы в меню администратора программы и в консоли управления сервером (в режиме Technical Support Mode).

  По умолчанию используется учетная запись admin.

- Sandbox. Учетная запись администратора для работы в меню администратора программы, в консоли управления сервером (в режиме Technical Support Mode) и в веб-интерфейсе Sandbox.

  По умолчанию используется учетная запись admin.

- Central Node. Следующие учетные записи:

  - Учетная запись администратора для работы в меню администратора программы и в консоли управления сервером (в режиме Technical Support Mode).

    По умолчанию используется учетная запись admin, созданная при установке программы.

  - Учетная запись локального администратора веб-интерфейса программы.

    По умолчанию используется учетная запись Administrator, созданная при установке программы. Вы можете создать другие учетные записи администратора веб-интерфейса программы (стр. 155) после установки.

  - Учетная запись администратора веб-интерфейса программы.

  - Учетные записи пользователей веб-интерфейса программы с ролями **Сотрудник службы безопасности** и **Старший сотрудник службы безопасности**.

Данные каждой из этих учетных записей хранятся на том сервере с компонентом программы, к которому она относится.

В режиме распределенного решения (стр. 42) и multitenancy данные каждой из этих учетных записей хранятся на PCN и на том сервере с компонентом программы, к которому она относится.

Учетная запись администратора для работы в консоли управления сервером обладает неограниченными правами на управление сервером с компонентом программы, к которому она относится (правами суперпользователя). Под этой учетной записью вы можете выключить или перезагрузить сервер, а также изменить параметры программы в режиме Technical Support Mode в консоли управления сервером.

Учетная запись администратора для работы в консоли управления сервером (admin) имеет неограниченный доступ к данным на этом сервере. Пароль учетной записи администратора для работы в консоли управления сервером должен быть надежным. Администратору необходимо обеспечить безопасность серверов самостоятельно. Администратор несет ответственность за доступ к данным, хранящимся на серверах.

Под учетной записью с ролью **Администратор** вы можете добавлять, включать и отключать учетные записи пользователей программы, а также изменять пароли учетных записей администраторов и пользователей

веб-интерфейса программы. В режиме распределенного решения (стр. 42) и multitenancy управление учетными записями пользователей осуществляется на PCN.

Учетная запись локального администратора веб-интерфейса программы предназначена для сотрудников вашей организации, в чьи обязанности входит управление Kaspersky Anti Targeted Attack Platform. При входе в программу под этой учетной записью отображаются все разделы веб-интерфейса, доступные пользователю с ролью **Администратор** (стр. 178).

Под учетной записью администратора веб-интерфейса программы можно управлять программой, но, в отличие от локального администратора веб-интерфейса программы, этой учетной записи недоступно управление серверами PCN и SCN, а также организациями в разделе **Режим работы**.

Роли **Сотрудник службы безопасности** и **Старший сотрудник службы безопасности** предназначены для сотрудников вашей организации, в чьи обязанности входит работа с событиями и задачами Kaspersky Anti Targeted Attack Platform. При входе в программу под учетными записями с этими ролями отображаются все разделы веб-интерфейса, доступные сотрудникам службы безопасности (стр. 231). Пользователю с ролью **Старший сотрудник службы безопасности** доступны все операции. Ограничения пользователей с ролью **Сотрудник службы безопасности** представлены в таблице ниже.

*Таблица 11. Ограничения доступа пользователей программы с ролью **Сотрудник службы безопасности***

Функциональная область / Раздел веб-интерфейса	Ограничения
Мониторинг	Недоступны графики событий группы VIP. Нет возможности перейти по ссылке на графике в раздел **Обнаружения**.
Обнаружения	Недоступны следующие действия: • просмотр информации об обнаружении; • отметка о завершении обработки обнаружения группы VIP; • операции над несколькими обнаружениями; • экспорт списка всех обнаружений.
Поиск угроз	Недоступны события, которые относятся к хостам из обнаружений группы VIP.
Задачи	Нет доступа.
Политики	Нет доступа.
IOC/IOA-анализ	Доступ на чтение.
Хранилище	Нет доступа к объектам, помещенным в Хранилище в результате выполнения задач. Полный доступ к объектам, загруженным пользователем вручную.
Endpoint Sensors	Доступ к просмотру таблиц компьютеров с компонентом Endpoint Sensors, ограничения по просмотру данных о задачах, о политиках и о сетевой изоляции.
Сетевая изоляция хостов	Нет доступа.

Функциональная область / Раздел веб-интерфейса	Ограничения
Отчеты	Нет доступа.
Параметры: Расписание IOC-проверки	Доступ на чтение.
Параметры: Endpoint Sensors	Доступ на чтение.
Параметры: Правила KPSN	Нет доступа.
Параметры: Отправка уведомлений	Нет доступа к правилам для отправки уведомлений об обнаружениях. Полный доступ к правилам отправки уведомлений о проблемах в работе программы.
Параметры: Статус VIP	Доступ на чтение.
Параметры: YARA-правила	Доступ только на экспорт правил.
Параметры: Белый список	Доступ на чтение и экспорт.
Параметры: Пароли к архивам	Нет доступа.
Параметры: Лицензия	Доступ на чтение.

Если вы используете режим распределенного решения и multitenancy, то для каждой учетной записи вы можете разрешить или запретить доступ к организациям и веб-интерфейсу сервера SCN.

Создание учетной записи администратора веб-интерфейса программы

Под учетной записью администратора веб-интерфейса программы можно управлять программой, но, в отличие от локального администратора веб-интерфейса программы, этой учетной записи недоступно управление серверами PCN и SCN, а также организациями в разделе **Режим работы**.

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

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый пользователь**.
4. Если вы хотите включить учетную запись, включите переключатель **Состояние**.

   По умолчанию учетная запись включена.

   Если учетная запись включена, доступ к веб-интерфейсу программы разрешен. Если учетная запись отключена, доступ к веб-интерфейсу программы запрещен.
5. В раскрывающемся списке **Роль** выберите **Администратор**.
6. В поле **Имя пользователя** введите имя пользователя, учетную запись которого вы хотите создать.

Имя пользователя должно удовлетворять следующим требованиям:

- должно быть уникальным в списке имен пользователей (регистр имеет значение);
- должно содержать максимум 32 символа;
- может содержать буквы A-Z, a-z, цифры 0-9, дефис (-) или символ подчеркивания (_);
- должно начинаться с буквы (A-Z или a-z).

7. В поле **Новый пароль** введите пароль доступа к веб-интерфейсу.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.

8. В поле **Подтвердить пароль** повторно введите пароль доступа к веб-интерфейсу.
9. Нажмите на кнопку **Добавить**.

Учетная запись администратора веб-интерфейса программы будет создана.

Если вы используете режим multitenancy, учетная запись администратора веб-интерфейса сервера PCN имеет доступ к данным всех организаций, связанных с этим сервером.

Создание учетной записи пользователя веб-интерфейса программы

Вы можете создавать учетные записи пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**.

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

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый пользователь**.
4. Если вы хотите включить учетную запись, включите переключатель **Состояние**.

   По умолчанию учетная запись включена.

Если учетная запись включена, доступ к веб-интерфейсу программы разрешен. Если учетная запись отключена, доступ к веб-интерфейсу программы запрещен.

5. В раскрывающемся списке **Роль** выберите одну из следующих ролей:
   - **Старший сотрудник службы безопасности**.
   - **Сотрудник службы безопасности**.
6. В поле **Имя пользователя** введите имя пользователя, учетную запись которого вы хотите создать.

   Имя пользователя должно удовлетворять следующим требованиям:
   - должно быть уникальным в списке имен пользователей (регистр имеет значение);
   - должно содержать максимум 32 символа;
   - может содержать буквы A-Z, a-z, цифры 0-9, дефис (-) или символ подчеркивания (_);
   - должно начинаться с буквы (A-Z или a-z).
7. В поле **Новый пароль** введите пароль доступа пользователя к веб-интерфейсу.

   Пароль должен удовлетворять следующим требованиям:
   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.
8. В поле **Подтвердить пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.
9. В разделе **Доступ** настройте права доступа:
   a. Включите переключатель **Веб-интерфейс SCN**, если вы хотите предоставить пользователю доступ не только к веб-интерфейсу этого сервера PCN, но и к веб-интерфейсам всех доступных серверов SCN.
   b. Справа от названия параметра **Организации** установите флажки рядом с названиями одной или нескольких организаций, к веб-интерфейсам серверов которых вы хотите предоставить доступ.

      Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех компаний.
10. Нажмите на кнопку **Добавить**.

Учетная запись пользователя программы будет создана.

Изменение прав доступа учетной записи пользователя веб-интерфейса программы

Вы можете изменить права доступа пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** к данным серверов PCN и SCN, а также организаций, связанных с этими серверами.

► *Чтобы изменить права доступа учетной записи пользователя веб-интерфейса программы, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. Выберите учетную запись, права доступа которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
4. Если вы хотите включить или отключить учетную запись, измените положение переключателя **Состояние**.
5. Если нужно, в разделе **Доступ** измените положение переключателя **Веб-интерфейс SCN**:
   - Переведите переключатель в положение **Включено**, если вы хотите предоставить пользователю доступ не только к веб-интерфейсу этого сервера PCN, но и к веб-интерфейсам всех доступных серверов SCN.
   - Переведите переключатель в положение **Отключено**, если вы хотите предоставить пользователю доступ только к веб-интерфейсу этого сервера PCN.
6. Справа от названия параметра **Организации** установите или снимите флажки рядом с названиями организаций, к веб-интерфейсам серверов которых вы хотите изменить доступ.

   Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех организаций.
7. Нажмите на кнопку **Сохранить**.

Права доступа учетной записи будут изменены.

Включение и отключение учетной записи администратора или пользователя веб-интерфейса программы

► *Чтобы включить или отключить учетную запись администратора или пользователя веб-интерфейса программы, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. В списке учетных записей выберите учетную запись пользователя, которую вы хотите включить или отключить.
4. Выполните одно из следующих действий в графе **Состояние**:
   - Включите переключатель рядом с именем учетной записи, если вы хотите включить учетную

запись.

- Выключите переключатель рядом с именем учетной записи, если вы хотите отключить учетную запись.

Отобразится окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Состояние учетной записи будет изменено.

Изменение пароля учетной записи администратора или пользователя программы

► *Чтобы изменить пароль учетной записи администратора или пользователя программы, выполните следующие действия в веб-интерфейсе PCN:*

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. В списке учетных записей выберите учетную запись, пароль которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
4. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу программы.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.
5. В поле **Подтвердить пароль** повторно введите новый пароль.
6. Нажмите на кнопку **Сохранить**.

Пароль учетной записи администратора или пользователя программы будет изменен.

Изменение пароля своей учетной записи

► *Чтобы изменить пароль своей учетной записи, выполните следующие действия:*

1. Войдите в веб-интерфейс под своей учетной записью.
2. В нижней части окна веб-интерфейса программы по ссылке с именем вашей учетной записи

раскройте список действий.

3. Выберите действие **Изменить пароль**.

   Откроется окно **Изменить пароль**.

4. В поле **Старый пароль** введите текущий пароль доступа к веб-интерфейсу программы.
5. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу программы.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;
   - должен содержать символы минимум трех типов:
     - символ верхнего регистра (A-Z);
     - символ нижнего регистра (a-z);
     - цифру;
     - специальный символ.

6. В поле **Подтвердить пароль** повторно введите новый пароль.
7. Нажмите на кнопку **Изменить пароль**.

Пароль доступа к веб-интерфейсу программы вашей учетной записи будет изменен.

Участие в Kaspersky Security Network и использование Kaspersky Private Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Anti Targeted Attack Platform использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (далее также "KSN") – это инфраструктура облачных служб, предоставляющая пользователям доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Anti Targeted Attack Platform на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие пользователей в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, данные о которых еще не вошли в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы, а также помогает другим пользователям Kaspersky Security Network оперативно получать информацию об угрозах IT-инфраструктуре предприятий.

Когда вы участвуете в Kaspersky Security Network, Kaspersky Anti Targeted Attack Platform отправляет в Kaspersky Security Network запросы о репутации файлов, интернет-ресурсов и программного обеспечения и получает ответ, содержащий данные о репутации этих объектов.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается на этапе установки Kaspersky Anti Targeted Attack Platform, его можно изменить в любой момент.

Подробнее об участии в Kaspersky Security Network вы можете прочитать в Положении о Kaspersky Security Network.

Если вы не хотите участвовать в KSN, вы можете использовать Kaspersky Private Security Network (далее также "KPSN") – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

По вопросам приобретения программы Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе.

Настройка участия в KSN производится на сервере Central Node и распространяется на все подключаемые серверы Sensor.
Если вы используете режим распределенного решения и multitenancy, настраивайте участие в KSN на сервере PCN. Настройка участия в KSN распространится на все серверы SCN, подключаемые к PCN.

Просмотр Положения о KSN и настройка участия в KSN

► *Чтобы настроить участие в Kaspersky Security Network, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Участие в KSN/KPSN**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **KSN**.
4. Ознакомьтесь с Положением о Kaspersky Security Network и выберите один из следующих вариантов:
   - **Я согласен участвовать в KSN**, если вы согласны с условиями Положения о KSN и хотите участвовать в KSN.
   - **Я не согласен участвовать в KSN**, если вы не согласны с условиями Положения о KSN и не хотите участвовать в KSN.

   Если вы не согласны с условиями Положения, использование Kaspersky Security Network не будет включено.
5. Нажмите на кнопку **Применить**.

Участие в Kaspersky Security Network будет настроено.

Включение использования KPSN

► *Чтобы включить использование KPSN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Участие в KSN/KPSN**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **KPSN**.
4. В блоке **Конфигурационные файлы KPSN** загрузите файлы kc_private.xms, kh_private.xms и ksncli_private.dat с помощью кнопки **Обзор**.
5. Нажмите на кнопку **Применить**.

Использование Kaspersky Private Security Network будет включено.

Настройка подключения к локальной репутационной базе KPSN

Программа может сохранять информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить подключение Kaspersky Anti Targeted Attack Platform к локальной репутационной базе KPSN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Репутационная база KPSN**.

3. В поле **Хост** укажите IP-адрес сервера KPSN, на котором хранится локальная репутационная база KPSN.
4. Нажмите на кнопку **Обзор** справа от поля **TLS-сертификат**.

   Откроется окно выбора файлов.
5. Выберите файл сертификата для аутентификации пользователей в KPSN и нажмите на кнопку **Открыть**.
6. Нажмите на кнопку **Обзор** справа от поля **TLS-ключ шифрования**.

   Откроется окно выбора файлов.
7. Выберите файл, содержащий закрытый ключ шифрования, и нажмите на кнопку **Открыть**.

Подключение к локальной репутационной базе KPSN будет настроено.

Настройка сохранения информации в локальную репутационную базу KPSN

Программа может сохранять информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

► *Чтобы настроить сохранение информации об обнаружениях в локальную репутационную базу KPSN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью старшего сотрудника службы безопасности.
2. Выберите раздел **Параметры**, подраздел **Правила KPSN**.
3. В блоке параметров **Важность обнаружения** установите флажки в зависимости от уровня важности обнаружений, информацию о которых вы хотите сохранять в локальной репутационной базе KPSN.
4. Нажмите на кнопку **Сохранить**.

Информация об обнаружениях выбранного уровня важности будет сохраняться в локальной репутационной базе KPSN.

Отказ от участия в KSN и использования KPSN

► *Чтобы отказаться от участия в Kaspersky Security Network и использования KPSN, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **Участие в KSN/KPSN**.
3. Справа от названия параметра **Тип подключения** нажмите на кнопку **Не подключен**.
4. Нажмите на кнопку **Применить**.

Вы не будете участвовать в KSN и использовать KPSN.

Работа с компонентом Sandbox через веб-интерфейс

Веб-интерфейс Sandbox расположен на сервере с компонентом Sandbox.

Веб-интерфейс Sandbox защищен от *CSRF-атак* и работает только в том случае, если браузер пользователя веб-интерфейса предоставляет заголовок Referrer HTTP-запроса POST. Убедитесь, что браузер, который вы используете для работы с веб-интерфейсом Sandbox, не модифицирует заголовок Referrer HTTP-запроса POST. Если соединение с веб-интерфейсом осуществляется через прокси-сервер вашей организации, проверьте параметры и убедитесь, что прокси-сервер не модифицирует заголовок Referrer HTTP-запроса POST.

► *Чтобы начать работу в веб-интерфейсе Sandbox, выполните следующие действия:*

1. В браузере на любом компьютере, на котором разрешен доступ к серверу с компонентом Sandbox, введите IP-адрес сервера с компонентом Sandbox (стр. 99).

   Откроется окно ввода учетных данных администратора компонента Sandbox.

2. Введите имя пользователя и пароль администратора компонента Sandbox, который вы задали при установке компонента Sandbox (стр. 98).

Вы можете начать работу в веб-интерфейсе Sandbox.

Если вы используете несколько серверов с компонентом Sandbox, производите настройку параметров каждого компонента Sandbox из веб-интерфейса Sandbox этого сервера.

Обновление баз компонента Sandbox

Базы компонента Sandbox представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код и признаки подозрительного поведения объектов.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений автоматически один раз в час или обновлять базы вручную.

Запуск обновления баз вручную

► *Чтобы запустить обновление баз вручную, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.

   В блоке параметров **Последнее обновление** отобразятся время и статус последней попытки обновления баз Sandbox.

2. Нажмите на кнопку **Обновить**.

Выбор источника обновления баз

► *Чтобы выбрать источник обновления баз, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. В блоке параметров **Источник обновлений** выберите источник, из которого вы хотите получать пакет обновлений:
   - **Сервер обновлений "Лаборатории Касперского"**.
   - **Другой сервер**.
3. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите URL-адрес пакета обновлений на вашем FTP- или HTTP-сервере или укажите полный путь к директории с пакетом обновлений.
4. Нажмите на кнопку **Применить** в нижней части окна.

Включение и отключение использования прокси-сервера для обновления баз

► *Чтобы включить или отключить использование прокси-сервера для обновления баз компонента Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. В рабочей области выполните одно из следующих действий:
   - Включите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы хотите использовать прокси-сервер при обновлении баз компонента Sandbox.
   - Выключите переключатель рядом с названием блока параметров **Прокси-сервер**, если вы не хотите использовать прокси-сервер при обновлении баз компонента Sandbox.

Настройка параметров соединения с прокси-сервером для обновления баз

► *Чтобы настроить параметры соединения с прокси-сервером для обновления баз компонента Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.
2. Включите переключатель рядом с названием блока параметров **Прокси-сервер**.
3. В поле **Адрес** введите адрес прокси-сервера.
4. В поле **Порт** укажите номер порта прокси-сервера.
5. В поле **Имя пользователя** введите имя пользователя прокси-сервера.
6. В поле **Пароль** введите пароль подключения к прокси-серверу.
7. Выполните одно из следующих действий:
   - Установите флажок **Не использовать прокси-сервер для локальных адресов**, если вы не хотите использовать прокси-сервер для внутренних адресов электронной почты вашей организации.
   - Снимите флажок **Не использовать прокси-сервер для локальных адресов**, если вы хотите

использовать прокси-сервер независимо от принадлежности адресов электронной почты к вашей организации.

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

Настройка соединения компонентов Sandbox и Central Node

Предусмотрен следующий порядок настройки соединения компонента Sandbox с компонентом Central Node:

1. В меню администратора или в веб-интерфейсе каждого сервера с компонентом Central Node создается запрос на подключение к компоненту Sandbox.
2. В веб-интерфейсе Sandbox отображаются запросы на подключение.

   Вы можете принять или отклонить каждый запрос.

Создание запроса на подключение к Sandbox в меню администратора Central Node

Для создания соединения между компонентами Central Node и Sandbox, необходимо отправить запрос на подключение к компоненту Sandbox с каждого компонента Central Node.

► *Чтобы создать запрос на подключение к компоненту Sandbox, выполните следующие действия:*

1. Зайдите в консоль сервера Central Node, с которого вы хотите создать запрос на подключение к Sandbox, по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя пользователя admin и пароль, заданный при установке и настройке компонента Central Node.

   Отобразится меню администратора программы.
3. В меню администратора программы выберите **Program Settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действия.
5. Выберите действие **ConСхема Sandbox connection**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно **Sandbox access**.
7. Выберите **New**.
8. Нажмите на клавишу **ENTER**.

   Откроется окно **Sandbox node**.
9. В поле **Sandbox name** введите доменное имя сервера Sandbox, запрос на подключение к которому вы создаете.
10. В поле **Sandbox node** введите IP-адрес сервера Sandbox, запрос на подключение к которому вы создаете.
11. Нажмите на кнопку **Ok**.

    Откроется окно выбора действия.

12. Выберите строку с IP-адресом сервера Sandbox.
13. Нажмите на клавишу **ENTER**.
14. Откроется окно **Sandbox key fingerprint**, содержащее отпечаток сертификата Sandbox и просьбу подтвердить подлинность отпечатка сертификата.
15. Убедитесь, что отпечаток сертификата соответствует отпечатку сертификата в веб-интерфейсе Sandbox, запрос на подключение к которому вы создаете.
16. После того, как вы убедились, что отпечатки сертификатов идентичны, нажмите на кнопку **Yes**.

    Откроется окно подтверждения отправки запроса на подключения к компоненту Sandbox.
17. Нажмите на кнопку **Yes**.

    Вы вернетесь к окну выбора действия с IP-адресом сервера Sandbox.

Если запрос на подключение к компоненту Sandbox отправлен успешно, напротив названия параметра Enabled отобразится значение **Yes**.

Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox

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

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

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

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

   В каждом запросе на подключение содержится следующая информация:

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

     Может иметь значения **Ожидание** или **Принят**.
2. Убедитесь, что отпечаток сертификата Cental Node соответствует отпечатку сертификата на стороне Cental Node.

   Вы можете проверить отпечаток сертификата Central Node в меню администратора сервера Central Node в разделе **Manage server certificate**.
3. Нажмите на одну из следующих кнопок в строке с запросом на подключение от компонента Central Node:

   - **Принять**, если вы хотите принять запрос на подключение.
   - **Отклонить**, если вы хотите отклонить запрос на подключение.
   - **Отозвать**, если вы хотите отозвать ранее принятый запрос на подключение.
4. Нажмите на кнопку **Применить** в нижней части окна.

Настройка сетевых интерфейсов компонента Sandbox

В этом разделе содержится информация о настройке сетевых интерфейсов компонента Sandbox.

Настройка параметров DNS

► *Чтобы настроить параметры DNS, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В поле **Имя хоста** введите имя сервера, на который вы устанавливаете компонент Sandbox, в формате FQDN (например, sandbox).
3. Справа от названия параметра **DNS-серверы** нажмите на кнопку **Добавить**.

   Добавится пустое поле ввода IP-адреса DNS-сервера.
4. Введите IP-адрес основного DNS-сервера в формате IPv4.
5. Нажмите на кнопку ✔ справа от поля ввода.

   DNS-сервер будет добавлен.
6. Если вы хотите добавить дополнительный DNS-сервер, повторите действия 2-5.
7. Если вы хотите удалить добавленный DNS-сервер, нажмите на кнопку 🗑 справа от строки с IP-адресом DNS-сервера.

   Вы можете удалить только дополнительные DNS-серверы. Вы не можете удалить основной DNS-сервер. Если вы добавили 2 и более DNS-сервера, вы можете удалить любой из них, при этом оставшийся DNS-сервер будет использоваться в качестве основного.

Настройка параметров управляющего сетевого интерфейса

Управляющий сетевой интерфейс предназначен для доступа к серверу с компонентом Sandbox по протоколу SSH, также через этот интерфейс компонент Sandbox будет принимать объекты от компонента Central Node.

Вы можете настроить управляющий сетевой интерфейс во время установки компонента Sandbox (стр. 98).

Вы также можете настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox.

► *Чтобы настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Управляющий интерфейс** в раскрывающемся списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.
3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу, если IP-адрес не назначен.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. Нажмите на кнопку **Применить** в нижней части окна.

Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет

Объекты, которые обрабатывает компонент Sandbox, могут предпринимать попытки действий в интернете через сетевой интерфейс для доступа обрабатываемых объектов в интернет. Компонент Sandbox может анализировать поведение этих объектов.

Если вы запретите доступ в интернет, компонент Sandbox не сможет анализировать поведение объектов в интернете, и будет анализировать поведение объектов без доступа в интернет.

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

Если в соответствии с политикой безопасности вашей организации с компьютеров пользователей локальной сети запрещен доступ в интернет, и вы настроили сетевой интерфейс Sandbox для доступа обрабатываемых объектов в интернет, есть риск возникновения следующего сценария: Злоумышленник может прикрепить вредоносную программу к произвольному файлу и запустить Sandbox-проверку этого файла с компьютера пользователя локальной сети. Этот файл будет выведен за пределы локальной сети через сетевой интерфейс для доступа обрабатываемых объектов в интернет в процессе проверки файла компонентом Sandbox.

Отсутствие сетевого интерфейса Sandbox для доступа обрабатываемых объектов в интернет исключает риски подобной передачи информации, однако снижает качество обнаружений.

► *Чтобы настроить сетевой интерфейс для доступа обрабатываемых объектов в интернет, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Интерфейс для выхода в интернет** в списке **Интерфейс** выберите сетевой интерфейс, который вы хотите использовать для доступа обрабатываемых объектов в интернет.

   Управляющий сетевой интерфейс, которые вы настроили ранее, недоступен для выбора в этом списке сетевых интерфейсов.
3. В поле **IP** введите IP-адрес, который вы хотите назначить этому сетевому интерфейсу.
4. В поле **Маска** введите маску сети, в которой вы хотите использовать этот сетевой интерфейс.
5. В поле **Шлюз по умолчанию** введите адрес шлюза сети, в которой вы хотите использовать этот сетевой интерфейс.
6. Нажмите на кнопку **Применить** в нижней части окна.

Добавление, изменение и удаление статических сетевых маршрутов

Вы можете настроить статические сетевые маршруты во время установки компонента Sandbox (стр. 100).

Вы также можете добавить, удалить или изменить статические сетевые маршруты в веб-интерфейсе Sandbox.

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

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** нажмите на кнопку **Добавить**.

   В списке статических сетевых маршрутов добавится строка с пустыми полями.
3. В поле **IP** введите IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
4. В поле **Маска** введите маску подсети.
5. В поле **Шлюз** введите IP-адрес шлюза.
6. В списке **Интерфейс** выберите сетевой интерфейс, для которого вы хотите добавить статический сетевой маршрут.
7. Нажмите на кнопку ✔.
8. Нажмите на кнопку **Применить** в нижней части окна.

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

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите удалить, нажмите на кнопку 🗑.
3. Нажмите на кнопку **Применить** в нижней части окна.

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

1. В окне веб-интерфейса Sandbox выберите раздел **Сетевые интерфейсы**.
2. В группе параметров **Статические маршруты** в строке со статическим сетевым маршрутом, который вы хотите изменить, нажмите на кнопку ✎.

   Строка статического сетевого маршрута станет доступна для редактирования. Вы можете изменить один или несколько параметров статического сетевого маршрута.
3. В поле **IP** измените IP-адрес сервера, для которого вы хотите настроить статический сетевой маршрут.
4. В поле **Маска** измените маску подсети.
5. В поле **Шлюз** измените IP-адрес шлюза.
6. В списке **Интерфейс** выберите сетевой интерфейс, для которого вы редактируете сетевой маршрут.
7. Нажмите на кнопку ✔.
8. Нажмите на кнопку **Применить** в нижней части окна.

Обновление системы Sandbox

"Лаборатория Касперского" может выпускать пакеты обновлений Kaspersky Anti Targeted Attack Platform и отдельных компонентов программы. Например, могут выпускаться срочные пакеты обновлений, устраняющие уязвимости и ошибки, плановые обновления, добавляющие новые или улучшающие существующие функции программы и ее компонентов.

После выпуска обновлений Sandbox вы можете установить их через веб-интерфейс Sandbox.

Перед установкой обновлений через веб-интерфейс Sandbox вам нужно загрузить пакет обновления в формате TGZ и инструкцию по установке данного обновления с сайта "Лаборатории Касперского" на ваш компьютер.

► *Чтобы обновить систему Sandbox через веб-интерфейс, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление системы**.

   Справа от названия параметра **Текущая версия** отобразится текущая версия компонента Sandbox.
2. Нажмите на кнопку **Обзор** справа от поля **Пакет обновления**.

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

   Окно выбора файлов закроется.

Вы можете следить за ходом обновления системы Sandbox в окне **Журнал обновлений** раздела **Обновление системы** веб-интерфейса Sandbox.

Пакет обновления будет установлен автоматически. Процесс обновления может занять несколько минут. Сервер Sandbox перезагрузится. Компонент Sandbox будет недоступен во время обновления системы.

Установка даты и времени системы Sandbox

► *Чтобы установить дату и время сервера с компонентом Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Дата и время**.
2. В раскрывающемся списке **Страна** выберите нужную страну.
3. В раскрывающемся списке **Часовой пояс** выберите нужный часовой пояс.
4. Если вы хотите синхронизировать время с NTP-сервером, включите переключатель справа от названия параметра **Синхронизация с NTP-серверами**.
5. Если вы хотите установить дату и время вручную, не включайте переключатель справа от названия параметра **Синхронизация с NTP-серверами** и выполните следующие действия:

   a. В поле **Дата** введите текущую дату или нажмите на кнопку  и выберите дату в календаре.

   b. В поле **Время** введите текущее время.
6. Нажмите на кнопку **Применить** в нижней части окна.

Установка и настройка образов операционных систем и программ для работы компонента Sandbox

В комплекте поставки вы получаете три ISO-образа операционных систем Windows XP SP3, 64-разрядной Windows 7, 64-разрядной Windows 10 и программ, необходимых для работы компонента Sandbox. Вам не требуется активировать эти операционные системы и программ. В поставляемых образах уже добавлен лицензионный ключ Microsoft.

Компонент Sandbox будет запускать объекты в этих операционных системах и анализировать поведение объектов для выявления вредоносной активности, признаков целевых атак и вторжений в IT-инфраструктуру организации.

При возникновении проблем с активацией операционных систем или программ в веб-интерфейсе компонента Sandbox отобразится сообщение об ошибке. В этом случае рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Загрузка ISO-образов операционных систем и программ для работы компонента Sandbox

► *Чтобы загрузить ISO-образ операционной системы и программ, необходимых для работы компонента Sandbox, выполните следующие действия для каждого ISO-образа:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В группе параметров **Образы виртуальных машин** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
3. Выберите файл формата ISO, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

В списке **Образы виртуальных машин** отобразится загруженный образ операционной системы и программ, необходимых для работы компонента Sandbox.

Выполните действия по загрузке образов операционных систем и программ, необходимых для работы компонента Sandbox, для каждого ISO-образа.

Создание виртуальных машин с образами операционных систем и программ для работы компонента Sandbox

► *Чтобы создать виртуальную машину с образом операционной системы и программ, необходимых для работы компонента Sandbox, выполните следующие действия для каждой виртуальной машины:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В списке **Образы виртуальных машин** в строке с названием образа операционной системы и программ для работы компонента Sandbox нажмите на кнопку **Создать VM**.

Откроется окно **Лицензионное соглашение**, содержащее тексты следующих лицензионных соглашений:

- MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1.
- MICROSOFT WINDOWS XP PROFESSIONAL EDITION SERVICE PACK 3.
- MICROSOFT OFFICE 2010 DESKTOP APPLICATION SOFTWARE.
- MICROSOFT OFFICE 2007 DESKTOP APPLICATION SOFTWARE.
- MICROSOFT OFFICE 2003 DESKTOP APPLICATION SOFTWARE.
- ADOBE® Personal Computer Software License Agreement.
- MICROSOFT VISUAL C++ 2005 RUNTIME LIBRARIES.
- MICROSOFT VISUAL C++ 2008 RUNTIME LIBRARIES (X86, IA64 AND X64), SERVICE PACK 1.
- MICROSOFT VISUAL C++ 2010 RUNTIME LIBRARIES.
- MICROSOFT VISUAL C++ 2012 RUNTIME LIBRARIES.
- MICROSOFT VISUAL C++ REDISTRIBUTABLE FOR VISUAL STUDIO 2013.
- MICROSOFT VISUAL STUDIO 2017 TOOLS, ADD-ONs and C++ REDISTRIBUTABLE.

3. Ознакомьтесь с текстами лицензионных соглашений и нажмите на кнопку **Принять** в правом нижнем углу окна **Лицензионное соглашение**.

   Откроется окно **Unpack**. Архив с образом операционной системы и программ для работы компонента Sandbox будет распакован.

4. В списке **Не установленные виртуальные машины** окна **Виртуальные машины** появится виртуальная машина, готовая к активации операционных систем и программ, а также к установке.

Выполните действия по созданию виртуальных машин с образами операционных систем и программ для работы компонента Sandbox для каждой виртуальной машины.

Установка виртуальных машин с образами операционных систем и программ для работы компонента Sandbox

► *Чтобы установить все готовые к установке виртуальные машины с образами операционных систем и программ для работы компонента Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В левом нижнем углу списка **Не установленные виртуальные машины** нажмите на кнопку **Установить готовые VM**.

   Виртуальные машины с операционными системами, рядом с названиями которых в списке **Не установленные виртуальные машины** отображается статус **Готова к установке**, будут установлены и отобразятся в списке в верхней части окна **Виртуальные машины**.

Удаление всех виртуальных машин, ожидающих установки

► *Чтобы удалить все виртуальные машины, ожидающие установки, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В левом нижнем углу списка **Не установленные виртуальные машины** нажмите на кнопку **Удалить все ожидающие VM**.

   Виртуальные машины с операционными системами и программами для работы компонента Sandbox, ожидающие установки, будут удалены.

Установка максимального количества одновременно запускаемых виртуальных машин

Задайте ограничение для количества одновременно запускаемых виртуальных машин с операционными системами, в которых компонент Sandbox будет обрабатывать объекты.

Количество одновременно запускаемых виртуальных машин не может превышать 200.

Рассчитывайте количество одновременно запускаемых виртуальных машин с образами операционных систем следующим образом: количество ядер процессора нужно умножить на 1,5.

► *Чтобы установить максимальное количество одновременно запускаемых виртуальных машин, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Виртуальные машины**.
2. В группе параметров **Гостевые виртуальные машины** в поле **Максимум VM одновременно** введите количество одновременно запускаемых виртуальных машин.

   Вы можете ввести число от 1 до 200.
3. Нажмите на кнопку **Сохранить**.

Загрузка журнала системы Sandbox на жесткий диск

Данные в журнале системы Sandbox хранятся в открытом незашифрованном виде. Данные хранятся за последние 7 дней.

► *Чтобы загрузить журнал системы Sandbox на жесткий диск, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Журнал системы** нажмите на кнопку **Скачать**.

   Журнал системы Sandbox загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы с программой.

Экспорт параметров Sandbox

► *Чтобы экспортировать параметры системы Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Параметры** нажмите на кнопку **Экспортировать**.

   Откроется окно **Предупреждение**, содержащее предупреждение об особенностях экспорта параметров системы.

   Параметры системы Sandbox зависят от аппаратных и программных параметров сервера, на котором установлен компонент Sandbox. Экспортируемые параметры системы Sandbox предназначены для импорта на этот же или строго идентичный по конфигурации сервер. Попытки восстановить конфигурацию системы Sandbox значениями параметров, сохраненными на другой системе Sandbox, могут нарушить работу системы Sandbox.

3. Нажмите на кнопку **Сохранить**.

Файл формата tar.gz загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы программы. В файле содержатся все текущие параметры системы Sandbox.

Архивы с резервной копией параметров системы могут содержать такие конфиденциальные данные, как, например, пароли, закрытые ключи. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность этих данных самостоятельно.

Импорт параметров Sandbox

► *Чтобы импортировать параметры Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Параметры** нажмите на кнопку **Импортировать**.

   Откроется окно **Предупреждение**, содержащее предупреждение об особенностях импорта параметров системы.

   Параметры компонента Sandbox зависят от аппаратных и программных параметров сервера, на котором установлен Sandbox. Экспортируемые параметры Sandbox предназначены для импорта на этот же или строго идентичный по конфигурации сервер. Попытки восстановить конфигурацию одной системы Sandbox настройками параметров, сохраненными на другой системе Sandbox, могут нарушить работу системы.

3. Нажмите на кнопку **Восстановить**.

   Откроется окно выбора файлов.

4. Выберите файл формата tar.gz с параметрами Sandbox, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

Окно выбора файлов закроется.

Если импорт параметров Sandbox прошел успешно, сервер Sandbox перезагрузится. Через несколько минут вам нужно обновить окно браузера и повторить вход.

Архивы с резервной копией конфигурации системы могут содержать такие конфиденциальные данные, как, например, пароли, закрытые ключи. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность хранения этих данных самостоятельно.

Перезагрузка сервера Sandbox

► *Чтобы перезагрузить сервер Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Питание** нажмите на кнопку **Перезагрузить**.

   Откроется окно подтверждения перезагрузки сервера Sandbox.
3. Нажмите на кнопку **Да**.

Сервер Sandbox перезагрузится. Через несколько минут вы сможете войти в систему.

Выключение сервера Sandbox

► *Чтобы выключить сервер Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Питание** нажмите на кнопку **Выключить**.

   Откроется окно подтверждения выключения сервера Sandbox.
3. Нажмите на кнопку **Да**.

Сервер Sandbox выключится.

Изменение пароля учетной записи администратора Sandbox

► *Чтобы изменить пароль учетной записи администратора Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В блоке параметров **Изменить пароль** отобразится имя учетной записи администратора Sandbox, которое вы задали при установке Sandbox (стр. 98) и поля для изменения пароля.
3. В поле **Текущий пароль** введите текущий пароль учетной записи администратора Sandbox.
4. В поле **Новый пароль** введите новый пароль учетной записи администратора Sandbox.
5. В поле **Подтвердить пароль** введите новый пароль учетной записи администратора Sandbox

повторно.

6. Нажмите на кнопку **Изменить пароль**.

   Пароль учетной записи администратора Sandbox будет изменен.

Администратору: работа в веб-интерфейсе программы

Этот раздел адресован специалистам, которые осуществляют установку и администрирование Kaspersky Anti Targeted Attack Platform, а также управление серверами PCN и SCN и организациями в режиме распределенного решения и multitenancy.

Интерфейс Kaspersky Anti Targeted Attack Platform

Работа с программой осуществляется через веб-интерфейс. Разделы веб-интерфейса программы различаются в зависимости от роли пользователя – **Администратор** или **Старший сотрудник службы безопасности** / **Сотрудник службы безопасности** (стр. 231).

Окно веб-интерфейса программы содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса программы;
- закладки в верхней части окна веб-интерфейса программы для некоторых разделов программы;
- рабочую область в нижней части окна веб-интерфейса программы.

Разделы окна веб-интерфейса программы

Веб-интерфейс программы для роли **Администратор** разделен на следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.
- **Режим работы**. Содержит информацию о серверах PCN и SCN, об организациях в режиме распределенного решения и multitenancy.
- **Endpoint Sensors**. Содержит информацию о подключенных компонентах Endpoint Sensors и их параметры.
- **Параметры**. Содержит параметры сервера с компонентом Central Node.
- **Серверы Sensor**. Содержит информацию о подключенных компонентах Sensor и их параметры.
- **Серверы Sandbox**. Содержит информацию о подключении компонента Central Node к компонентам Sandbox.
- **Внешние системы**. Содержит информацию об интеграции программы с почтовыми сенсорами.

Рабочая область окна веб-интерфейса программы

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса программы, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью графиков в разделе **Мониторинг** окна веб-интерфейса программы. Вы можете добавлять, удалять, перемещать графики, настраивать масштаб графиков и выбирать период отображения данных.

О графиках и схемах расположения графиков

С помощью графиков вы можете осуществлять мониторинг работы программы.

Схема расположения графиков – вид рабочей области окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать графики на схеме расположения графиков.

В программе доступны следующие графики:

- **Обработка данных**. Отображение состояния обработки трафика компонентом Sensor.
- **Очереди** (стр. 183). Отображение сведений о количестве и объеме объектов, ожидающих проверки модулями и компонентами программы.
- **Время обработки в Sandbox** (стр. 184). Отображение среднего времени, за которое были получены результаты проверки объектов компонентом Sandbox.

Если вы используете режим multitenancy, в разделе отображаются данные по выбранной вами организации и серверу (стр. 180).

Выбор организации и сервера для работы в разделе Мониторинг

Если вы используете режим multitenancy, перед началом работы в разделе **Мониторинг** вам нужно выбрать организацию и сервер, данные по которым вы хотите просмотреть.

► *Чтобы выбрать организацию и сервер для отображения данных в разделе **Мониторинг**, выполните следующие действия:*

1. В верхней части меню веб-интерфейса программы нажмите на стрелку рядом с именем сервера.
2. В раскрывшемся меню выберите организацию и нужный вам сервер из списка.

Отобразятся данные по выбранному вами серверу. Если вы хотите изменить организацию и сервер, вам нужно повторить действия по выбору организации и сервера.

Добавление графика на текущую схему расположения графиков

► *Чтобы добавить график на текущую схему расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на кнопку **Графики**.
5. В появившемся окне **Настроить графики** выполните следующие действия:
   - Если вы хотите добавить график **Очереди**, включите переключатель рядом с названием этого графика.
   - Если вы хотите добавить график **Время обработки в Sandbox**, включите переключатель рядом с названием этого графика.
   - Если вы хотите добавить график **Обработка данных**, нажмите на кнопку  рядом с названием этого графика.

Выбранный график будет добавлен на текущую схему расположения графиков.

Перемещение графика на текущей схеме расположения графиков

► *Чтобы переместить график на текущей схеме расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Выберите график, который вы хотите переместить на схеме расположения графиков.
5. Нажав и удерживая левую клавишу мыши на верхней части графика, перетащите график на другое

место схемы расположения графиков.

6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения графиков будет сохранена.

Удаление графика с текущей схемы расположения графиков

► *Чтобы удалить график с текущей схемы расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок  в правом верхнем углу графика, который вы хотите удалить со схемы расположения графиков.

   График будет удален из рабочей области окна веб-интерфейса программы.
5. Нажмите на кнопку **Сохранить**.

График будет удален с текущей схемы расположения графиков.

Сохранение схемы расположения графиков в PDF

► *Чтобы сохранить схему расположения графиков в PDF, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Сохранить как PDF**.

   Откроется окно **Сохранение в PDF**.
4. В нижней части окна в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.

   Схема расположения графиков в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.
6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на графиках

Вы можете настроить отображение данных на графиках за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

► *Чтобы настроить отображение данных на графиках за сутки (с 00:00 до 23:59), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за неделю (с понедельника по воскресенье), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за месяц (календарный месяц), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

Мониторинг приема и обработки входящих данных

На графике **Обработка данных** вы можете оценить статус обработки данных, поступающих от компонента Sensor на сервер с компонентом Central Node, и отследить ошибки обработки данных.

Вы можете выбрать Sensor, поступление данных с которого вы хотите оценить, в раскрывающемся списке справа от названия графика **Обработка данных**.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от списка Sensor:

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на графиках (стр. 181).

В левой части каждого графика отображается легенда графика по цветам, которые используются на самих графиках.

Если выбран тип отображения данных **Текущая загрузка**, справа от легенды отображается средняя скорость обработки данных за последние 5 минут.

Пример:

На графике **Обработка данных**, где выбраны Sensor типа **(SPAN)** и тип отображения данных **Текущая загрузка**, отображается скорость обработки данных зеркалированного трафика локальной сети, поступающих от компонента Sensor на сервер с компонентом Central Node в определенное время.

Отображаются следующие данные:

- **Трафик** – скорость поступления трафика на сервер с компонентом Sensor зеленым цветом.
- **Файлы** – скорость обработки файлов серым цветом.
- **URL-адреса** – скорость обработки URL-адресов синим цветом.
- **Ошибки обработки** – ошибки обработки данных вертикальными линиями красного цвета.

При наведении курсора мыши на график появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.

Если выбран тип отображения данных **Выбранный период**, справа от легенды отображается средняя скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов за выбранный период.

Пример:

На графике **Обработка данных**, где выбраны Sensor типа **(SMTP)** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных (стр. 181) **Месяц**, отображается скорость поступления почтового трафика по протоколу SMTP на сервер с компонентом Central Node, а также количество файлов и URL-адресов, извлеченных из почтового трафика за выбранный месяц.

Отображаются следующие данные:

- **Средний трафик** – скорость поступления трафика на сервер с компонентом Central Node зеленым цветом.
- **Файлы** – количество извлеченных файлов серым цветом.
- **URL-адреса** – количество извлеченных URL-адресов синим цветом.
- **Ошибки обработки** – ошибки обработки данных вертикальными линиями красного цвета.

При наведении курсора мыши на график появляется всплывающее окно, в котором отображается скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов в определенное время.

Мониторинг очередей обработки данных модулями и компонентами программы

На графике **Очереди** вы можете оценить статус обработки данных модулями программы **YARA**, **AM Engine**, компонентом **Sandbox** и отследить ошибки обработки данных.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия графика **Очереди**:

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на графиках.

В левой части графика отображается легенда графика по цветам, которые используются на графике.

На графике **Очереди** отображаются следующие данные:

- **Количество сообщений** и **Объем данных**, обработанных модулями и компонентами программы:
  - **YARA** – синим цветом.
  - **Sandbox** – фиолетовым цветом.
  - **AM Engine** – зеленым цветом.
- **Ошибки** – ошибки обработки данных вертикальными линиями красного цвета.

При наведении курсора мыши на график появляется всплывающее окно, в котором отображается статус обработки данных модулями программы **YARA**, **AM Engine** и компонентом **Sandbox**, а также ошибки обработки данных в определенное время.

Мониторинг обработки данных компонентом Sandbox

На графике **Время обработки в Sandbox** отображается среднее время, прошедшее от момента отправки данных на один или несколько серверов с компонентом Sandbox (включая время ожидания отправки) до отображения результатов обработки данных компонентом Sandbox в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в выбранный период.

Пример:

Если настроен период отображения данных на графиках **Месяц**, на графике **Время обработки в Sandbox** отображаются столбики оранжевого цвета на каждый день месяца.

При наведении курсора мыши на каждый столбик появляется всплывающее окно, в котором отображается среднее время, прошедшее от момента отправки данных на один или несколько серверов с компонентом Sandbox до отображения результатов обработки данных компонентом Sandbox в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в выбранный день.

Вы можете увеличить скорость обработки данных компонентом Sandbox и пропускную способность компонента Sandbox, увеличив количество серверов с компонентом Sandbox (стр. **Error! Bookmark not defined.**) и распределив по этим серверам данные, предназначенные для обработки.

Просмотр информации о сбоях в работе модулей и компонентов программы

Если в работе модулей и компонентов программы возникли ошибки, в верхней части окна раздела **Мониторинг** веб-интерфейса программы отображается рамка красного цвета с указанием возникших ошибок.

Пользователю с ролью **Локальный администратор** или **Администратор** доступна информация о сбоях программы на том сервере Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** доступна информация о сбоях программы:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о сбоях

программы на том сервере Central Node, на котором он сейчас работает.

- Если вы используете режим распределенного решения и multitenancy, и пользователь работает на сервере SCN, пользователю доступна информация о сбоях программы на этом сервере SCN в рамках тех организаций, к данным которых у него есть доступ (стр. 158).
- Если вы используете режим распределенного решения и multitenancy, и пользователь работает на сервере PCN, пользователю доступна информация о сбоях программы на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу, в рамках тех организаций, к данным которых у него есть доступ (стр. 158).

► *Чтобы получить более подробную информацию о возникших ошибках,*

по ссылке **Просмотреть сведения** откройте окно **Ошибки системы**.

В окне **Ошибки системы** отображается следующая информация:

- Если в работе нет сбоев, в строке отображается значок  .
- Если обнаружены проблемы с работой программы, в строке отображается значок с количество найденных ошибок (например, ).

  В этом случае в правой части окна **Ошибки системы** отображается подробная информация об ошибках.

Окно **Ошибки системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов программы.

  Содержит информацию о статусе работы следующих модулей и компонентов программы:

  - **YARA**.
  - **Sandbox**.
  - **URL Reputation**.
  - **Intrusion Detection System**.
  - **Anti-Malware Engine**.
  - **Targeted Attack Analyzer**.
  - **IOC-проверка**.
  - **IOA-анализ**.
  - **Обновление баз** – на всех серверах, на которых работает программа.

    Если базы одного или нескольких компонентов программы не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок  .
  - **Карантин**.
- **Обработка данных** – наличие ошибок приема и обработки входящих данных. Статус формируется на основе следующих критериев:
  - Наличие ошибок, связанных с получением данных с серверов с компонентом Sensor и с сервера или виртуальной машины с почтовым сенсором.
  - Информация о превышении максимально допустимого времени, которое объекты ожидают в

очереди на проверку модулями и компонентами программы.

- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и multitenancy).

В случае обнаружения проблем в работоспособности модулей и компонентов программы, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (стр. 405).

Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса программы

С помощью веб-интерфейса программы вы можете выполнять следующие действия с сервером, на котором установлен компонент Central Node:

- настраивать дату и время сервера;
- выключать и перезагружать сервер;
- заменять сертификат сервера;
- настраивать сетевые параметры сервера.

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Настройка даты и времени сервера

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить дату и время сервера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Дата и время**.
2. В раскрывающемся списке **Страна** выберите страну физического местоположения сервера с установленным компонентом Central Node.
3. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, в котором находится сервер с установленным компонентом Central Node.

   Вы можете указать страну и часовой пояс, выбрав нужный регион на карте под раскрывающимися списками.
4. Настройте синхронизацию с NTP-серверами:
   - Включите переключатель рядом с названием параметра **Синхронизация с NTP-серверами**, если вы хотите включить синхронизацию.
   - Выключите переключатель рядом с названием параметра **Синхронизация с NTP-серверами**, если вы хотите отключить синхронизацию.
5. В блоке **NTP-серверы** выполните следующие действия:
   - Если вы хотите добавить новый NTP-сервер, выполните следующие действия:
     a. Нажмите на кнопку **Добавить**.
     b. В появившемся поле введите IP-адрес или доменное имя NTP-сервера.
     c. Справа от поля нажмите на кнопку ✓.
   - Если вы хотите изменить IP-адрес или доменное имя NTP-сервера, в строке с этим сервером

нажмите на кнопку .

- Если вы хотите удалить NTP-сервер, в строке с этим сервером нажмите на кнопку .

6. Если синхронизация с NTP-серверами отключена, укажите дату и время сервера вручную:
   - В поле **Дата** укажите текущую дату вручную или выберите ее в календаре по кнопке справа от поля.
   - В поле **Время** укажите текущее время.
7. Нажмите на кнопку **Применить**.

Дата и время сервера будут настроены.

Выключение и перезагрузка сервера

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы выключить или перезагрузить сервер через веб-интерфейс программы, выполните следующие:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Управление сервером** выполните следующие действия:
   - Если вы хотите выключить сервер, на котором установлен компонент Central Node, PCN или SCN, нажмите на кнопку **Выключить**.
   - Если вы хотите перезагрузить сервер, на котором установлен компонент Central Node, PCN или SCN, нажмите на кнопку **Перезагрузить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Сервер будет выключен или перезагружен.

Замена сертификата сервера

После создания нового сертификата необходимо повторно авторизовать почтовые сенсоры, подключить Central Node, PCN или SCN к Sandbox, загрузить новый сертификат в Active Directory, а также перезапустить службу компонентов Endpoint Sensors.

Вы можете создать новый сертификат через веб-интерфейс программы или загрузить созданный ранее сертификат.

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы создать новый сертификат сервера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Отпечаток сертификата** нажмите на кнопку **Создать новый**.
3. В окне подтверждения нажмите на кнопку **Да**.

Новый сертификат сервера будет создан. Связь с почтовыми сенсорами и компонентом Sandbox будет прервана до повторной авторизации.

Выполняйте действия в веб-интерфейсе того сервера, на который вы хотите загрузить сертификат.

► *Чтобы загрузить созданный ранее сертификат, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Отпечаток сертификата** нажмите на кнопку **Загрузить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Сертификат будет загружен. Связь с почтовыми сенсорами и компонентом Sandbox будет прервана до повторной авторизации.

Сохранение файла сертификата сервера на компьютере

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы сохранить файл сертификата сервера на компьютере, выполните следующие действия:*

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

Файл сертификата сервера будет сохранен в папке загрузки браузера.

Назначение DNS-имени сервера

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы назначить имя сервера для использования DNS-серверами, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В поле **Имя сервера (FQDN)** введите полное доменное имя сервера.

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

Имя хоста будет назначено.

Настройка параметров DNS

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить параметры DNS, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Если вы хотите настроить назначение DNS-адресов с помощью DHCP-сервера, выполните следующие действия:
   a. В блоке параметров **Параметры DNS** в строке **Режим** выберите **DHCP**.
   b. В раскрывающемся списке **Сетевой интерфейс** выберите имя сетевого интерфейса для соединения с DNS-сервером.
3. Если вы хотите настроить назначение статических DNS-адресов, выполните следующие действия:
   a. В блоке параметров **Параметры DNS** в строке **Режим** выберите **Статический**.
   b. В поле **Домены** укажите имя домена.
   c. В поле **Главный и дополнительный DNS-серверы** введите IP-адреса DNS-серверов.
4. Нажмите на кнопку **Применить**.

Параметры DNS будут настроены.

Включение и отключение сетевого интерфейса

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

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

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Выберите сетевой интерфейс, который вы хотите включить.

Откроется окно **Изменить сетевой интерфейс**.

3. В строке **Состояние** переведите переключатель в положение **Включено**.
4. Нажмите на кнопку **Инициализировать**.

Сетевой интерфейс будет включен.

► *Чтобы отключить сетевой интерфейс, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Выберите сетевой интерфейс, который вы хотите отключить.

   Откроется окно **Изменить сетевой интерфейс**.
3. В строке **Состояние** переведите переключатель в положение **Отключено**.
4. Нажмите на кнопку **Сохранить**.

Сетевой интерфейс будет отключен.

Настройка параметров сетевого интерфейса

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить параметры сетевого интерфейса, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. Выберите сетевой интерфейс, параметры которого вы хотите настроить.

   Откроется окно **Изменить сетевой интерфейс**.
3. В строке **Режим** выберите один из следующих вариантов:
   - Если вы хотите, чтобы IP-адрес сетевого интерфейса был назначен с помощью DHCP-сервера, выберите **DHCP**.
   - Если вы хотите назначить сетевому интерфейсу статический IP-адрес, выберите **Статический**.
4. Если вы выбрали **Статический**, выполните следующие действия:
   a. В поле **IP** укажите IP-адрес сетевого интерфейса.
   b. В поле **Маска подсети** укажите маску подсети сетевого интерфейса.
5. Если вы хотите включить сетевой интерфейс, в строке **Состояние** переведите переключатель в положение **Включено**.
6. Нажмите на кнопку **Инициализировать**.

Параметры сетевого интерфейса будут настроены.

Настройка сетевого маршрута для использования по умолчанию

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить сетевой маршрут для использования по умолчанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В блоке параметров **Сетевой маршрут** в раскрывающемся списке **Сетевой интерфейс** выберите сетевой интерфейс, для которого вы хотите настроить сетевой маршрут.
3. В строке **Режим** выберите один из следующих вариантов:
   - Если вы хотите настроить сетевой маршрут с помощью DHCP-сервера, выберите **DHCP**.
   - Если вы хотите настроить статический сетевой маршрут, выберите **Статический**.
4. Если вы выбрали **Статический**, в поле **Шлюз** введите IP-адрес шлюза.
5. Нажмите на кнопку **Применить**.

Сетевой маршрут для использования по умолчанию будет настроен.

Настройка параметров соединения с прокси-сервером

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

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

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Прокси-сервер** переведите переключатель в положение **Включено**.
3. В поле **Хост** укажите URL-адрес прокси-сервера.
4. В поле **Порт** укажите порт подключения к прокси-серверу.
5. В поле **Имя пользователя** укажите имя пользователя для аутентификации на прокси-сервере.
6. В поле **Пароль** укажите пароль для аутентификации на прокси-сервере.
7. Если вы не хотите использовать прокси-сервер при подключении к локальным адресам, установите флажок **Не использовать прокси-сервер для локальных адресов**.
8. Нажмите на кнопку **Применить**.

Параметры соединения с прокси-сервером будут настроены.

Управление компонентом Sensor

Компонент Sensor выполняет прием данных из сетевого и почтового трафика.

Вы можете установить компоненты Sensor и Central Node на одном сервере или на отдельных серверах. Если компонент Sensor установлен на отдельном сервере, необходимо подключить его к серверу с компонентом Central Node.

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия по подключения к серверам PCN или SCN.

Обработка запроса на подключение от компонента Sensor

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Вы можете принять, отклонить или отозвать ранее принятый запрос на подключение от компонента Sensor.

► *Чтобы обработать запрос на подключение от компонента Sensor, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   В таблице **Список серверов** отобразятся уже подключенные компоненты Sensor, а также запросы на подключение.
2. В строке с запросом на подключение компонента Sensor выполните одно из следующих действий:
   - Если вы хотите подключить компонент Sensor, нажмите на кнопу **Принять**.
   - Если вы не хотите подключать компонент Sensor, нажмите на кнопку **Отклонить**.
3. В окне подтверждения нажмите на кнопку **Да**.

Запрос на подключение от компонента Sensor будет обработан.

Просмотр таблицы серверов с компонентом Sensor

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Таблица серверов с компонентом Sensor находится в разделе **Серверы Sensor** окна веб-интерфейса программы. В таблице содержится следующая информация:

- **IP/имя** – IP-адрес или доменное имя сервера с компонентом Sensor.
- **Тип** – тип компонента Sensor. Может принимать следующие значения:
  - **Central Node** – компонент Sensor установлен на том же сервере, что и компонент Central Node.
  - **Удаленный** – компонент Sensor установлен на другом сервере или в качестве компонента Sensor используется почтовый сенсор.

- **Отпечаток сертификата** – отпечаток TLS-сертификата, с помощью которого устанавливается шифрованное соединение между серверами с компонентами Sensor и Central Node.
- **KSN/KPSN** – состояние подключения к репутационным базам KSN/KPSN.
- **SPAN** – состояние обработки SPAN-трафика.
- **SMTP** – состояние интеграции с почтовым сервером по протоколу SMTP.
- **ICAP** – состояние интеграции с прокси-сервером по протоколу ICAP.
- **POP3** – состояние интеграции с почтовым сервером по протоколу POP3.
- **Состояние** – состояние запроса на подключение.

Настройка максимального размера проверяемого файла

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить максимальный размер проверяемого файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.
2. Выберите компонент Sensor, для которого вы хотите настроить максимальный размер проверяемого файла.

   Откроется страница с параметрами компонента Sensor.
3. Выберите раздел **Общие параметры**.
4. Если вы хотите, чтобы программа проверяла файлы любых размеров, установите флажок **Без ограничений**.
5. Если вы хотите установить максимальный размер, при превышении которого программа не будет проверять файлы, выполните следующие действия:
   a. Снимите флажок **Без ограничений**.
   b. В поле под флажком введите максимально допустимый размер файла.
   c. В раскрывающемся списке справа от поля выберите единицу измерения.
6. Нажмите на кнопку **Применить**.

Максимальный размер проверяемого файла будет настроен.

Настройка получения зеркалированного трафика со SPAN-портов

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить получение зеркалированного трафика со SPAN-портов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, для которого вы хотите настроить получение зеркалированного трафика со SPAN-портов.

   Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **Обработка SPAN-трафика**.

   Отобразится таблица **Сетевые интерфейсы**.

4. В строке сетевого интерфейса, с которого вы хотите настроить получение зеркалированного трафика, переведите переключатель в графе **Проверка SPAN-трафика** в положение **Включено**.

5. В раскрывающемся списке **Поток перехвата** выберите поток, который будет обрабатывать этот сетевой интерфейс.

6. В раскрывающемся списке **Выбор процессора** выберите процессор, который будет обрабатывать сетевой трафик.

7. Нажмите на кнопку **Применить**.

Получение зеркалированного трафика со SPAN-портов будет настроено.

Настройка интеграции с почтовым сервером по протоколу SMTP

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

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

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, для которого вы хотите настроить интеграцию с почтовым сервером по протоколу SMTP.

   Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **SMTP-интеграция**.

4. В поле **Состояние** переведите переключатель в положение **Включено**.

5. В поле **Домены назначения** укажите имя почтового домена или поддомена. Программа будет проверять сообщения электронной почты, отправленные на почтовые ящики указанных доменов.

   Чтобы отключить домен или поддомен, заключите его в форму `!domain.tld`.

   Если вы оставите имя почтового домена пустым, программа будет принимать сообщения, отправленные на любые адреса электронной почты.

6. В поле **Клиенты** укажите IP-адреса хостов и/или маски подсетей в нотации CIDR, с которыми программе разрешено взаимодействовать по протоколу SMTP.

   Чтобы отключить хост или подсеть, заключайте адрес в форму `!host`.

   Если вы оставите это поле пустым, программа будет принимать следующие сообщения:

   - с любых адресов электронной почты, если вы указали почтовые домены в поле **Домены назначения**;
   - от почтового сервера, находящегося в той же подсети, что и сервер с компонентом Sensor, если в поле **Домены назначения** не указан ни один домен.

7. Если вы хотите, чтобы программа принимала сообщения любых размеров, в группе параметров **Ограничение по размеру сообщения** установите флажок **Без ограничений**.
8. Если вы хотите установить максимально допустимый размер входящих сообщений, выполните следующие действия:
   a. Снимите флажок **Без ограничений**.
   b. В поле под флажком введите максимально допустимый размер сообщения.
   c. В раскрывающемся списке справа от поля выберите единицу измерения.
9. Нажмите на кнопку **Применить**.

Интеграция с почтовым сервером по протоколу SMTP будет настроена. Программа будет проверять сообщения электронной почты, полученные по протоколу SMTP, согласно заданным параметрам.

Настройка TLS-шифрования соединений с почтовым сервером по протоколу SMTP

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы настроить TLS-шифрование соединений с почтовым сервером по протоколу SMTP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.

2. Выберите компонент Sensor, для которого вы хотите настроить TLS-шифрование соединений с почтовым сервером по протоколу SMTP.

   Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **SMTP-интеграция**.
4. В поле **Состояние** переведите переключатель в положение **Включено**, если он выключен.

5. В блоке **Режим TLS-безопасности клиента** выберите один из следующих вариантов:
   - **Не использовать TLS-шифрование**.

     Программа не будет устанавливать TLS-шифрование соединений с почтовым сервером.
   - **Проверять возможность TLS-шифрования входящих сообщений**.

     Программа будет поддерживать TLS-шифрование соединений, но шифрование не будет являться обязательным.
   - **Требовать TLS-шифрование входящих сообщений**.

     Программа будет принимать сообщения только по зашифрованным каналам.
6. Нажмите на кнопку **Скачать TLS-сертификат**, чтобы сохранить TLS-сертификат сервера с компонентом Sensor на компьютере в папке загрузки браузера.

   Этот сертификат необходим для проверки подлинности на почтовом сервере.
7. В блоке **Запрос клиентского TLS-сертификата** выберите один из следующих вариантов:
   - **Не запрашивать**.

     Программа не будет проверять TLS-сертификат почтового сервера.
   - **Запрашивать**.

     Программа будет запрашивать у почтового сервера TLS-сертификат при его наличии.
   - **Требовать**.

     Программа будет принимать сообщения только от тех почтовых серверов, у которых есть TLS-сертификат.
8. Загрузите TLS-сертификат почтового сервера, который будет использован для проверки подлинности при установке соединения с компонентом Sensor. Для этого выполните следующие действия:
   a. Нажмите на кнопку **Загрузить TLS-сертификат**.

      Откроется окно выбора файла.
   b. Выберите файл сертификата с расширением .pem и нажмите на кнопку Открыть.
9. Нажмите на кнопку **Применить**.

TLS-шифрование соединений с почтовым сервером по протоколу SMTP будет настроено.

Включение интеграции с прокси-сервером по протоколу ICAP

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

► *Чтобы включить интеграцию с прокси-сервером по протоколу ICAP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.
2. Выберите компонент Sensor, для которого вы хотите настроить интеграцию с прокси-сервером по

протоколу ICAP.

Откроется страница с параметрами компонента Sensor.

3. Выберите раздел **ICAP-интеграция с прокси-сервером**.
4. В поле **Состояние** переведите переключатель в положение **Включено**.

   В поле **Хост** отобразится URL-адрес службы Response Modification (RESPMOD), которая обрабатывает входящий трафик.

   Используйте этот URL-адрес для настройки интеграции с Kaspersky Anti Targeted Attack Platform по протоколу ICAP на прокси-сервере, который используется в вашей организации.
5. Нажмите на кнопку **Применить**.

Интеграция с прокси-сервером по протоколу ICAP будет включена.

Настройка интеграции с почтовым сервером по протоколу POP3

Если вы используете режим распределенного решения и multitenancy (стр. 42), выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

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

1. В окне веб-интерфейса программы выберите раздел **Серверы Sensor**.

   Отобразится таблица **Список серверов**.
2. Выберите компонент Sensor, для которого вы хотите настроить интеграцию с почтовым сервером по протоколу POP3.

   Откроется страница с параметрами компонента Sensor.
3. Выберите раздел **POP3-интеграция**.
4. Переведите переключатель рядом с параметром **Состояние** в положение **Включено**.
5. В поле **Почтовый сервер** укажите IP-адрес почтового сервера, с которым вы хотите настроить интеграцию.
6. В поле **Порт** укажите порт подключения к почтовому серверу.
7. В поле **Принимать каждые** укажите частоту соединения с почтовым сервером в секундах.
8. Если вы хотите использовать TLS-шифрование соединений с почтовым сервером по протоколу POP3, установите флажок **Использовать TLS-шифрование**.
9. В поле **Имя пользователя** укажите имя учетной записи для доступа к почтовому серверу.
10. В поле **Пароль** укажите пароль доступа к почтовому серверу.
11. В раскрывающемся списке **TLS-сертификат** выберите один из следующих вариантов:
    - **Принимать любой**.
    - **Принимать недоверенный самоподписанный**.
    - **Принимать только доверенный**.

При установке соединения с внешним почтовым сервером рекомендуется настроить прием только доверенных TLS-сертификатов. Прием недоверенных TLS-сертификатов не гарантирует защиту соединения от MITM-атак. Прием доверенных TLS-сертификатов также не полностью гарантирует защиту соединения от MITM-атак, но является самым безопасным из поддерживаемых способов интеграции с почтовым сервером по протоколу POP3.

12. При необходимости в поле **Набор шифров** измените параметры OpenSSL, используемые при установке соединения с почтовым сервером по протоколу POP3.

    Вы можете ознакомиться со справочной информацией OpenSSL по ссылке **Справка**.

13. Нажмите на кнопку **Применить**.

Интеграция с почтовым сервером по протоколу POP3 будет настроена.

Управление компонентом Endpoint Sensors

Компонент Endpoint Sensors (стр. 39) устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**, **Локальный администратор** и **Администратор** могут оценить регулярность получения данных с хостов, на которых установлен компонент Endpoint Sensors, на закладке **Endpoint Sensors** окна веб-интерфейса программы в рамках тех организаций, к данным которых у них есть доступ (стр. 158). Если вы используете режим распределенного решения и multitenancy, то в веб-интерфейсе сервера PCN отображается список компонентов Endpoint Sensors для PCN и всех подключенных SCN.

Пользователи с ролью **Локальный администратор** и **Администратор** могут настроить отображение регулярности получения данных с хостов, на которых установлен компонент Endpoint Sensors, в рамках тех организаций, к данным которых у них есть доступ (стр. 158).

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети (стр. 294) любой из хостов с компонентом Endpoint Sensors в рамках тех организаций, к данным которых у него есть доступ (стр. 158). При этом соединение между сервером с компонентом Central Node и хостом с компонентом Endpoint Sensors не будет прервано.

Для оказания поддержки при неполадках в работе компонента Endpoint Sensors специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode (стр. 152)):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов программы.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

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

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

Выбор организации для работы в разделе Endpoint Sensors

Если вы используете режим multitenancy, перед началом работы в разделе **Endpoint Sensors** вам нужно выбрать организацию, данные по которой вас интересуют.

► *Чтобы выбрать организацию для работы в разделе **Endpoint Sensors**, выполните следующие действия:*

1. В верхней части меню веб-интерфейса программы нажмите на стрелку рядом с названием организации.
2. В раскрывшемся списке выберите организацию.

Отобразятся данные по выбранной вами организации. Если вы хотите изменить организацию, вам нужно повторить действия по выбору организации.

Просмотр таблицы Endpoint Sensors на отдельном сервере Central Node

Таблица хостов с компонентом Endpoint Sensors находится в разделе **Endpoint Sensors** окна веб-интерфейса программы.

Если вы используете отдельный сервер Central Node, не используете интеграцию с KSC, режим распределенного решения и multitenancy, в таблице хостов с компонентом Endpoint Sensors могут отображаться следующие данные:

- **Хост** – имя хоста с компонентом Endpoint Sensors.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Версия** – версия установленного компонента Endpoint Sensors.
- **Активность** – показатель активности компонента Endpoint Sensors. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Просмотр таблицы Endpoint Sensors на отдельном сервере Central Node при интеграции с KSC

Если вы настроили интеграцию с KSC, таблица хостов с компонентом Endpoint Sensors находится в разделе **Endpoint Sensors** окна веб-интерфейса программы.

В разделе **Endpoint Sensors** отображаются следующие подразделы:

- **Central Node**. Отображается информация о хостах с компонентом Endpoint Sensors, подключенных к этому серверу Central Node.
- **KSC**. Отображается информация о всех хостах, подключенных к KSC.

В подразделе **Central Node** может отображаться следующая информация:

- **Хост** – имя хоста с компонентом Endpoint Sensors.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Версия** – версия установленного компонента Endpoint Sensors.
- **Активность** – показатель активности компонента Endpoint Sensors. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

В подразделе **KSC** может отображаться следующая информация:

- **Хост** – имя хоста с компонентом Endpoint Sensors.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Endpoint Sensor** – тип компонента, используемого в качестве Endpoint Sensors.

  Компонент может быть одного из следующих типов:
  - **Endpoint Sensor**.

    Компонент Endpoint Sensors (стр. 39), который был установлен из пакета Kaspersky Anti Targeted Attack Platform.
  - **В составе KES**.

    Компонент Endpoint Sensors, входящий в состав программы Kaspersky Endpoint Security для Windows.
- **Версия** – версия установленного компонента Endpoint Sensors.
- **Сервер** – имя сервера с компонентом Central Node.
- **Состояние сенсора** – статус компонента Endpoint Sensors, установленного на компьютере.

  Компонент Endpoint Sensors может иметь один из следующих статусов:
  - **Запущен**.
  - **Остановлен**.

  - **Сбой**.
  - **Не установлен**.
- **Состояние хоста** – состояние хоста компьютера с компонентом Endpoint Sensors.

  Хост может находиться в одном из следующих состояний:

  - **Отключено**.
  - **Онлайн**.
- **С ошибкой** – статус наличия ошибок в работе компонента Endpoint Sensors. Статус может принимать значение **Нет ошибок** или содержать информацию о типе ошибки работы компонента Endpoint Sensors.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

По ссылке с IP-адресом компьютера, на который установлен компонент Endpoint Sensors, вы также можете выбрать действие **Перейти к обнаружениям, отфильтрованным по этому значению**.

По ссылке с именем хоста, на который установлен компонент Endpoint Sensors, вы также можете выбрать действия:

- **Изолировать от сети**.
- **Найти события**.
- **Найти обнаружения**.

Просмотр таблицы Endpoint Sensors в режиме распределенного решения и multitenancy

Таблица хостов с компонентом Endpoint Sensors находится в разделе **Endpoint Sensors** окна веб-интерфейса программы.

Если вы используете режим распределенного решения и multitenancy и не используете интеграцию с KSC, в таблице содержится информация о компонентах Endpoint Sensors, подключенных к PCN и всем серверам SCN. В таблице могут отображаться следующие данные:

- **Хост** – имя хоста с компонентом Endpoint Sensors.

  По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Новое правило запрета**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.

- **Серверы** – имена серверов, к которым подключен хост с компонентом Endpoint Sensors.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Версия** – версия установленного компонента Endpoint Sensors.
- **Активность** – показатель активности компонента Endpoint Sensors. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

По ссылке с IP-адресом компьютера, на который установлен компонент Endpoint Sensors, вы также можете выбрать действие **Перейти к обнаружениям, отфильтрованным по этому значению**.

Просмотр информации о хосте

► *Чтобы просмотреть информацию о хосте с компонентом Endpoint Sensors, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. Выберите хост, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- **Состояние** – состояние хоста с компонентом Endpoint Sensors.

  Хост может находиться в одном из следующих состояний:
  - **Онлайн**.
  - **Отключено**.
- **Хост** – имя хоста компьютера с компонентом Endpoint Sensors.

  По ссылке с именем хоста вы можете выполнить действие **Скопировать значение в буфер**.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, на компьютере, на который установлен компонент Endpoint Sensors.

- **Защита** – состояние защиты хоста с компонентом Endpoint Sensors.
- **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и multitenancy.
- **Имя сервера** – имя сервера Central Node.
- **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
- **Версия** – тип и версия установленного компонента Endpoint Sensors.
- **Состояние** – состояние компонента Endpoint Sensors.

Фильтрация и поиск Endpoint Sensors по имени хоста

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по имени хоста, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **Хост** откройте окно настройки фильтрации.
4. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Sensors**.
5. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
6. В поле ввода укажите один или несколько символов имени хоста.
7. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
8. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
9. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors, изолированных от сети

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors, изолированные*

от сети (стр. 294), выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **Хост** откройте окно настройки фильтрации.
4. Установите флажок **Показывать только изолированные Endpoint Sensors**.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по именам серверов PCN и SCN

Если вы используете режим распределенного решения и multitenancy, вы можете отфильтровать или найти хосты с компонентом Endpoint Sensors по именам серверов PCN и SCN, к которым подключены эти хосты.

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по именам серверов PCN и SCN, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. По ссылке **Серверы** откройте окно настройки фильтрации.
3. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с компонентом Endpoint Sensors.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по IP-адресу компьютера

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по IP-адресу компьютера, на котором установлен компонент Endpoint Sensors, выполните следующие*

действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **IP** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по версии операционной системы на компьютере

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по версии операционной системы, установленной на компьютере с компонентом Endpoint Sensors, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.

3. По ссылке **ОС** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов версии операционной системы.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по версии компонента Endpoint Sensor

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по версии компонента Endpoint Sensors, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **Версия** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов версии компонента Endpoint Sensors.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.

8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по их активности

► *Чтобы отфильтровать или найти компоненты Endpoint Sensors по их активности, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.

2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **Активность** откройте окно настройки фильтрации.
4. Установите флажки рядом с одним или несколькими показателями активности компонента Endpoint Sensors (стр. 211):
   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра компьютеров с компонентом Endpoint Sensors

► *Чтобы быстро создать фильтр хостов с компонентом Endpoint Sensors, выполните*

следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.

2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:

   - **Central Node**.
   - **KSC**.

3. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением графы таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

4. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра Endpoint Sensors

► *Чтобы сбросить фильтр хостов с компонентом Endpoint Sensors по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:

   - **Central Node**.
   - **KSC**.

3. Нажмите на кнопку  справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Настройка показателей активности Endpoint Sensors

Пользователи с ролью **Локальный администратор** и **Администратор** могут определить, какой период бездействия компонентов Endpoint Sensors считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности компонентов Endpoint Sensors. Просматривать показатели активности Endpoint Sensors могут все пользователи.

► *Чтобы настроить показатели активности компонентов Endpoint Sensors, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью **Локальный администратор** или **Администратор**.
2. В окне веб интерфейса программы выберите раздел **Параметры**, подраздел **Endpoint Sensors**.
3. В полях под названием раздела введите количество дней бездействия компьютеров с компонентом Endpoint Sensors, которое вы хотите отображать как **Предупреждение** и **Критическая**.
4. Нажмите на кнопку **Применить**.

Пользователи с правами **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** смогут увидеть настроенные вами показатели активности компонентов Endpoint Sensors в графе **Активность** таблицы хостов с компонентом Endpoint Sensors в разделе **Endpoint Sensors** окна веб-интерфейса программы.

Создание задачи для перезапуска компонентов Endpoint Sensors в KSC

Вы можете создать групповую задачу для перезапуска компонентов Endpoint Sensors на всех компьютерах в Консоли администрирования Kaspersky Security Center. Если интеграция программы с Kaspersky Security Center не настроена, вы можете использовать для перезапуска компонентов групповую политику Windows. Подробнее о групповых политиках см. в документации к операционной системе.

► *Чтобы создать групповую задачу для перезапуска компонентов Endpoint Sensors, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке с управляемыми устройствами дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку со списком задач.
4. Нажмите на кнопку создания задачи.

   Запустится мастер создания задачи.
5. В окне выбора типа задачи выберите запуск или остановку программы.
6. Следуйте указаниям мастера создания задачи.

Задача для перезапуска службы компонентов Endpoint Sensors будет создана. Подробнее о групповых задачах и запуске задач см. Справку Kaspersky Security Center https://help.kaspersky.com/KSC/SP3/ru-RU/5022.htm.

Настройка интеграции с компонентом Sandbox

Вы можете подключить один компонент Sandbox к нескольким компонентам Central Node.

Предусмотрен следующий порядок настройки соединения компонента Sandbox с компонентом Central Node:

a. **Создание запроса на подключение к компоненту Sandbox**

Вы можете создать запрос в меню администратора (стр. 166) или в веб-интерфейсе программы (стр. 212) под учетной записью администратора. Необходимо создавать запрос для каждого сервера с компонентом Central Node, который вы хотите подключить к компоненту Sandbox.

b. **Обработка запроса на подключение (стр. 167) в веб-интерфейсе Sandbox**

Вы можете принять или отклонить каждый запрос.

Просмотр таблицы серверов с компонентом Sandbox

Таблица серверов с компонентом Sandbox находится на закладке **Серверы Sandbox** окна веб-интерфейса программы.

Таблица содержит следующую информацию:

- **IP и имя** – IP-адрес или полное доменное имя сервера с компонентом Sandbox.
- **Отпечаток сертификата** – отпечаток сертификата сервера с компонентом Sandbox.
- **Авторизация** – статус запроса на подключение к компоненту Sandbox.
- **Состояние** – состояние подключения к компоненту Sandbox.

Создание запроса на подключение к серверу с компонентом Sandbox

► *Чтобы создать запрос на подключение к серверу с компонентом Sandbox через веб-интерфейс программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sandbox**.
2. В правом верхнем углу окна нажмите на кнопку **Добавить**.

   Откроется окно **Подключение сервера Sandbox**.
3. В поле **IP** укажите IP-адрес сервера с компонентом Sandbox, к которому вы хотите подключиться.
4. Нажмите на кнопку **Получить отпечаток сертификата**.

   В рабочей области отобразится отпечаток сертификата сервера с компонентом Sandbox.
5. Сравните полученный отпечаток сертификата с отпечатком, указанным в веб-интерфейсе Sandbox в разделе **Авторизация KATA** в поле **Отпечаток сертификата**.

   Если отпечатки сертификата совпадают, выполните дальнейшие шаги инструкции.

Не рекомендуется подтверждать подключение при несовпадении отпечатков сертификата. Убедитесь в правильности введенных данных.

6. В поле **Имя** укажите имя компонента Sandbox, которое будет отображаться в веб-интерфейсе компонента Central Node.

   Это имя не связано с именем хоста, на котором установлен Sandbox.

7. Если вы хотите сделать соединение с Sandbox активным сразу после подключения, установите флажок **Включить**.

8. Нажмите на кнопку **Добавить**.

Запрос на подключение отобразится в веб-интерфейсе компонента Sandbox.

Включение и отключение соединения с компонентом Sandbox

► *Чтобы сделать соединение с компонентом Sandbox активным или отключить его, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sandbox**.

   Отобразится таблица серверов с компонентами Sandbox.

2. В строке с нужным сервером в графе **Состояние** выполните одно из следующих действий:

   - Если вы хотите сделать соединение с компонентом Sandbox активным, переведите переключатель в положение **Включено**.
   - Если вы хотите отключить соединение с компонентом Sandbox, переведите переключатель в положение **Отключено**.

3. Нажмите на кнопку **Применить**.

Соединение с компонентом Sandbox станет активным или будет отключено.

Удаление соединения с компонентом Sandbox

► *Чтобы удалить соединение с компонентом Sandbox, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Серверы Sandbox**.

   Отобразится таблица компьютеров, на которых установлен компонент Sandbox.

2. Установите флажок в строке с компонентом Sandbox, соединение с которым вы хотите удалить.

3. В правом верхнем углу окна нажмите на кнопку **Удалить**.

4. В окне подтверждения нажмите на кнопку **Да**.

Соединение с компонентом Sandbox будет удалено.

Настройка интеграции с внешними системами

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с внешними системами для проверки хранящихся в них файлов. Результаты их проверки будут отображаться в таблице обнаружений (стр. 238).

В роли внешней системы может выступать почтовый сенсор – программа "Лаборатории Касперского" Kaspersky Secure Mail Gateway или Kaspersky Security для Linux Mail Server. Почтовый сенсор отправляет сообщения электронной почты на обработку в Kaspersky Anti Targeted Attack Platform. По результатам обработки сообщений электронной почты в Kaspersky Anti Targeted Attack Platform почтовый сенсор может блокировать пересылку сообщений.

Предусмотрен следующий порядок интеграции Kaspersky Anti Targeted Attack Platform с внешними системами:

a. **Ввод параметров интеграции и создание запроса на интеграцию на стороне внешней системы**

Подробнее о вводе параметров интеграции на стороне почтового сенсора см. Справку Kaspersky Secure Mail Gateway https://help.kaspersky.com/KSMG/1.1.2/ru-RU/100512.htm или Справку Kaspersky Security для Linux Mail Server https://help.kaspersky.com/KLMS/8.2/ru-RU/100512.htm.

Для интеграции других внешних систем необходимо использовать REST API.

b. **Подтверждение интеграции на стороне Kaspersky Anti Targeted Attack Platform (стр. 215)**

Внешние системы могут использовать одинаковые идентификаторы и сертификаты для авторизации на сервере с компонентом Central Node. В этом случае в интерфейсе Kaspersky Anti Targeted Attack Platform будет отображаться один запрос на интеграцию.

c. **Проверка соединения внешней системы с Kaspersky Anti Targeted Attack Platform**

Просмотр таблицы внешних систем

Таблица внешних систем находится в разделе **Внешние системы** окна веб-интерфейса программы. В таблице содержится следующая информация:

- **Sensor** – IP-адрес или доменное имя сервера внешней системы.
- **Тип** – тип внешней системы (почтовый сенсор или другая система).
- **Имя** – название интегрированной внешней системы, не являющейся почтовым сенсором.

  Для почтового сенсора в этой графе отображается прочерк.
- **ID** – идентификатор внешней системы.
- **Отпечаток сертификата** – отпечаток TLS-сертификата сервера с внешней системой, с помощью которого устанавливается шифрованное соединение с сервером с компонентом Central Node.

  > Отпечаток сертификата сервера с компонентом Central Node отображается в верхней части окна в поле **Отпечаток сертификата**.

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

Обработка запроса от внешней системы

► *Чтобы обработать запрос на интеграцию от внешней системы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Внешние системы**.

   В таблице **Список серверов** отобразятся уже подключенные внешние системы, а также запросы на интеграцию с Kaspersky Anti Targeted Attack Platform от внешних систем.

2. В строке с запросом на интеграцию выполните одно из следующих действий:

   - Если вы хотите настроить интеграцию с внешней системой, нажмите на кнопу **Принять**.
   - Если вы не хотите настраивать интеграцию с внешней системой, нажмите на кнопку **Отклонить**.

3. В окне подтверждения нажмите на кнопку **Да**.

Запрос на интеграцию от внешней системы будет обработан.

Удаление внешней системы из списка разрешенных к интеграции

После того как вы приняли запрос на интеграцию от внешней системы, вы можете удалить ее из списка разрешенных к интеграции. В этом случае соединение между Kaspersky Anti Targeted Attack Platform и внешней системой будет прервано.

► *Чтобы удалить внешнюю систему из списка разрешенных к интеграции, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Внешние системы**.

   В списке **Список серверов** отобразятся уже добавленные внешние системы, а также запросы на интеграцию с Kaspersky Anti Targeted Attack Platform от внешних систем.

2. Нажмите на кнопку **Удалить** в строке с запросом на интеграцию от той внешней системы, которую вы хотите удалить.

3. В окне подтверждения нажмите на кнопку **Да**.

Внешняя система будет удалена из списка разрешенных к интеграции.

Настройка приоритета обработки трафика от почтовых сенсоров

Вы можете включить или отключить максимальный приоритет обработки трафика от почтовых сенсоров.

► *Чтобы включить или отключить максимальный приоритет обработки трафика от почтовых сенсоров, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Внешние системы**.

2. Выполните одно из следующих действий:

   - Включите переключатель рядом с названием параметра **Обрабатывать трафик с максимальным приоритетом**, если вы хотите включить максимальный приоритет обработки трафика от почтовых сенсоров.
   - Выключите переключатель рядом с названием параметра **Обрабатывать трафик с максимальным приоритетом**, если вы хотите отключить максимальный приоритет обработки трафика от почтовых сенсоров.

Приоритет обработки трафика от почтовых сенсоров будет настроен.

Настройка интеграции с SIEM-системой

Kaspersky Anti Targeted Attack Platform может публиковать обнаружения в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

Для передачи данных вы можете использовать TLS-шифрование.

Включение и отключение записи событий в локальный журнал

Вы можете настроить запись событий в локальный журнал, хранящийся на компьютере с компонентом Central Node. Файл этого журнала можно импортировать в SIEM-систему, для которой не настроена интеграция с программой.

► *Чтобы включить или отключить запись событий в локальный журнал, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Выполните одно из следующих действий:
   - Включите переключатель рядом с названием параметра **Локальный журнал**, если вы хотите включить запись событий в локальный журнал.
   - Выключите переключатель рядом с названием параметра **Локальный журнал**, если вы хотите отключить запись событий в локальный журнал.
3. Нажмите на кнопку **Применить** в нижней части окна.

Запись событий в локальный журнал будет включена или отключена.

Включение и отключение записи событий в удаленный журнал

Удаленный журнал хранится на сервере, на котором установлена SIEM-система. Для записи в удаленный журнал должны быть настроены параметры интеграции с SIEM-системой (стр. 217).

► *Чтобы включить или отключить запись событий в удаленный журнал, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Выполните одно из следующих действий:
   - Включите переключатель рядом с названием параметра **Удаленный журнал**, если вы хотите включить запись событий в удаленный журнал.
   - Выключите переключатель рядом с названием параметра **Удаленный журнал**, если вы хотите отключить запись событий в удаленный журнал.
3. Нажмите на кнопку **Применить** в нижней части окна.

Настройка основных параметров интеграции с SIEM-системой

► *Чтобы настроить основные параметры интеграции с SIEM-системой, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Включите переключатель рядом с названием параметра **Удаленный журнал**, если он выключен.
3. В поле **Хост/IP** введите IP-адрес или имя хоста сервера вашей SIEM-системы.
4. В поле **Порт** введите номер порта подключения к вашей SIEM-системе.
5. В поле **Протокол** выберите **TCP** или **UDP**.
6. В поле **ID внешнего устройства** укажите идентификатор устройства, на котором установлена ваша SIEM-система.
7. В поле **Периодичность сигнала** введите интервал отправки сообщений в SIEM-систему о статусе компонентов Kaspersky Anti Targeted Attack Platform.
8. Нажмите на кнопку **Применить** в нижней части окна.

Основные параметры интеграции с SIEM-системой будут настроены.

Включение и отключениеTLS-шифрования соединения с SIEM-системой

► *Чтобы включить или отключить TLS-шифрование соединения с SIEM-системой, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Включите переключатель рядом с названием параметра **Удаленный журнал**, если он выключен.
3. В разделе **TLS-шифрование** выполните одно из следующих действий:
   - Включите переключатель рядом с названием параметра **TLS-шифрование**, если вы хотите включить TLS-шифрование соединения с SIEM-системой.
   - Выключите переключатель рядом с названием параметра **TLS-шифрование**, если вы хотите отключить TLS-шифрование соединения с SIEM-системой.

   Переключатель рядом с названием параметра **TLS-шифрование** доступен только если загружен TLS-сертификат.
4. Нажмите на кнопку **Применить** в нижней части окна.

TLS-шифрование соединения с SIEM-системой будет включено или отключено.

Загрузка TLS-сертификата

► *Чтобы загрузить TLS-сертификат для шифрования соединения с SIEM-системой, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Включите переключатель рядом с названием параметра **Удаленный журнал**, если он выключен.
3. В разделе **TLS-шифрование** нажмите на кнопку **Загрузить**.

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

   Окно выбора файлов закроется.

   TLS-сертификат будет добавлен в программу.
5. Нажмите на кнопку **Применить** в нижней части окна.

Загруженный TLS-сертификат будет использоваться для шифрования соединения с SIEM-системой.

Содержание и свойства syslog-сообщений об обнаружениях

Информация о каждом обнаружении передается в отдельной syslog-категории (syslog facility), не использующейся системой для передачи сообщений от других источников. Информация о каждом обнаружении передается как отдельное syslog-сообщение формата CEF. Если обнаружение выполнено модулем Targeted Attack Analyzer, то информация о нем передается как несколько отдельных syslog-сообщений формата CEF.

Максимальный размер syslog-сообщения об обнаружении по умолчанию составляет 32 Кб. Сообщения, превышающие максимальный размер, обрываются в конце.

В заголовке каждого syslog-сообщения об обнаружении содержится следующая информация:

- Версия формата.

  Номер текущей версии: `0`. Текущее значение поля: `CEF:0`.

- Производитель.

  Текущее значение поля: `AO Kaspersky Lab`.

- Название программы.

  Текущее значение поля: `Kaspersky Anti Targeted Attack Platform`.

- Версия программы.

  Текущее значение поля: `3.6`.

- Тип обнаружения.

  См. таблицу ниже.

- Наименование события.

  См. таблицу ниже.

- Важность обнаружения.

  Допустимые значения поля: `Low`, `Medium`, `High` или `0` (для сообщений типа `heartbeat`).

- Дополнительная информация.

Пример:

```
CEF:0|AO Kaspersky Lab| Kaspersky Anti Targeted Attack Platform |3.6|url_web|
URL from web detected|Low|
```

Тело syslog-сообщения об обнаружении соответствует информации об этом обнаружении, отображающейся в веб-интерфейсе программы. Все поля представлены в формате `"<ключ>=<значение>"`. В зависимости от того, в сетевом или почтовом трафике произошло обнаружение, а также от технологии, которая выполнила обнаружение, в теле syslog-сообщения могут передаваться разные ключи. Если значение пустое, то ключ не передается.

Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Таблица 12. Информация об обнаружении в syslog-сообщениях

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
`file_web`	`File from web detected` В сетевом трафике обнаружен файл.	• `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения>. • `dst` = <IP-адрес назначения>. • `dpt` = <порт назначения>. • `src` = <IP-адрес источника>. • `spt` = <порт источника>. • `shost` = <имя хоста, на котором обнаружен файл>. • `suser` = <имя пользователя>. • `fName` = <имя файла внутри составного объекта>. • `fsize` = <размер файла внутри составного объекта (в байтах)>. • `fileType` = <формат файла внутри составного объекта>. • `fileHash` = <MD5-хеш файла внутри составного объекта >. • `KasperskyLabKATAcompositeFilePath` = <имя составного объекта>. • `KasperskyLabKATAcompositeFileSize` = <общий размер составного объекта (в байтах)>. • `KasperskyLabKATAcompositeFileHash` = <MD5-хеш составного объекта>. • `KasperskyLabKATAfileSHA256` = <SHA256-хеш составного объекта>. • `cs2` = <технология, с помощью которой обнаружен файл>. • `cs3Label` = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). • `cs1` = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. • `cs3` = <версия баз, с помощью которых проверен файл>. • `app` = <название протокола прикладного уровня> (HTTP(S) или FTP). • `requestMethod` = <метод HTTP-запроса> (только для протокола HTTP(S)). • `requestClientApplication` = <User Agent клиентского компьютера> (только для протокола HTTP(S)). • `request` = <URL обнаруженного объекта> (только для протокола HTTP(S)). • `requestContext` = <HTTP-заголовок Referer> (только для протокола HTTP(S)).

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
file_mail	File from mail detected В почтовом трафике обнаружен файл.	• eventId = <ID обнаружения>. • rt = <дата и время обнаружения>. • fName = <имя файла внутри составного объекта>. • fsize = <размер файла внутри составного объекта (в байтах)>. • fileType = <формат файла внутри составного объекта >. • fileHash = <MD5-хеш файла внутри составного объекта >. • KasperskyLabKATAcompositeFilePath = <имя составного объекта>. • KasperskyLabKATAcompositeFileSize = <общий размер составного объекта (в байтах)>. • KasperskyLabKATAcompositeFileHash = <MD5-хеш составного объекта>. • KasperskyLabKATAfileSHA256 = <SHA256-хеш составного объекта>. • cs2 = <технология, с помощью которой обнаружен файл>. • cs3Label = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). • cs1 = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. • cs3 = <версия баз, с помощью которых проверен файл>. • externalId = <ID сообщения электронной почты>. • suser = <адрес электронной почты отправителя>. • duser = <адреса электронной почты получателей>. • msg = <тема сообщения>.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
ids	IDS event detected Обнаружение выполнено модулем Intrusion Detection System.	• eventId = <ID обнаружения>. • requestMethod = <метод HTTP-запроса> (только для протокола HTTP(S)). • requestClientApplication = <User Agent клиентского компьютера> (только для протокола HTTP(S)). • rt = <дата и время обнаружения>. • dst = <IP-адрес назначения>. • dpt = <порт назначения>. • src = <IP-адрес источника>. • spt = <порт источника>. • proto = <название протокола сетевого уровня> (TCP или UDP). • cs1 = <тип обнаруженного объекта по классификации "Лаборатории Касперского">. • cs2Label = <название правила IDS>. • cs2 = <номер правила IDS>. • cs3 = <версия баз модуля Intrusion Detection System>. • requestMethod = <метод HTTP-запроса> (только для протокола HTTP). • requestClientApplication = <User Agent клиентского компьютера> (только для протокола HTTP). • request = <URL обнаруженного объекта>.
url_web	URL from web detected Обнаружение выполнено технологией URL Reputation в сетевом трафике.	• eventId = <ID обнаружения>. • rt = <дата и время обнаружения>. • dst = <IP-адрес назначения>. • dpt = <порт назначения>. • src = <IP-адрес источника>. • spt = <порт источника>. • shost = <имя хоста, на котором обнаружен файл>. • suser = <имя пользователя>. • cs1 = <список категорий, к которым принадлежит URL-адрес обнаруженного объекта>. • requestMethod = <метод HTTP-запроса>. • requestClientApplication = <User Agent клиентского компьютера>. • request = <URL-адрес обнаруженного объекта>. • requestContext = <HTTP-заголовок Referer>. • reason = <код HTTP-ответа>.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
`url_mail`	`URL from mail detected` Обнаружение выполнено технологией URL Reputation в почтовом трафике.	• `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения>. • `externalId` = <ID сообщения электронной почты>. • `suser` = <адрес электронной почты отправителя>. • `duser` = <адреса электронной почты получателей>. • `msg` = <тема сообщения>. • `request` = <URL-адрес обнаруженного объекта>. • `cs2` = <технология, с помощью которой выполнено обнаружение> (Sandbox или URL Reputation). • `cs3Label` = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). • `cs1` = <список типов обнаруженных объектов по классификации "Лаборатории Касперского"> (для компонента Sandbox) или <список категорий> (для технологии URL Reputation). • `cs3` = <версия баз, с помощью которых проверен файл> (для компонента Sandbox).
`dns`	`DNS request detected` Обнаружение выполнено технологией URL Reputation в DNS-трафике.	• `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения>. • `dst` = <IP-адрес назначения>. • `dpt` = <порт назначения>. • `src` = <IP-адрес источника>. • `spt` = <порт источника>. • `shost` = <имя хоста, на котором обнаружен файл>. • `suser` = <имя пользователя>. • `cs2` = <список URL-категорий, к которым принадлежат доменные имена>. • `requestMethod` = <тип DNS-сообщения> (request или response). • `flexString1` = <тип записи из DNS-запроса>. • `dhost` = <имя хоста из DNS-запроса>. • `cs1` = <список доменных имен из DNS-ответа>.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
taa	Suspicious process activity Обнаружение выполнено технологией Targeted Attack Analyzer. Подозрительная активность процесса.	• eventId = <ID обнаружения>. • rt = <дата и время обнаружения>. • src = <IP-адрес источника>. • shost = <имя хоста, на котором обнаружен файл>. • fName = <имя файла внутри составного объекта>. • fileHash = <MD5-хеш файла внутри составного объекта>. • FilePath = <путь к файлу на компьютере с компонентом Endpoint Sensors>. • KasperskyLabKATAfileSHA256 = <SHA256-хеш составного объекта>. • cs1 = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">.
taa	Suspicious remote host activity Обнаружение выполнено технологией Targeted Attack Analyzer. Подозрительная активность удаленного хоста.	• eventId = <ID обнаружения>. • rt = <дата и время обнаружения>. • src = <IP-адрес источника>. • shost = <имя хоста, на котором обнаружен файл>. • dhost = <имя удаленного хоста>. • cs1 = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
file_endpoint	File from endpoint detected Обнаружение выполнено компонентом Endpoint Sensors на компьютере пользователя и содержит файл.	• eventId = <ID обнаружения>. • rt = <дата и время обнаружения>. • src = <IP-адрес источника>. • shost = <имя хоста, на котором обнаружен файл>. • fName = <имя файла внутри составного объекта>. • fsize = <размер файла внутри составного объекта (в байтах)>. • fileType = <формат файла внутри составного объекта >. • fileHash = <MD5-хеш файла внутри составного объекта >. • KasperskyLabKATAcompositeFilePath = <имя составного объекта>. • KasperskyLabKATAcompositeFileSize = <общий размер составного объекта (в байтах)>. • KasperskyLabKATAcompositeFileHash = <MD5-хеш составного объекта>. • KasperskyLabKATAfileSHA256 = <SHA256-хеш составного объекта>. • cs2 = <технология, с помощью которой обнаружен файл>. • cs3Label = <имя виртуальной машины, на которой обнаружен файл> (только для компонента Sandbox). • cs1 = <список типов обнаруженных объектов по классификации "Лаборатории Касперского">. • cs3 = <версия баз, с помощью которых проверен файл>. • app = <название протокола прикладного уровня> (HTTP(S) или FTP). • FilePath = <путь к файлу на компьютере с компонентом Endpoint Sensors>.
iocScanningEP	IOC has tripped on endpoint Обнаружение выполнено во время IOC-проверки компьютеров с компонентом Endpoint Sensors. Этот тип обнаружений доступен, если вы используете только функциональность KEDR.	• eventId = <ID обнаружения>. • rt = <дата и время обнаружения>. • src = <IP-адрес источника>. • shost = <имя хоста, на котором обнаружен файл>. • cs1 = <имя IOC-файла>.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
`iocScanning`	`IOC has tripped on events database` Обнаружение выполнено во время IOC-проверки базы событий. Этот тип обнаружений доступен, если вы используете только функциональность KEDR.	• `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения>. • `shost` = <имя хоста, на котором обнаружен файл>. • `cs1` = <имя IOC-файла>.
`heartbeat`	Периодическое сообщение, содержащее статус компонентов.	• `dvc` = <IP-адрес сервера с компонентом Central Node>. • `rt` = <дата и время события>. • `KasperskyLabKATAcomponentName` = <название компонента>. • `KasperskyLabKATAcomponentState` = <статус компонента> (`0` – ОК, `>0` – Ошибка).

Настройка интеграции с Kaspersky Security Center

Интеграция с Kaspersky Security Center недоступна в режиме распределенного решения (стр. 42).

При работе в веб-интерфейсе программы пользователь с ролью **Администратор** может настроить интеграцию с программой Kaspersky Security Center и получать статистику работы компонента Endpoint Sensors.

Для интеграции с программой Kaspersky Security Center вам необходимо создать в программе Kaspersky Security Center учетную запись пользователя.

► *Чтобы настроить необходимые права учетной записи пользователя, выполните следующие действия:*

1. Откройте консоль KSC.
2. Откройте окно свойств нужного Сервера администрирования.
3. В левой части окна свойств сервера выберите раздел с параметрами безопасности.
4. В правой части окна свойств сервера выберите учетную запись пользователя, права которого вы хотите настроить.
5. Предоставьте пользователю права на следующие действия:
   a. Чтение и изменение – в узле общего функционала в папке базовой функциональности.
   b. Чтение и выполнение – в узле общего функционала в папке операций с Сервером администрирования.
   c. Чтение и создание туннелей – в узле управления системой в папке подключений.
6. Сохраните изменения.

Подробную информацию о работе в программе Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Включение и отключение интеграции с Kaspersky Security Center

Интеграция с Kaspersky Security Center недоступна в режиме распределенного решения (стр. 42).

► *Чтобы включить или отключить интеграцию с Kaspersky Security Center, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Интеграция с Kaspersky Security Center**.
2. Выполните одно из следующих действий:
   - Включите переключатель рядом с названием параметра **Интеграция**, если вы хотите включить интеграцию с Kaspersky Security Center.

Интеграция с Kaspersky Security Center будет включена.

- Выключите переключатель рядом с названием параметра **Интеграция**, если вы хотите отключить интеграцию с Kaspersky Security Center.

  Интеграция с Kaspersky Security Center будет отключена.

Настройка параметров интеграции с Kaspersky Security Center

Интеграция с Kaspersky Security Center недоступна в режиме распределенного решения (стр. 42).

► *Чтобы настроить параметры интеграции с Kaspersky Security Center, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Интеграция с Kaspersky Security Center**.
2. Включите переключатель рядом с названием параметра **Интеграция**, если он выключен.
3. В поле **Хост/IP** введите IP-адрес Kaspersky Security Center.
4. В поле **Порт** введите порт подключения к Kaspersky Security Center.
5. В поле **Имя пользователя KSC** введите имя пользователя с правами администратора Kaspersky Security Center.
6. В поле **Пароль KSC** введите пароль доступа к Kaspersky Security Center.
7. Нажмите на кнопку **Применить** в нижней части окна.

Параметры интеграции с Kaspersky Security Center будут настроены.

Настройка параметров сервера для отправки уведомлений

Программа может отправлять уведомления об обнаружениях. Для этого необходимо настроить параметры сервера для отправки уведомлений.

► *Чтобы настроить параметры сервера для отправки уведомлений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сервер для отправки уведомлений**.
2. В поле **Хост** укажите IP-адрес почтового сервера.
3. В поле **Порт** укажите порт подключения к почтовому серверу.
4. В поле **Отправлять с адреса** укажите адрес электронной почты, с которого будут отправляться уведомления.
5. Если вы хотите включить проверку подлинности на почтовом сервере, установите флажок **Использовать SMTP-проверку подлинности получателей сообщений**.
6. В поле **Имя пользователя** укажите имя пользователя для аутентификации на сервере для отправки

уведомлений.

7. В поле **Пароль** укажите пароль для аутентификации на сервере для отправки уведомлений.
8. Если вы хотите использовать TLS-шифрование при отправке уведомлений, установите флажок **Использовать TLS-шифрование**.
9. Если вы хотите проверить сертификат почтового сервера, установите флажок **Подтверждать TLS-шифрование**.

   В поле **Отпечаток сертификата** отобразится отпечаток сертификата почтового сервера.

   > Если флажок **Подтверждать TLS-шифрование** не установлен, программа будет считать любой сертификат почтового сервера доверенным.

10. Нажмите на кнопку **Применить**.

Параметры сервера для отправки уведомлений будут настроены.

Об обновлении баз

Базы программы (далее также "базы") представляют собой файлы с записями, на основании которых компоненты и модули программы обнаруживают события, происходящие в IT-инфраструктуре вашей организации.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, в том числе угроз "нулевого дня", создают для них идентифицирующие записи и включают их в пакеты обновлений баз (далее также "пакеты обновлений"). *Пакет обновлений* представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений. При установке программы дата выпуска баз соответствует дате выпуска программы, поэтому базы нужно обновить сразу после установки программы.

Программа периодически автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского" (с периодичностью один раз в 30 минут). По умолчанию, если базы компонентов программы по каким-либо причинам не обновляются в течение 24 часов, Kaspersky Anti Targeted Attack Platform отображает эту информацию в разделе **Мониторинг** окна веб-интерфейса программы.

Выбор источника обновления баз

Вы можете выбрать источник, из которого программа будет загружать обновления баз. Источником обновлений может быть сервер "Лаборатории Касперского", а также сетевая или локальная папка одного из компьютеров вашей организации.

► *Чтобы выбрать источник обновления баз программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Обновление баз** в раскрывающемся списке **Источник обновлений** выберите одно из следующих значений:
   - **Серверы "Лаборатории Касперского"**.
   - **Пользовательский URL-адрес**.

3. Если вы выбрали **Пользовательский URL-адрес**, в поле под раскрывающемся списком укажите сетевой путь к папке, в которой будут храниться обновления баз программы.
4. Нажмите на кнопку **Применить**.

Источник обновления баз программы будет выбран.

Запуск обновления баз вручную

► *Чтобы запустить обновление баз программы вручную, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Обновление баз** нажмите на кнопку **Обновить**.

Обновление баз программы будет запущено. Справа от кнопки отобразится сообщение о результате выполнения обновления.

Создание списка паролей для архивов

Программа не проверяет архивы, защищенные паролем. Вы можете создать список наиболее часто встречающихся паролей для архивов, которые используются при обмене файлами в вашей организации. В этом случае при проверке архива программа будет проверять пароли из списка. Если какой-либо из паролей подойдет, архив будет разблокирован и проверен.

Список паролей, заданный в параметрах программы, также передается на сервер с компонентом Sandbox.

► *Чтобы создать список паролей для архивов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пароли к архивам**.
2. В поле **Пароли к архивам** введите пароли, которые программа будет использовать для архивов, защищенных паролем.

   Вводите каждый пароль с новой строки. Вы можете ввести до 50 паролей.
3. Нажмите на кнопку **Применить**.

Список паролей для архивов будет создан. При проверке файлов формата PDF, а также файлов программ Microsoft Word, Excel, PowerPoint, защищенных паролем, программа будет подбирать пароли из заданного списка.

Сотруднику службы безопасности: работа в веб-интерфейсе программы

Этот раздел адресован специалистам, в обязанности которых входит обеспечение безопасности данных организации. Он содержит информацию и инструкции по настройке средств для защиты IT-инфраструктуры организации и своевременного обнаружения угроз.

Программа допускает совместную работу нескольких специалистов по информационной безопасности.

Интерфейс Kaspersky Anti Targeted Attack Platform

Работа с программой осуществляется через веб-интерфейс. Разделы веб-интерфейса программы различаются в зависимости от роли пользователя – **Администратор** или **Старший сотрудник службы безопасности** / **Сотрудник службы безопасности** (стр. 231).

Окно веб-интерфейса программы содержит следующие элементы:

- разделы в левой части и в нижней части окна веб-интерфейса программы;
- закладки в верхней части окна веб-интерфейса программы для некоторых разделов программы;
- рабочую область в нижней части окна веб-интерфейса программы.

Разделы окна веб-интерфейса программы

Веб-интерфейс программы для пользователей с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** разделен на следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.
- **Обнаружения**. Содержит информацию об обнаружениях в сети вашей организации.
- **Поиск угроз**. Содержит информацию о событиях, найденных на хостах вашей организации.
- **Задачи**. Содержит информацию о задачах, с помощью которых вы можете работать с файлами и программами на хостах.
- **Политики**. Содержит информацию о политиках, с помощью которых вы можете управлять запретами запуска файлов на выбранных хостах.
- **IOC/IOA-анализ**. Содержит информацию об IOA-анализе событий и обнаружений, IOC-проверке событий, работе с IOC-файлами и белым списком IOA.
- **Хранилище**. Содержит информацию о работе с объектами в Хранилище и Карантине.
- **Endpoint Sensors**. Содержит информацию об управлении компонентом Endpoint Sensors и просмотре данных.
- **Отчеты**. Содержит конструктор отчетов и список созданных отчетов об обнаружениях.
- **Параметры**. Содержит информацию о расписании IOC-проверки, параметрах публикации объектов в KPSN, присвоении обнаружениям статуса VIP на основе информации, содержащейся в обнаружениях, YARA-правилах, белом списке, паролях к архивам и добавленных ключах.

Рабочая область окна веб-интерфейса программы

В рабочей области отображается информация, просмотр которой вы выбираете в разделах и на закладках окна веб-интерфейса программы, а также элементы управления, с помощью которых вы можете настроить отображение информации.

Выбор организации для работы в веб-интерфейсе программы

Если вы используете режим multitenancy, перед началом работы с веб-интерфейсом вам нужно выбрать организацию, в рамках которой вы хотите работать с веб-интерфейсом программы.

► *Чтобы выбрать организацию для работы в веб-интерфейсе программы, выполните следующие действия:*

1. В верхней части меню веб-интерфейса программы нажмите на стрелку рядом с названием организации.
2. В раскрывшемся меню **Выберите организацию** выберите организацию из списка.

   Вы также можете ввести несколько символов названия организации в строку поиска и выбрать организацию из списка результатов поиска.

Все действия в веб-интерфейсе программы будут связаны с выбранной организацией. Если вы хотите изменить организацию, вам нужно повторить действия по выбору организации.

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью графиков в разделе **Мониторинг** окна веб-интерфейса программы. Вы можете добавлять, удалять, перемещать графики, настраивать масштаб графиков и выбирать период отображения данных.

О графиках и схемах расположения графиков

С помощью графиков вы можете осуществлять мониторинг работы программы.

Схема расположения графиков – вид рабочей области окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать графики на схеме расположения графиков, а также настраивать масштаб графиков.

Если вы используете режим распределенного решения и multitenancy, в разделе отображаются данные по выбранной вами организации (стр. 232).

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

В разделе **Мониторинг** отображаются следующие графики:

- Обнаружения:
  - **Обнаружения по вектору атаки**. Отображение обнаруженных объектов по направлению атаки.
  - **Обнаружения по степени важности**. Отображение важности обнаружений для пользователя

Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние они могут оказать на безопасность компьютеров или локальной сети организации, по опыту «Лаборатории Касперского».

- **Обнаружения по состоянию**. Отображение состояния обнаружения в зависимости от того, какой пользователь Kaspersky Anti Targeted Attack Platform его обрабатывает и от того, обработано это обнаружение или нет.
- **Обнаружения по технологии**. Отображение названий модулей или компонентов программы, сделавших обнаружение.
- **VIP-обнаружения по степени важности**. Отображение важности обнаружений со статусом VIP в соответствии с тем, какое влияние они могут оказать на безопасность компьютера или локальной сети организации, по опыту "Лаборатории Касперского".

В левой части каждого графика перечислены векторы атаки, степени важности обнаружений, состояния обнаружений и технологии, выполнившие обнаружения. В правой части каждого графика отображается количество раз, которое программа обнаружила их за выбранный период отображения данных на графиках (стр. 181).

По ссылке с названием вектора атаки, степенью важности обнаружений, состоянием обнаружений и технологией, выполнившей обнаружения, можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть связанные обнаружения. При этом обнаружения будут отфильтрованы по выбранному элементу.

- Топ 10:
  - **Топ 10 доменов**. 10 доменов, наиболее часто встречающихся в обнаружениях.
  - **Топ 10 адресов получателей**. 10 получателей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.
  - **Топ 10 IP-адресов**. 10 IP-адресов, наиболее часто встречающихся в обнаружениях.
  - **Топ 10 адресов отправителей**. 10 отправителей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.
  - **Топ 10 IOA-хостов**. 10 хостов, наиболее часто встречающихся в событиях по результатам IOA-анализа.
  - **Топ 10 IOA-правил**. 10 IOA-правил, по которым было найдено наибольшее количество событий.

  В левой части каждого графика перечислены домены, адреса получателей, IP-адреса и адреса отправителей сообщений, имена хостов и названия IOA-правил. В правой части каждого графика отображается количество раз, которое программа обнаружила их за выбранный период отображения данных на графиках (. 181).

  По ссылке с именем каждого домена, адреса получателя, IP-адреса и адреса отправителя сообщений , именем хоста и названию IOA-правила можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть связанные обнаружения. При этом обнаружения будут отфильтрованы по выбранному элементу.

Добавление графика на текущую схему расположения графиков

► *Чтобы добавить график на текущую схему расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на кнопку **Графики**.
5. В появившемся окне **Настроить графики** включите переключатель рядом с графиком, который вы хотите добавить.

График будет добавлен на текущую схему расположения графиков.

Перемещение графика на текущей схеме расположения графиков

► *Чтобы переместить график на текущей схеме расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Выберите график, который вы хотите переместить на схеме расположения графиков.
5. Нажав и удерживая левую клавишу мыши на верхней части графика, перетащите график на другое место схемы расположения графиков.
6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения графиков будет сохранена.

Удаление графика с текущей схемы расположения графиков

► *Чтобы удалить график с текущей схемы расположения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок  в правом верхнем углу графика, который вы хотите удалить со схемы расположения графиков.

   График будет удален из рабочей области окна веб-интерфейса программы.
5. Нажмите на кнопку **Сохранить**.

График будет удален с текущей схемы расположения графиков.

Сохранение схемы расположения графиков в PDF

► *Чтобы сохранить схему расположения графиков в PDF, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Сохранить как PDF**.

   Откроется окно **Сохранение в PDF**.
4. В нижней части окна в раскрывающемся списке **Ориентация** выберите ориентацию страницы.
5. Нажмите на кнопку **Скачать**.

   Схема расположения графиков в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.
6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на графиках

Вы можете настроить отображение данных на графиках за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

► *Чтобы настроить отображение данных на графиках за сутки (с 00:00 до 23:59), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **День**.
3. В календаре справа от названия периода **День** выберите дату, за которую вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за неделю (с понедельника по воскресенье), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Неделя**.
3. В календаре справа от названия периода **Неделя** выберите неделю, за которую вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

► *Чтобы настроить отображение данных на графиках за месяц (календарный месяц),*

выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу окна веб-интерфейса программы в раскрывающемся списке периодов отображения данных выберите **Месяц**.
3. В календаре справа от названия периода **Месяц** выберите месяц, за который вы хотите получить данные на графике.

На всех графиках страницы **Мониторинг** отобразятся данные за выбранный вами период.

Настройка размера отображения графиков

Вы можете настроить размер отображения графиков типа "Обнаружения". В правом верхнем углу графиков, размер отображения которых можно настроить, есть значок  .

► *Чтобы настроить размер отображения графиков, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывающемся списке выберите **Изменить**.
4. Нажмите на значок  в правом верхнем углу графика.
5. В раскрывшемся списке выберите один из следующих размеров отображения графика:
   - **1x1 размер**.
   - **2x1 размер**.
   - **3x1 размер**.

   Размер отображения выбранного графика изменится.
6. Повторите действия для всех графиков, размер отображения которых вы хотите изменить.
7. Нажмите на кнопку **Сохранить**.

Размер отображения графиков будет настроен.

Основные принципы работы с графиками типа "Обнаружения"

Для всех графиков типа "Обнаружения" можно настроить размер отображения (стр. 236).

В левой части каждого графика отображается легенда графика по цветам, которые используются на графиках.

Пример:

На графике **Обнаружения по степени важности** отображается количество обнаружений различной степени важности.

Важность – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

На графике **Обнаружения по степени важности** важность обнаружений отмечена следующими цветами:

- красным – обнаружения высокой степени важности;
- оранжевым – обнаружения средней степени важности;
- зеленым – обнаружения низкой степени важности.

Справа от легенды отображается количество обнаружений каждого типа за выбранный период отображения данных на графиках (стр. 181).

По ссылке с типом каждого обнаружения можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть все обнаружения этого типа. При этом обнаружения будут отфильтрованы по данному типу.

Пример:

На графике **Обнаружения по вектору атаки** отображаются обнаружения **Файлы из почты** – количество файлов, которые Kaspersky Anti Targeted Attack Platform обнаружила в почтовом трафике за выбранный период отображения данных на графиках (стр. 181).

По ссылке **Файлы из почты** откроется раздел **Обнаружения** и отобразятся все обнаружения, связанные с обнаружением файлов в почтовом трафике за выбранный период отображения данных на графиках. Данные будут отфильтрованы по следующим параметрам: **Время**, **Тип объекта**=FILE и **Источник объекта**=MAIL.

В правой части каждого графика отображаются столбцы данных. На вертикальной оси отображается количество событий, на горизонтальной оси отображаются дата и время обнаружения. Вы можете изменить период отображения данных на графиках (стр. 181) и выбрать организацию (стр. 232), информация о которых должна быть представлена на графике.

При наведении курсора мыши на каждый столбец данных отображается количество обнаружений, подсчитанных за период, представленный этим столбцом. По умолчанию отображается количество необработанных обнаружений. Вы можете включить отображение обработанных обнаружений, установив флажок **Обработано** в правом верхнем углу окна. В этом случае будет отображаться количество всех обнаружений.

Таблица обнаружений

Kaspersky Anti Targeted Attack Platform обрабатывает данные из следующих источников:

- Зеркалированного трафика локальной сети организации (HTTP-, FTP- и DNS-протоколов).
- HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- Копий сообщений электронной почты, полученных по протоколу POP3, SMTP, а также копий сообщений электронной почты, полученных от программ Kaspersky Secure Mail Gateway или Kaspersky Security для Linux Mail Server, если они используется в вашей организации.
- Данных о запущенных процессах, открытых сетевых соединениях и изменяемых файлах, полученных от отдельных компьютеров, которые входят в IT-инфраструктуру организации и работают под управлением операционной системы Microsoft Windows.

Kaspersky Anti Targeted Attack Platform отображает обнаруженные признаки целевых атак и вторжений в IT-инфраструктуру организации в виде таблицы обнаружений.

В таблице обнаружений не отображается информация об объектах, для которых выполняется хотя бы одно из следующих условий:

- Объект имеет репутацию *Доверенный* в базе KSN.
- Объект имеет цифровую подпись одного из доверенных производителей:
  - "Лаборатория Касперского".
  - Apple.
  - Google.

Информация об этих обнаружениях сохраняется в базе данных программы (на Central Node или SCN).

Информация об обнаружениях в базе данных ротируется ежедневно в ночное время при достижении максимально разрешенного количества обнаружений:

- Обнаружения, выполненные компонентами **(IDS) Intrusion Detection System**, **(URL) URL Reputation** – 100000 обнаружений для каждого из компонентов.
- Все остальные обнаружения – 20000 обнаружений для каждого из модулей или компонентов.

Если вы используете режим распределенного решения и multitenancy, то ротация производится на всех SCN, а затем происходит синхронизация с PCN. После синхронизации все удаленные обнаружения автоматически удаляются также на PCN.

Таблица обнаружений находится в разделе **Обнаружения**.

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

В таблице обнаружений содержится следующая информация:

1. **VIP** – наличие у обнаружения статуса с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователями программы **Сотрудник службы**

безопасности.

2. **Создано** – время, в которое программа выполнила обнаружение и **Обновлено** – время, в которое обнаружение было обновлено.
3.  – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

   Обнаружения могут принимать одну из следующих степеней важности:

   - **Высокая**, отмеченную знаком  , – обнаружение высокой степени важности.
   - **Средняя**, отмеченную знаком  , – обнаружение средней степени важности.
   - **Низкая**, отмеченную знаком , – обнаружение низкой степени важности.
4. **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если программа обнаружила файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
5. **Сведения** – краткая информация об обнаружении. Например, имя обнаруженного файла или URL-адрес вредоносной ссылки.
6. **Адрес источника** – адрес источника обнаруженного объекта. Например, адрес электронной почты, с которого был отправлен вредоносный файл, или URL-адрес, с которого был загружен вредоносный файл.
7. **Адрес назначения** – адрес назначения обнаруженного объекта. Например, адрес электронной почты почтового домена вашей организации, на который был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.
8. **Серверы** – имена серверов, на которых выполнено обнаружение. Серверы относятся к той организации, с которой вы работаете в веб-интерфейсе программы (стр. 232). Информация о серверах отображается только когда вы работаете в режиме распределенного решения и multitenancy.
9. **Технологии** – названия модулей или компонентов программы, выполнивших обнаружение.

   В графе **Технологии** могут быть указаны следующие модули и компоненты программы:

   - **(YARA) YARA**.
   - **(SB) Sandbox**.
   - **(URL) URL Reputation**.
   - **(IDS) Intrusion Detection System**.
   - **(AM) Anti-Malware Engine**.
   - **(TAA) Targeted Attack Analyzer**.
   - **(IOA) IOA-анализ**.
   - **(IOC) IOC-проверка**.
10. **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.

    Обнаружения могут быть в одном из следующих состояний:

- **Новое** – новые обнаружения.
- **В обработке** – обнаружения, которые один из пользователей Kaspersky Anti Targeted Attack Platform уже обрабатывает.
- **Повторная проверка** – обнаружения, выполненные в результате повторной проверки объекта.

Кроме того, в этой графе отображается имя пользователя, которому назначено данное обнаружение. Например, Administrator.

Если информация в графах таблицы отображается в виде ссылки, по ссылке раскрывается список, в котором вы можете выбрать действие над объектом. В зависимости от типа значения ячейки вы можете выполнить одно из следующих действий:

- Любой тип значения ячейки:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- MD5-хеш:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Найти события**.
  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- SHA256-хеш:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Найти события**.
  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

Модуль **Intrusion Detection System** консолидирует информацию об обработанных сетевых событиях в одном обнаружении при одновременном соблюдении следующих условий:

- для сетевых событий совпадает название сработавшего правила, версия баз программы и источник;
- между событиями прошло не более 24 часов.

Для всех сетевых событий, удовлетворяющих этим условиям, отображается одно обнаружение. В уведомлении об обнаружении содержится информация только о первом сетевом событии.

Фильтрация и поиск обнаружений

Вы можете отфильтровать обнаружения для отображения в таблице обнаружений по одной или нескольким графам таблицы или выполнить поиск обнаружений по некоторым графам таблицы по указанным вами показателям.

Вы можете создавать, сохранять и удалять фильтры, а также запускать фильтрацию и поиск обнаружений по условиям, заданным в сохраненных фильтрах.

Если вы используете режим распределенного решения и multitenancy, вы не сможете сохранять фильтры на PCN.

Фильтры сохраняются для каждого из пользователей на том сервере, на котором они созданы.

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

Фильтрация обнаружений по наличию статуса VIP

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю ☆ – наличие у обнаружения статуса с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.

► *Чтобы отфильтровать обнаружения по наличию статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Нажатием на заголовок столбца **VIP** раскройте список параметров фильтрации.
3. Настройте фильтрацию обнаружений:
   - Если вы хотите, чтобы в таблице обнаружений отобразились только обнаружения со статусом VIP, выберите **VIP**.
   - Если вы хотите, чтобы в таблице обнаружений отобразились все обнаружения, выберите **Все**.

   Если ни одно из значений не выбрано, в таблице отображаются все обнаружения.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по времени

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Создано** – время, в которое произошло обнаружение, а также **Обновлено** – время, в которое

обнаружение было обновлено.

► *Чтобы отфильтровать или найти обнаружения по времени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке **Создано** раскройте список периодов отображения обнаружений.
3. В списке **Время** выберите один из следующих периодов отображения обнаружений:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все обнаружения.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице обнаружения, произошедшие за последний час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице обнаружения, произошедшие за последний день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице обнаружения, произошедшие за указанный вами период.
4. Если вы выбрали период отображения событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения обнаружений.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
5. Если вы хотите отфильтровать обнаружения по времени изменения обнаружений, нажмите на **Переключиться на время обновления** в верхней части списка и выполните действия по выбору периода отображения обнаружений.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация обнаружений по степени важности

Вы можете отфильтровать события, обнаруженные программой, а также осуществить поиск событий в таблице событий по показателю **Важность** – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".

► *Чтобы отфильтровать обнаружения по степени важности, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По значку раскройте список параметров фильтрации.
3. Выберите одну или несколько из следующих степеней важности обнаружений:
   - **Высокая** – обнаружение высокой степени важности.
   - **Средняя** – обнаружение средней степени важности.

- **Низкая** – обнаружение низкой степени важности.

  Если ни одно из значений не выбрано, в таблице отображаются обнаружения всех степеней важности.

4. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по категориям обнаруженных объектов

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Обнаружено** – одна или несколько категорий объекта, обнаруженного в событии. Например, если вы хотите, чтобы программа отображала в таблице обнаружения файлов, зараженных определенным вирусом, вы можете задать фильтр по названию этого вируса.

► *Чтобы отфильтровать или найти обнаружения по категориям обнаруженных объектов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке **Обнаружено** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода введите название категории (например, Trojan) или несколько символов из названия категории.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по полученной информации

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Сведения** – краткая информация об обнаружении. Например, имя обнаруженного файла или URL-адрес вредоносной ссылки.

► *Чтобы отфильтровать или найти обнаружения по полученной информации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке **Сведения** откройте окно настройки фильтрации.
3. В левом раскрывающемся списке выберите один из следующих критериев поиска:
   - **Сведения**. Поиск будет осуществляться по всем сведениям об обнаруженном объекте.
   - **ID**.
   - **Имя файла**.
   - **Тип файла**.
   - **MD5**.
   - **SHA256**.
   - **URL**.
   - **Домен**.
   - **User Agent**.
   - **Тема**.
   - **HTTP-статус**.
   - **Источник объекта**.
   - **Тип объекта**.
4. В правом раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
5. В поле ввода укажите один или несколько символов информации об обнаружении.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по адресу источника

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Адрес источника** – адрес источника обнаружения. Например, адрес электронной почты, с которого был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

► *Чтобы отфильтровать или найти обнаружения по адресу источника, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

Откроется таблица обнаружений.

2. По ссылке **Адрес источника** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
4. В поле ввода укажите один или несколько символов адреса источника обнаружения.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по адресу назначения

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Адрес назначения** – адрес назначения обнаруженного объекта. Например, адрес электронной почты почтового домена вашей организации, на который был отправлен вредоносный файл, или IP-адрес компьютера локальной сети вашей организации, на который был загружен вредоносный файл.

► *Чтобы отфильтровать или найти обнаружения по адресу назначения, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Адрес назначения** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**.
   - **Не содержит**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
4. В поле ввода укажите один или несколько символов адреса назначения обнаруженного объекта.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по имени сервера

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Серверы** – имена серверов, на которых выполнено обнаружение.

Если вы используете режим распределенного решения и multitenancy, серверы относятся к той организации, с которой вы работаете в веб-интерфейсе программы (стр. 232). Фильтрация доступна только на PCN.

► *Чтобы отфильтровать или найти обнаружения по имени сервера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Серверы** раскройте список серверов, на которых выполнены обнаружения.
3. Установите флажки рядом с одним или несколькими именами серверов.
4. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по названиям модулей и компонентов программы

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Технологии** – названия модулей или компонентов программы, выполнивших обнаружение.

► *Чтобы отфильтровать обнаружения по названиям модулей и компонентов программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:
   - **Содержит**, если вы хотите, чтобы программа отображала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Не содержит**, если вы хотите, чтобы программа скрывала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Равняется**, если вы хотите, чтобы программа отображала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Не равняется**, если вы хотите, чтобы программа скрывала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
4. В раскрывающемся списке справа от выбранного вами оператора фильтрации обнаружений выберите название модуля или компонента программы, по которому вы хотите отфильтровать

обнаружения:

- **(YARA) YARA**.
- **(SB) Sandbox**.
- **(URL) URL Reputation**.
- **(IDS) Intrusion Detection System**.
- **(AM) Anti-Malware Engine**.
- **(TAA) Targeted Attack Analyzer**.
- **(IOA) IOA-анализ**.
- **(IOC) IOC-проверка**.

Например, если вы хотите, чтобы программа отобразила в списке обнаружения, выполненные компонентом Sandbox, выберите оператор фильтрации **Содержит** и название компонента **(SB) Sandbox**.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по состоянию их обработки пользователем

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.

► *Чтобы отфильтровать или найти обнаружения по состоянию их обработки пользователем Kaspersky Anti Targeted Attack Platform, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Если вы хотите включить в фильтр обработанные обнаружения, включите переключатель **Обработано** в правом верхнем углу окна.
3. По ссылке **Состояние** раскройте список вариантов обнаружений в зависимости от состояния их обработки пользователем Kaspersky Anti Targeted Attack Platform.
4. Выберите одно из следующих значений:
   - **Новое**, если вы хотите, чтобы программа отображала новые обнаружения, которые ни один из пользователей еще не начал обрабатывать.
   - **В обработке**, если вы хотите, чтобы программа отображала обнаружения, которые один из пользователей Kaspersky Anti Targeted Attack Platform уже обрабатывает.
   - **Повторная проверка**, если вы хотите, чтобы программа отображала обнаружения, произошедшие в результате повторной проверки.

5. В поле **Имя пользователя** введите имя пользователя, если вы хотите найти обнаружения, назначенные определенному пользователю **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности**.
6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Быстрое создание фильтра обнаружений

► *Чтобы быстро создать фильтр обнаружений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:
   a. Наведите курсор мыши на ссылку с тем значением графы таблицы, которое вы хотите добавить в качестве условия фильтрации.
   b. Нажмите на левую клавишу мыши.

      Откроется список действий над значением.
   c. В открывшемся списке выберите одно из следующих действий:
      - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
      - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.
3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Сброс фильтра обнаружений

► *Чтобы сбросить фильтр обнаружений по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. Нажмите на кнопку справа от того заголовка графы таблицы обнаружений, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Просмотр обнаружений

В веб-интерфейсе программы отображаются следующие типы обнаружений, на которые пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание:

- На компьютер локальной сети организации был загружен файл или была предпринята попытка загрузки файла. Программа обнаружила этот файл в зеркалированном трафике локальной сети организации или в ICAP-данных HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- На адрес электронной почты пользователя локальной сети организации был отправлен файл. Программа обнаружила этот файл в в копиях сообщений электронной почты, полученных по протоколу POP3 или SMTP, или полученных с виртуальной машины или сервера с программой Kaspersky Secure Mail Gateway, если она используется в вашей организации.
- На компьютере локальной сети организации была открыта ссылка на веб-сайт. Программа обнаружила эту ссылку на веб-сайт в зеркалированном трафике локальной сети организации или в ICAP-данных HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.
- IP-адрес или доменное имя компьютера локальной сети организации были замечены в сетевой активности. Программа обнаружила эту сетевую активность в зеркалированном трафике локальной сети организации.
- На компьютере локальной сети организации были запущены процессы. Программа обнаружила эти процессы модулем Endpoint Sensors, установленным на отдельные компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows.

Если обнаружен файл, в зависимости от того, какие модули или компоненты программы выполнили обнаружение, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и обнаруженном файле (например, IP-адрес компьютера, на котором обнаружен файл, имя обнаруженного файла);
- результаты антивирусной проверки файла, выполненной ядром AM Engine;
- результаты проверки файла на наличие признаков вторжения в IT-инфраструктуру организации, выполненной модулем YARA;
- результаты исследования поведения файла при попадании в операционные системы Windows XP SP3, 64-разрядную Windows 7 и 64-разрядную Windows 10, выполненного компонентом Sandbox;
- результаты анализа исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения.

Если обнаружена ссылка на веб-сайт, в зависимости от того, какие модули или компоненты программы выполнили обнаружение, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и обнаруженной ссылке на веб-сайт (например, IP-адрес компьютера, на котором обнаружена ссылка на веб-сайт, адрес ссылки на веб-сайт);
- результаты проверки ссылки на наличие признаков вредоносного, фишингового URL-адреса или URL-адреса, который ранее использовался злоумышленниками для целевых атак на IT-инфраструктуру организаций, выполненной модулем URL Reputation.

Если обнаружена сетевая активность IP-адреса или доменного имени компьютера локальной сети организации, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и обнаруженной сетевой активности;
- результаты исследования сетевой активности компьютера, выполненного модулем Targeted Attack Analyzer;
- результаты проверки интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации по предустановленным правилам, выполненной модулем Intrusion Detection System (IDS).

Если обнаружены процессы, запущенные на компьютере локальной сети организации, на котором установлен компонент Endpoint Sensors, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и процессах, запущенных на этом компьютере;
- результаты исследования сетевой активности компьютера, выполненного модулем Targeted Attack Analyzer.

Просмотр информации об обнаружении

► *Чтобы просмотреть информацию об обнаружении, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об обнаружении.

Общая информация об обнаружении

В заголовке окна с информацией об обнаружении отображается идентификатор обнаружения. Рядом с состоянием отображается значок ☆ или ★ в зависимости от наличия у обнаружения статуса VIP.

В правом верхнем углу окна отображается состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.

В верхней части окна с информацией об обнаружении может отображаться следующая общая информация об обнаружении:

- **Важность** – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или локальной сети вашей организации, по опыту "Лаборатории Касперского".
- **Сервер** – имя сервера, на котором выполнено обнаружение. Серверы относятся к той организации, с которой вы работаете в веб-интерфейсе программы (стр. 232).
- **Хост** – доменное имя компьютера, на котором произошло обнаружение
- **Источник данных** – источник данных. Например, SMTP Sensor или SPAN Sensor.
- **Время создания** – время, когда было выполнено обнаружение.
- **Время обновления** – время, когда была обновлена информация об обнаружении.

Информация в блоке Информация об объекте

В блоке **Информация об объекте** может отображаться следующая информация об обнаруженном файле:

- **Объект** – имя файла.

  По ссылке **Скачать** рядом с именем файла вы можете загрузить файл на жесткий диск вашего компьютера.

  Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.
- **Тип объекта** – тип файла. Например, ExecutableWin32.
- **Размер файла** – размер файла.
- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Найти события**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **SHA256** – SHA256-хеш файла.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Найти на virustotal.com**.
  - **Найти события**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **Сообщение от** – адрес электронной почты, с которого было отправлено сообщение, содержащее файл.
- **Получатели сообщения** – один или несколько адресов электронной почты, на которые было отправлено сообщение, содержащее файл.
- **Тема сообщения** – тема сообщения.
- **Заголовки сообщения** – расширенный набор заголовков сообщения электронной почты. Например, может содержать информацию об адресах электронной почты отправителя и получателей сообщения, о почтовых серверах, передавших сообщение, о типе контента сообщения электронной почты.
- **Файл подписан** – подпись файла, если он подписан.

Информация в блоке Информация об обнаружении

В блоке **Информация об обнаружении** может отображаться следующая информация об обнаружении:

- ,  или  – важность обнаружения для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние это обнаружение может оказать на безопасность компьютера или

локальной сети вашей организации, по опыту "Лаборатории Касперского".

- **Время** – время, в которое программа выполнила обнаружение.
- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если программа обнаружила файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
- **Метод** – метод HTTP-запроса. Например, Get или Post.
- **URL** – обнаруженный URL-адрес. Может также содержать код ответа.

  По ссылке с **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Найти события**.
  - **Скопировать значение в буфер**.
- **Referrer** – URL-адрес, с которого произошло перенаправление на ссылку на веб-сайт, требующую внимания. В HTTP-протоколе это один из заголовков запроса клиента, содержащий URL-адрес источника запроса.
- **IP назначения** – IP-адрес ресурса, к которому обращался пользователь или программа.

  По ссылке с **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Найти события**.
  - **Скопировать значение в буфер**.
- **Имя пользователя** – имя учетной записи пользователя, действия которого привели к возникновению события.
- **Запрос/Ответ** – длина запроса и ответа.

Информация в блоке Результаты проверки

В блоке **Результаты проверки** могут отображаться следующие результаты проверки обнаружения:

- Названия модулей или компонентов программы, выполнивших обнаружение.
- Одна или несколько категорий обнаруженного объекта. Например, может отображаться название вируса Virus.Win32.Chiton.i.
- Версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, выполнивших обнаружение.
- Результаты проверки обнаружений модулями и компонентами программы:
  - **Anti-Malware Engine** – категория обнаруженного объекта по антивирусной базе. Например, может отображаться название вируса Virus.Win32.Chiton.i.
  - **Sandbox** – результаты исследования поведения файла, выполненного компонентом Sandbox.

    Вы можете посмотреть подробный журнал исследования поведения файла во всех операционных системах по ссылке **Скачать сведения об отладке**.

    Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя проверенного файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.

По умолчанию максимальный объем жесткого диска для хранения журналов исследования поведения файлов во всех операционных системах составляет 300 ГБ. По достижении этого ограничения программа удаляет журналы исследования поведения файлов, созданные раньше остальных, и заменяет их новыми журналами.

  - **YARA** – категория обнаруженного файла в YARA-правилах (например, может отображаться название категории susp_fake_Microsoft_signer).
  - **Intrusion Detection System** – категория обнаруженного объекта по базе Intrusion Detection System. Например, может отображаться категория Bot.AridViper.UDP.C&C.
  - **Targeted Attack Analyzer** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer.
- Название IOC-файла, по которому было найдено обнаружение.

  При выборе IOC-файла открывается окно с информацией об обнаружении. В блоке **IOC** приведен XML-код IOC-файла. Критерий, по которому было выполнено обнаружение, выделен желтым цветом.
- Название IOA-правила, по которому было найдено обнаружение.

  По ссылке открывается информация об IOA-правиле. Если IOA-правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о технике MITRE, соответствующей обнаружению, а также рекомендации по реагированию на событие.
- Размер файла.
- MD5-хеш файла.
- Дата и время обработки обнаружения.

Информация в блоке Сетевое событие

По ссылке **Скачать артефакт IDS** вы можете скачать файл с данными об обнаружении.

В блоке **Сетевое событие** может отображаться следующая информация о ссылке на веб-сайт, открытой на компьютере:

- **Метод** – тип HTTP-запроса, например, GET или POST.
- **IP источника** – IP-адрес компьютера, на котором была открыта ссылка на веб-сайт.
- **Адрес назначения** – IP-адрес компьютера, с которого была открыта ссылка на веб-сайт.
- **User Agent** – информация о браузере, с помощью которого был загружен файл или была предпринята попытка загрузки файла, или была открыта ссылка на веб-сайт. Текстовая строка в составе HTTP-запроса, обычно содержащая название и версию браузера, а также название и версию операционной системы, установленной на компьютере пользователя.

Информация в блоке Результаты проверки в Sandbox

В блоке **Результаты проверки в Sandbox** могут отображаться следующие сведения об обнаружении:

- **Файл** – полное имя и путь проверенного файла.
- **Размер файла** – размер файла.
- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на Kaspersky Threat Intelligence Portal**.
- **Найти события**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

- **Подписано** – автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу.
- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если программа обнаружила файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
- **Время обработки** – время выполнения проверки файла.
- **Версии баз** – версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, выполнивших обнаружение.

Информация о результатах исследования поведения файла приводится для каждой операционной системы, в которой компонент Sandbox выполнил проверку. Для операционной системы Windows 79 (64-разрядная) вы можете просмотреть журналы активности файла для двух режимов проверки компонента Sandbox – **Режим быстрой проверки** и **Режим ведения полного журнала**.

Для каждого режима проверки могут быть доступны следующие журналы активности:

- **Список активностей** – действия файла внутри операционной системы.
- **Дерево активностей** – графическое представление процесса исследования файла.
- **Журнал HTTP-активности** – журнал HTTP-активности файла. Содержит следующую информацию:
  - **IP назначения** – IP-адрес, на который файл пытается перейти из операционной системы.
  - **Метод** – метод HTTP-запроса, например, GET или POST.
  - **URL** – URL-адрес ссылки на веб-сайт, которую файл пытается открыть из операционной системы.

  По ссылкам **IP назначения** и **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти на Kaspersky Threat Intelligence Portal**.
    - **Найти события**.
    - **Скопировать значение в буфер**.
- **Журнал действий IDS** – журнал действий IDS. Содержит следующую информацию:
  - **IP источника** – IP-адрес хоста, на котором хранится файл.
  - **IP назначения** – IP-адрес, на который файл пытается перейти из операционной системы.
  - **Метод** – метод HTTP-запроса, например, GET или POST.
  - **URL** – URL-адрес ссылки на веб-сайт, которую файл пытается открыть из операционной системы.
- **Журнал DNS-активности** – журнал DNS-активности файла. Содержит следующую информацию:
  - **Запрос** – имя и тип DNS-запроса.
  - **Ответ** – имя, тип ответа от DNS-сервера, а также имя хоста или IP-адрес компьютера, с которого был получен ответ.
- **Скачать полный журнал** – журнал исследования поведения файла в каждой операционной системе.

Информация в блоке Удаленные хосты

В блоке **Удаленные хосты** отображается список хостов, с которыми связана обнаруженная сетевая активность. По ссылке с именем хоста вы можете раскрыть блок информации о сетевой активности, связанной с этим хостом.

Отобразится следующая информация:

- **Имя хоста** – IP-адрес или доменное имя компьютера, с которым связывался компьютер локальной сети организации.
- **Регистратор** – название организации – регистратора доменов, которая зарегистрировала этот домен.
- **Информация о домене** – подробная информация о домене.
- **Популярность в мире** – популярность домена в мире.
- **Обнаружено в локальной сети** – дата и время обнаружения хоста Kaspersky Anti Targeted Attack Platform.
- **Активность домена** – информация об активности домена доступна, если обнаружение было выполнено с использованием данных от компонента Endpoint Sensors. Отображается следующая информация:
  - **Время** – время совершения активности.
  - **Сведения** – описание выполненных операций.
  - **Имя пользователя** – учетная запись пользователя, от имени которого совершена активность.

Информация в блоке Хосты

В блоке **Хосты** отображается следующая информация о хостах, на которых сработало IOA-правило:

- **Имя хоста** – IP-адрес или доменное имя компьютера, на котором произошло событие. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного IOA-правила и выбранный хост.
- **Количество событий** – количество событий, произошедших на хосте.
- **Найти события**. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного IOA-правила.

Информация о сетевой активности компьютера в блоке Процессы

В блоке **Процессы** отображается список процессов, с которыми связана обнаруженная сетевая активность. По ссылке с путем к процессу вы можете раскрыть блок информации об этом процессе.

Отобразится следующая информация:

- **Путь к файлу** – путь к файлу процесса.
- **Название программы** – название программы, запустившей процесс.
- **Описание файла** – дополнительная информация об обнаруженном файле.
- **Размер файла** – размер обнаруженного файла.
- **Версия файла** – версия обнаруженного файла.

- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Поставщик** – компания, выпустившая программу, к которой относится процесс.
- **Версия программы** – версия программы.
- **Подписано** – автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу.
- **Подпись действительна** – информация о том, является ли цифровая подпись действительной.
- **Обнаружено в локальной сети** – дата и время обнаружения процесса в локальной сети.
- **Обнаружено на компьютерах** – количество компьютеров, на которых этот процесс был обнаружен в локальной сети.
- **Компьютеров с подобной активностью** – количество компьютеров, на которых был обнаружен подобный процесс.
- **Популярность файла в мире** – популярность файла, запустившего процесс, в мире.
- **Популярность пути в мире** – популярность пути, по которому был загружен процесс, в мире.

По ссылке **Активность процесса** вы можете раскрыть блок с информацией о сетевой активности процесса:

- **Время** – время сетевого события.
- **Сведения** – путь к процессу.
- **Имя пользователя** – имя учетной записи пользователя, запустившего процесс.

Информация в блоке Данные учетной записи пользователя

В блоке **Данные учетной записи пользователя** отображается информация об учетной записи пользователя компьютера, на котором была обнаружена сетевая активность.

Отображается следующая информация:

- **Тип учетной записи** – тип учетной записи. Например, Administrator.
- **Тип входа** – тип входа в компьютер.
- **Обнаружен в сети** – дата и время, когда сетевая активность была впервые обнаружена в локальной сети.
- **Обнаружен на компьютере** – дата и время, когда активность была впервые обнаружена на компьютере.
- **Используется на компьютерах** – количество компьютеров, на которых была обнаружена аналогичная сетевая активность.

Информация в блоке Модули, загруженные процессом

В блоке **Модули, загруженные процессом** отображается информация о модулях, загруженных процессом, с которым связана обнаруженная сетевая активность. Например, процессом может быть загружена библиотека dll. По ссылке с путем к модулю вы можете раскрыть блок информации об этом процессе.

Отобразится следующая информация:

- **Путь к файлу** – путь к файлу, загруженному процессом.

- **Название программы** – имя файла, загруженного процессом.
- **Описание файла** – дополнительная информация об обнаруженном файле.
- **Размер файла** – размер обнаруженного файла.
- **Версия файла** – версия обнаруженного файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Поставщик** – компания, выпустившая программу, к которой относится процесс.
- **Версия программы** – версия программы.
- **Подписано** – автор сертификата, в котором содержится цифровая подпись к обнаруженному файлу.
- **Подпись действительна** – информация о том, является ли сертификат действительным.
- **Обнаружено в локальной сети** – дата и время обнаружения процесса в локальной сети.
- **Обнаружено на компьютерах** – количество раз, которое этот процесс был обнаружен в локальной сети.
- **Компьютеров с подобной активностью** – количество компьютеров, на которых был обнаружен подобный процесс.
- **Популярность файла в мире** – популярность файла, запустившего процесс, в мире.
- **Популярность пути в мире** – популярность пути, по которому был загружен процесс, в мире.

По ссылке **Просмотреть журнал** вы можете раскрыть блок с информацией о операциях с загруженным модулем:

- **Время** – время загрузки модуля.
- **Сведения** – путь к загруженному файлу.
- **Имя пользователя** – имя учетной записи пользователя, загрузившего модуль.

Информация в блоке Журнал изменений

В блоке **Журнал изменений** может отображаться следующая информация об обнаружении:

- Дата и время изменения обнаружения.
- Автор изменений.

  Например, **Система** или имя пользователя программы.
- Изменение, произошедшее с обнаружением.

  Например, обнаружению может быть присвоена принадлежность группе VIP, или оно может быть отмечено как обработанное.

Отправка данных об обнаружении

Вы можете предоставить в "Лабораторию Касперского" данные об обнаружении (кроме технологий URL Reputation, IOA-анализ и IOC-проверка) для дальнейшего исследования.

Для этого необходимо скопировать данные об обнаружении в буфер обмена, а затем отправить их в

"Лабораторию Касперского" по электронной почте.

Данные об обнаружении могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Вам необходимо самостоятельно согласовать отправку этих данных для дальнейшего исследования в "Лабораторию Касперского" со Службой безопасности вашей организации.

► *Чтобы скопировать данные об обнаружении в буфер обмена, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об обнаружении.

3. Нажмите на ссылку **Предоставить данные об обнаружении в "Лабораторию Касперского"** в нижней части окна с информацией об обнаружении.

   Откроется окно **Подробнее**.

4. Просмотрите данные об обнаружении для отправки в "Лабораторию Касперского".

5. Если вы хотите скопировать эти данные, нажмите на кнопку **Скопировать в буфер**.

   Данные об обнаружении будут скопированы в буфер обмена. Вы сможете отправить их в "Лабораторию Касперского" для дальнейшего исследования.

Действия пользователей над обнаружениями

При работе в веб-интерфейсе программы под учетной записью с ролью **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** вы можете выполнять следующие действия над обнаружениями:

- Назначить обнаружение себе или другому пользователю веб-интерфейса программы.

  Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем (стр. 247).

- Отметить обнаружение как обработанное.

  Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем (стр. 247).

- Добавить комментарий к обнаружению.

  Вы можете найти обнаружения, содержащие комментарий, по ключевым словам комментария, используя фильтр обнаружений по полученной информации (стр. 243).

- Присвоить обнаружению статус VIP.

  Это действие доступно только пользователям с ролью **Старший сотрудник службы безопасности**. Пользователи с этой ролью могут просмотреть все обнаружения со статусом VIP, используя фильтр обнаружений по наличию статуса VIP (стр. 241).

Назначение нескольких обнаружений определенному пользователю

► *Чтобы назначить обнаружение себе или другому пользователю веб-интерфейса программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, которые вы хотите назначить пользователю.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. В появившейся панели в нижней части окна нажатием на стрелку справа от кнопки **Отметить как обработанное** раскройте список пользователей.

4. Выберите пользователя, которому вы хотите назначить обнаружения.

   Откроется окно подтверждения действия.

5. Нажмите на кнопку **Продолжить**

Обнаружения будут назначены выбранному пользователю.

Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем (стр. 247).

Назначение обнаружений себе или другому пользователю

► *Чтобы назначить одно или несколько обнаружений себе или другому пользователю,*

выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, которые вы хотите назначить себе или другому пользователю.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. В появившейся панели в нижней части окна нажмите на кнопку **Отметить как обработанное**.
4. Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

5. Нажмите на кнопку **Продолжить**.

Обнаружение будет назначено выбранному пользователю.

Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем.

Отметка о завершении обработки одного обнаружения

► *Чтобы отметить в таблице обнаружений одно обнаружение, назначенное вам, как обработанное, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. В графе **Состояние** того обнаружения, которое вы хотите отметить как обработанное, левой кнопкой мыши нажмите на ваше имя пользователя.
3. В списке действий выберите **Отметить как обработанное**.

Обнаружение будет отмечено как обработанное.

► *Чтобы отметить обнаружение как обработанное в процессе работы с этим обнаружением, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Откройте обнаружение, которое вы хотите отметить как обработанное.
3. В правом верхнем углу окна нажатием на стрелку справа от кнопки со статусом обнаружения раскройте список действий.
4. В списке действий выберите **Отметить как обработанное**.

Обнаружение будет отмечено как обработанное. Если обнаружение было назначено другому пользователю, оно будет отмечено как обработанное вами.

Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем.

Отметка о завершении обработки обнаружений

► *Чтобы отметить одно или несколько обнаружений как обработанные, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, которые вы хотите отметить как обработанные.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. В появившейся панели в нижней части окна нажмите на кнопку **Отметить как обработанное**.

   Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

4. Нажмите на кнопку **Продолжить**.

Выбранные обнаружения будут отмечены как обработанные. Если обнаружения были назначены другим пользователям, они будут отмечены как обработанные вами.

Вы можете просмотреть все обработанные обнаружения, используя фильтр обнаружений по состоянию их обработки пользователем (стр. 247).

Изменение статуса VIP обнаружений

Пользователи с ролью **Старший сотрудник службы безопасности** могут присваивать обнаружениям статус VIP и лишать обнаружения статуса VIP.

► *Чтобы изменить статус VIP обнаружений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив тех обнаружений, статус VIP которых вы хотите изменить.

   Вы можете установить флажок в заголовке таблицы, чтобы выбрать все обнаружения.

3. Выполните одно из следующих действий:

   - Если вы хотите присвоить обнаружениям статус VIP, в появившейся панели в нижней части окна нажмите на кнопку **Присвоить статус VIP**.
   - Если вы хотите лишить обнаружения статуса VIP, в появившейся панели в нижней части окна в раскрывающемся списке **Присвоить статус VIP** выберите пункт **Лишить статуса VIP**.

   Откроется окно подтверждения действия.

   Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

4. Нажмите на кнопку **Продолжить**

Статус VIP обнаружений будет изменен.

Пользователи с ролью **Старший сотрудник службы безопасности** могут просмотреть все обнаружения со статусом VIP, используя фильтр обнаружений по наличию статуса VIP (стр. 241).

Добавление комментария к обнаружению

► *Чтобы добавить комментарий к обнаружению, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Выберите обнаружение, к которому вы хотите добавить комментарий.

   Откроется окно с информацией об обнаружении.

3. В поле добавления комментария под названием блока **Журнал изменений** введите комментарий к обнаружению.

4. Нажмите на кнопку **Добавить**.

   Комментарий к обнаружению будет добавлен и отобразится в блоке **Журнал изменений** этого обнаружения.

Вы можете найти обнаружения, содержащие комментарий, по ключевым словам комментария, используя фильтр обнаружений по полученной информации (стр. 243).

Поиск угроз по базе событий

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** могут формировать поисковые запросы и использовать IOC-файлы и IOA-правила для поиска угроз по базе событий в рамках тех организаций, к данным которых у них есть доступ (стр. 158).

Для формирования поисковых запросов по базе событий вы можете использовать *режим конструктора* или *режим исходного кода*.

В режиме конструктора вы можете создавать и изменять поисковые запросы с помощью раскрывающихся списков с вариантами типа значения поля и операторов.

В режиме исходного кода (стр. 265) вы можете создавать и изменять поисковые запросы с помощью текстовых команд.

Вы можете загрузить IOC-файл (стр. 267) и искать события по условиям, заданным в этом IOC-файле.

Вы также можете создавать IOA-правила (стр. 268) на основе условий поиска событий.

Поиск событий с помощью режима конструктора

► *Чтобы задать условия поиска событий в режиме конструктора, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Конструктор** или **Редактор кода**.

   Откроется форма поиска событий.
2. В раскрывающемся списке выберите критерий для поиска событий в одной из следующих групп:
   - **Поиск по всему тексту**.
   - **Общие сведения**.
   - **Свойства IOA**.
   - **Свойства файла**.
   - **Запущен процесс**.
   - **Удаленное соединение**.
   - **Изменение в реестре**.
   - **Событие в журнале Windows**.
   - **Изменено имя хоста**.
   - **Обнаружение и результат обработки**.
3. В раскрывающемся списке выберите один из следующих операторов сравнения:
   - **=**.
   - **!=**.
   - **CONTAINS**.

- **!CONTAINS**.
- **STARTS**.
- **!STARTS**.
- **ENDS**.
- **!ENDS**.
- **>**.
- **<**.

Для каждого типа значения поля будет доступен свой релевантный набор операторов сравнения. Например, при выборе типа значения поля **EventType** будут доступны операторы **=** и **!=**.

4. В зависимости от выбранного типа значения поля выполните одно из следующих действий:
   - Укажите в поле один или несколько символов, по которым вы хотите выполнить поиск событий.
   - В раскрывающемся списке выберите вариант значения поля, по которому вы хотите выполнить поиск событий.

   Например, для поиска полного совпадения по имени пользователя введите имя пользователя.
5. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.
6. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.
7. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.
8. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **За все время** выберите один из следующих периодов поиска событий:
   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.
9. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.
10. Нажмите на кнопку **Найти**.

    Отобразятся уровни группировки найденных событий: **Все серверы** – Названия организаций – Имена серверов.
11. Нажмите на имя того сервера, события по которому вы хотите просмотреть.

    Откроется таблица хостов выбранного сервера. Уровни группировки событий отобразятся над

таблицей. Таблица хостов содержит следующую информацию:

- **Хост** – имя хоста, на котором обнаружены события.
- **Количество событий** – количество событий, обнаруженных на этом хосте.
- **Первое событие** – дата и время, в которое на этом хосте обнаружено первое событие.
- **Все серверы** – дата и время, в которое на этом хосте обнаружено последнее событие.

12. Выберите хост, события по которому вы хотите просмотреть.

    Откроется таблица событий, соответствующих заданным вами условиям поиска. Уровни группировки событий отобразятся над таблицей.

    Вы можете вернуться к окну выбора хоста по ссылке с названием организации и именем сервера или вернуться к выбору организации и сервера по ссылке **Все серверы**.

Поиск событий с помощью режима исходного кода

► *Чтобы задать условия поиска событий в режиме исходного кода, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Редактор кода**.

   Откроется форма с полем ввода условий поиска событий в режиме исходного кода.

2. Введите условия поиска событий, используя команды, логические операторы `OR` и `AND`, а также скобки для создания групп условий.

   Команды должны соответствовать следующему синтаксису: `<тип поля> <оператор сравнения> <значение поля>`.

Пример:

```
EventType = "filechange"
AND (
    FileName CONTAINS "example"
    OR UserName = "example"
)
```

3. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:

   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события,

найденные за указанный вами период.

4. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

5. Нажмите на кнопку **Найти**.

   Отобразятся уровни группировки найденных событий: **Все серверы** – Названия организаций – Имена серверов.

6. Нажмите на имя того сервера, события по которому вы хотите просмотреть.

   Откроется таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей. Таблица хостов содержит следующую информацию:

   - **Хост** – имя хоста, на котором обнаружены события.
   - **Количество событий** – количество событий, обнаруженных на этом хосте.
   - **Первое событие** – дата и время, в которое на этом хосте обнаружено первое событие.
   - **Все серверы** – дата и время, в которое на этом хосте обнаружено последнее событие.

7. Выберите хост, события по которому вы хотите просмотреть.

   Откроется таблица событий, соответствующих заданным вами условиям поиска. Уровни группировки событий отобразятся над таблицей.

   Вы можете вернуться к окну выбора хоста по ссылке с названием организации и именем сервера или вернуться к выбору организации и сервера по ссылке **Все серверы**.

Изменение условий поиска событий

► *Чтобы изменить условия поиска событий, выполните следующие действия в разделе **Поиск угроз** окна веб-интерфейса программы:*

1. Нажмите на форму с условиями поиска событий в верхней части окна.
2. Выберите одну из следующих закладок:
   - **Конструктор**, если вы хотите изменить условия поиска событий в режиме конструктора.
   - **Редактор кода**, если вы хотите изменить условия поиска событий в режиме исходного кода.
3. Внесите необходимые изменения.
4. Нажмите на одну из следующих кнопок:
   - **Обновить**, если вы хотите обновить текущий поиск событий новыми условиями.
   - **Новый поиск**, если вы хотите выполнить новый поиск событий.

   Отобразятся уровни группировки найденных событий: **Все серверы** – Названия организаций – Имена серверов.

5. Нажмите на имя того сервера, события по которому вы хотите просмотреть.

   Откроется таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей. Таблица хостов содержит следующую информацию:

   - **Хост** – имя хоста, на котором обнаружены события.
   - **Количество событий** – количество событий, обнаруженных на этом хосте.
   - **Первое событие** – дата и время, в которое на этом хосте обнаружено первое событие.
   - **Все серверы** – дата и время, в которое на этом хосте обнаружено последнее событие.

6. Выберите хост, события по которому вы хотите просмотреть.

   Откроется таблица событий, соответствующих заданным вами условиям поиска. Уровни группировки событий отобразятся над таблицей.

   Вы можете вернуться к окну выбора хоста по ссылке с названием организации и именем сервера или вернуться к выбору организации и сервера по ссылке **Все серверы**.

Загрузка IOC-файла и поиск событий по условиям, заданным в IOC-файле

► *Чтобы загрузить IOC-файл и искать события по условиям, заданным в этом IOC-файле, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

3. Выберите IOC-файл, который хотите загрузить, и нажмите на кнопку **Открыть**.

   IOC-файл загрузится.

   На закладке **Редактор кода** в форме с условиями поиска событий отобразятся условия, заданные в загруженном IOC-файле.

   Вы можете искать события по этим условиям. Вы также можете изменить условия, заданные в загруженном IOC-файле, или добавить условия поиска событий в режиме исходного кода (стр. 265).

4. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:

   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.

- **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.

5. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

6. Нажмите на кнопку **Найти**.

   Отобразятся уровни группировки найденных событий: **Все серверы** – Названия организаций – Имена серверов.

7. Нажмите на имя того сервера, события по которому вы хотите просмотреть.

   Откроется таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей. Таблица хостов содержит следующую информацию:

   - **Хост** – имя хоста, на котором обнаружены события.
   - **Количество событий** – количество событий, обнаруженных на этом хосте.
   - **Первое событие** – дата и время, в которое на этом хосте обнаружено первое событие.
   - **Все серверы** – дата и время, в которое на этом хосте обнаружено последнее событие.

8. Выберите хост, события по которому вы хотите просмотреть.

   Откроется таблица событий, соответствующих заданным вами условиям поиска. Уровни группировки событий отобразятся над таблицей.

   Вы можете вернуться к окну выбора хоста по ссылке с названием организации и именем сервера или вернуться к выбору организации и сервера по ссылке **Все серверы**.

Создание IOA-правила на основе условий поиска событий

► *Чтобы создать IOA-правило на основе условий поиска событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Выполните поиск событий с помощью режима конструктора или режима исходного кода.
3. Нажмите на кнопку **Сохранить как IOA-правило**.

   Откроется окно **Сохранить**.

4. В поле **Имя нового IOA-правила** введите имя IOA-правила.
5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В разделе **IOC/IOA-анализ**, подразделе **IOA-анализ** отобразится новое IOA-правило с заданным именем.

Информация о событиях

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут просматривать информацию о событиях в рамках тех организаций, к данным которых у них есть доступ (стр. 158).

Если вы используете режим распределенного решения и multitenancy, в разделе отображаются данные по выбранной вами организации (стр. 232).

► *Чтобы включить отображение событий по всем организациям,*

включите переключатель **Искать по всем организациям**.

Просмотр таблицы событий

Таблица событий отображается в разделе **Поиск угроз** окна веб-интерфейса программы после выполнения поиска угроз по базе событий (стр. 263).

События сгруппированы по хостам выбранных серверов и организаций. В таблице событий содержится следующая информация:

1. **Время события** – дата и время обнаружения события.
2. **Событие** – тип события.
3. **Сведения** – сведения о событии.
4. **Имя пользователя** – имя пользователя.

Каждому типу событий соответствует свой тип значения ячейки в графе таблицы событий **Сведения** (см. таблицу ниже).

*Таблица 13. Соответствие типов значений ячеек в графах **Событие** и **Сведения***

Событие	Сведения
Запущен процесс	Имя файла процесса, который был запущен. SHA256- и MD5-хеш.
Загружен модуль	Имя динамической библиотеки, которая была загружена. SHA256- и MD5-хеш.
Удаленное соединение	URL-адрес, к которому была произведена попытка удаленного подключения. Имя файла, который пытался осуществить удаленное подключение.
Правило запрета	Имя файла приложения, запуск которого был заблокирован. SHA256- и MD5-хеш.
Документ заблокирован	Имя документа, запуск которого был заблокирован. SHA256- и MD5-хеш.
Создан файл	Имя созданного файла. SHA256- и MD5-хеш.

Событие	Сведения
Событие в журнале Windows	Канал записи событий в журнал Windows. Идентификатор типа события.
Изменение в реестре	Имя ключа в реестре. `<имя переменной в ключе>=<значение переменной>`.
Прослушан порт	Адрес сервера и порт. Имя файла процесса, который осуществляет прослушивание порта.
Загружен драйвер	Имя файла драйвера, который был загружен. SHA256- и MD5-хеш.
Изменено имя хоста	Старое имя хоста. Новое имя хоста.

По ссылке с названием типа события, сведениями, дополнительной информацией и именем пользователя раскрывается список, в котором вы можете выбрать действие над объектом. В зависимости от типа значения ячейки вы можете выполнить одно из следующих действий:

- Любой тип значения ячейки:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- Имя файла:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Отправить файл в Карантин**.
- MD5-хеш:
  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Создать правило запрета**.
  - **Найти в Хранилище**.
- SHA256-хеш:
  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Найти на virustotal.com**.
  - **Создать правило запрета**.
  - **Найти в Хранилище**.

Просмотр информации о событии

► *Чтобы просмотреть информацию о событии, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Конструктор** или

Редактор кода.

Откроется форма поиска событий.

2. Если вы используете режим распределенного решения и multitenancy и хотите включить отображение событий по всем организациям, включите переключатель **Искать по всем организациям**.
3. Выполните поиск событий с помощью режима конструктора (стр. 263) или режима исходного кода (стр. 265).

   Отобразятся уровни группировки найденных событий: **Все серверы** – Названия организаций – Имена серверов.
4. Нажмите на имя того сервера, события по которому вы хотите просмотреть.

   Откроется таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей. Таблица хостов содержит следующую информацию:

   - **Хост** – имя хоста, на котором обнаружены события.
   - **Количество событий** – количество событий, обнаруженных на этом хосте.
   - **Первое событие** – дата и время, в которое на этом хосте обнаружено первое событие.
   - **Все серверы** – дата и время, в которое на этом хосте обнаружено последнее событие.
5. Выберите хост, события по которому вы хотите просмотреть.

   Откроется таблица событий, соответствующих заданным вами условиям поиска. Уровни группировки событий отобразятся над таблицей.

   > Вы можете вернуться к окну выбора хоста по ссылке с названием организации и именем сервера или вернуться к выбору организации и сервера по ссылке **Все серверы**.

6. Выберите событие, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о событии.

Информация о запуске процесса

В окне с информацией о событиях типа **Запущен процесс** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- **Запущен процесс**:
  - **Время события** – время запуска процесса.
  - **Файл** – имя файла процесса.
  - **Параметры запуска** – параметры запуска процесса.
  - **MD5** – MD5-хеш файла процесса.
  - **SHA256** – SHA256-хеш файла процесса.
  - **Размер** – размер файла процесса.

- **ID процесса** – идентификатор процесса.
- **Время завершения** – время завершения процесса.
- **Время создания** – время создания файла процесса.
- **Время изменения** – время последнего изменения файла процесса.
- **Имя хоста** – имя хоста, на котором был запущен процесс.
- **Имя пользователя** – имя пользователя, запустившего процесс.

- **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.

Информация о загрузке модуля

В окне с информацией о событиях типа **Загружен модуль** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- **Загружен модуль**:
  - **Время события** – время загрузки модуля.
  - **Файл** – имя файла загруженного модуля.
  - **MD5** – MD5-хеш файла загруженного модуля.
  - **SHA256** – SHA256-хеш файла загруженного модуля.
  - **Имя хоста** – имя хоста, на котором был загружен модуль.
  - **Имя пользователя** – имя пользователя, загрузившего модуль.
  - **Размер** – размер загруженного модуля.
  - **Время создания** – время создания загруженного модуля.
  - **Время изменения** – дата последнего изменения загруженного модуля.
- **Родительский процесс**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

Информация об удаленном соединении

В окне с информацией о событиях типа **Удаленное соединение** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- **Удаленное соединение**:
  - **Время события** – время попытки удаленного соединения.
  - **Удаленный IP-адрес** – IP-адрес хоста, на который была произведена попытка удаленного соединения.
  - **Локальный IP-адрес** – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
  - **Имя хоста** – имя хоста, с которого была произведена попытка удаленного соединения.
  - **Имя пользователя** – имя пользователя, который пытался установить удаленное соединение.
- **Родительский процесс**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

Информация о срабатывании правила запрета

В окне с информацией о событиях типа **Правило запрета** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- **Правило запрета**:
  - **Время события** – время срабатывания запрета запуска файла.
  - **Файл** – имя файла, запуск которого был запрещен..
  - **Параметры запуска** – параметры, с которыми была произведена попытка запуска файла.
  - **MD5** – MD5-хеш файла, запуск которого был запрещен.
  - **SHA256** – SHA256-хеш файла, запуск которого был запрещен.
  - **Размер** – размер файла, запуск которого был запрещен.
  - **Время создания** – время создания файла, запуск которого был запрещен.
  - **Время изменения** – дата последнего изменения файла, запуск которого был запрещен.
  - **Имя хоста** – имя хоста, на котором сработал запрет запуска файла.

- **Имя пользователя** – имя пользователя, попытавшегося запустить файл.

- **Родительский процесс**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.

Информация о блокировании документа

В окне с информацией о событиях типа **Документ заблокирован** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- **Документ заблокирован**:
  - **Время события** – время блокирования документа.
  - **Файл** – имя заблокированного документа.
  - **MD5** – MD5-хеш заблокированного документа.
  - **Файл процесса** – имя файла процесса, который попытался открыть документ.
  - **MD5 процесса** – MD5-хеш процесса, который попытался открыть документ.
  - **SHA256 процесса** – SHA256-хеш процесса, который попытался открыть документ.
  - **ID процесса** – идентификатор процесса, который попытался открыть документ.
  - **Имя хоста** – имя хоста, на котором был заблокирован документ.
  - **Имя пользователя** – имя пользователя, попытавшегося открыть документ.

- **Родительский процесс**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.

Информация о создании файла

В окне с информацией о событиях типа **Создан файл** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- **Создан файл**:
  - **Время события** – время обнаружения события.
  - **Файл** – имя созданного файла.
  - **MD5** – MD5-хеш созданного файла.
  - **SHA256** – SHA256-хеш созданного файла.
  - **Размер** – размер созданного файла.
  - **Время создания** – время создания файла.
  - **Время изменения** – время последнего изменения файла.
  - **Имя хоста** – имя хоста, на котором был создан файл.
  - **Имя пользователя** – имя пользователя, создавшего файл.
- **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

Информация о событии в журнале Windows

В окне с информацией о событиях типа **Событие в журнале Windows** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- **Событие в журнале Windows**:
  - **Время события** – время обнаружения события.
  - **ID события безопасности** – идентификатор типа события безопасности в журнале Windows.
  - **ID записи** – идентификатор события в журнале Windows.
  - **Провайдер** – имя провайдера.
  - **Имя журнала** – имя журнала Windows.
  - **Домен** – домен, которому принадлежит хост, на котом произошло событие.
  - **Имя хоста** – имя хоста, на котором произошло событие.
  - **Имя пользователя** – имя пользователя хоста, на котором произошло событие.

  Также блок параметров **Событие в журнале Windows** содержит данные из системного журнала Windows. Состав данных зависит от типа события Windows.

Информация об изменении в реестре

В окне с информацией о событиях типа **Изменение в реестре** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- **Изменение в реестре**:
  - **Время события** – время внесения изменения в реестр.
  - **Путь к разделу реестра** – путь к разделу реестра, в котором было произведено изменение.
  - **Имя параметра реестра** – имя параметра реестра.
  - **Параметр реестра** – значение параметра реестра.
  - **Имя хоста** – имя хоста, на котором было произведено изменение в реестре.
  - **Имя пользователя** – имя пользователя, совершившего изменение в реестре.
- **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

Информация о прослушивании порта

В окне с информацией о событиях типа **Прослушан порт** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.
- **Прослушан порт**:
  - **Время события** – время прослушивания порта.
  - **Порт** – порт, который был прослушан.
  - **Локальный IP-адрес** – IP-адрес сетевого интерфейса, порт которого был прослушан.
  - **Имя хоста** – имя хоста, порт которого был прослушан.
  - **Имя пользователя** – имя пользователя, от имени которого было совершено прослушивание порта.
- **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

Информация о загрузке драйвера

В окне с информацией о событиях типа **Загружен драйвер** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- **Загружен драйвер**:
  - **Время события** – время загрузки драйвера.
  - **Файл** – имя файла загруженного драйвера.
  - **MD5** – MD5-хеш файла загруженного драйвера.
  - **SHA256** – SHA256-хеш файла загруженного драйвера.
  - **Имя хоста** – имя хоста, на который был загружен драйвер.
  - **Размер** – размер загруженного драйвера.
  - **Время создания** – время создания загруженного драйвера.
  - **Время изменения** – время последнего изменения загруженного драйвера.

Информация об изменении имени хоста

В окне с информацией о событиях типа **Изменено имя хоста** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- **Изменено имя хоста**:
  - **Время события** – время изменения имени хоста.
  - **Имя хоста** – новое имя хоста.
  - **Имя пользователя** – имя пользователя, изменившего имя хоста.
  - **Старое имя хоста** – старое имя хоста.

Информация об обнаружении

В окне с информацией о событии типа **Обнаружение** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- На закладке **Сведения** в блоке параметров **Обнаружение**:

- **Время события** – дата и время события.
- **Обнаруженный объект** – имя обнаруженного объекта. Вы можете нажать на имя объекта и по ссылке **Найти события** найти все события, в которых был обнаружен этот объект.
- **Последнее действие** – последнее действие над обнаруженным объектом.
- **Имя хоста** – имя хоста, на котором выполнено обнаружение.
- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
- **Тип объекта** – тип объекта (например, файл).
- **Имя объекта** – полное имя файла, в котором обнаружен объект.
- **MD5** – MD5-хеш файла, в котором обнаружен объект.
- **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
- **Режим обнаружения** – режим проверки, в котором выполнено обнаружение.
- **ID записи** – идентификатор записи об обнаружении в базе.
- **Версия баз** – версия баз, с помощью которых выполнено обнаружение.

- На закладке **Сведения** в блоке параметров **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.
- На закладке **История** в таблице:
  - **Тип** – тип события: **Обнаружение** и **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время обнаружения и результата обработки обнаружения.

Информация о результатах обработки обнаружения

В окне с информацией о событии типа **Результат обработки обнаружения** содержатся следующие сведения:

- Дерево событий.

  Отображает дочерние и родительские события, а также связи между ними. Корневым узлом дерева событий является хост, события которого вы просматриваете.

  Вы можете выбирать события в дереве событий, чтобы просмотреть информацию об этих событиях.

- На закладке **Сведения** в блоке параметров **Результат обработки обнаружения**:
  - **Время события** – дата и время события.
  - **Обнаруженный объект** – имя обнаруженного объекта. Вы можете нажать на имя объекта и по ссылке **Найти события** найти все события, в которых был обнаружен этот объект.

- **Последнее действие** – последнее действие над обнаруженным объектом.
- **Имя хоста** – имя хоста, на котором выполнено обнаружение.
- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
- **Тип объекта** – тип объекта (например, файл).
- **Имя объекта** – полное имя файла, в котором обнаружен объект.
- **MD5** – MD5-хеш файла, в котором обнаружен объект.
- **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
- **Режим обнаружения** – режим проверки, в котором выполнено обнаружение.
- **ID записи** – идентификатор записи об обнаружении в базе.
- **Версия баз** – версия баз, с помощью которых выполнено обнаружение.

- На закладке **Сведения** в блоке параметров **Родительский процесс**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.
- На закладке **История** в таблице:
  - **Тип** – тип события **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время результата обработки обнаружения.

Управление компонентом Endpoint Sensors

Компонент Endpoint Sensors (стр. 39) устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**, **Локальный администратор** и **Администратор** могут оценить регулярность получения данных с хостов, на которых установлен компонент Endpoint Sensors, на закладке **Endpoint Sensors** окна веб-интерфейса программы в рамках тех организаций, к данным которых у них есть доступ (стр. 158). Если вы используете режим распределенного решения и multitenancy, то в веб-интерфейсе сервера PCN отображается список компонентов Endpoint Sensors для PCN и всех подключенных SCN.

Пользователи с ролью **Локальный администратор** и **Администратор** могут настроить отображение регулярности получения данных с хостов, на которых установлен компонент Endpoint Sensors, в рамках тех организаций, к данным которых у них есть доступ (стр. 158).

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети (стр. 294) любой из хостов с компонентом Endpoint Sensors в рамках тех организаций, к данным которых у него есть доступ (стр. 158). При этом соединение между сервером с компонентом Central Node и хостом с компонентом Endpoint Sensors не будет прервано.

Для оказания поддержки при неполадках в работе компонента Endpoint Sensors специалисты Службы технической поддержки могут попросить вас в отладочных целях выполнить следующие действия (в том числе в режиме Technical Support Mode):

- Активировать функциональность получения расширенной диагностической информации.
- Изменить параметры отдельных компонентов программы.
- Изменить параметры хранения и отправки получаемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

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

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

Просмотр таблицы Endpoint Sensors на отдельном сервере Central Node

Таблица хостов с компонентом Endpoint Sensors находится в разделе **Endpoint Sensors** окна веб-интерфейса программы.

Если вы используете отдельный сервер Central Node, не используете интеграцию с KSC, режим распределенного решения и multitenancy, в таблице хостов с компонентом Endpoint Sensors могут отображаться следующие данные:

- **Хост** – имя хоста с компонентом Endpoint Sensors.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Версия** – версия установленного компонента Endpoint Sensors.
- **Активность** – показатель активности компонента Endpoint Sensors. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Просмотр таблицы Endpoint Sensors на отдельном сервере Central Node при интеграции с KSC

Если вы настроили интеграцию с KSC, таблица хостов с компонентом Endpoint Sensors находится в разделе **Endpoint Sensors** окна веб-интерфейса программы.

В разделе **Endpoint Sensors** отображаются следующие подразделы:

- **Central Node**. Отображается информация о хостах с компонентом Endpoint Sensors, подключенных к этому серверу Central Node.
- **KSC**. Отображается информация о всех хостах, подключенных к KSC.

В подразделе **Central Node** может отображаться следующая информация:

- **Хост** – имя хоста с компонентом Endpoint Sensors.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Версия** – версия установленного компонента Endpoint Sensors.
- **Активность** – показатель активности компонента Endpoint Sensors. Может принимать следующие значения:

- **Нормальная активность** – хосты, от которых последние данные были получены недавно.
- **Предупреждение** – хосты, от которых последние данные были получены давно.
- **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

В подразделе **KSC** может отображаться следующая информация:

- **Хост** – имя хоста с компонентом Endpoint Sensors.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Endpoint Sensor** – тип компонента, используемого в качестве Endpoint Sensors.

  Компонент может быть одного из следующих типов:

  - **Endpoint Sensor**.

    Компонент Endpoint Sensors (стр. 39), который был установлен из пакета Kaspersky Anti Targeted Attack Platform.

  - **В составе KES**.

    Компонент Endpoint Sensors, входящий в состав программы Kaspersky Endpoint Security для Windows.
- **Версия** – версия установленного компонента Endpoint Sensors.
- **Сервер** – имя сервера с компонентом Central Node.
- **Состояние сенсора** – статус компонента Endpoint Sensors, установленного на компьютере.

  Компонент Endpoint Sensors может иметь один из следующих статусов:

  - **Запущен**.
  - **Остановлен**.
  - **Сбой**.
  - **Не установлен**.
- **Состояние хоста** – состояние хоста компьютера с компонентом Endpoint Sensors.

  Хост может находиться в одном из следующих состояний:

  - **Отключено**.
  - **Онлайн**.
- **С ошибкой** – статус наличия ошибок в работе компонента Endpoint Sensors. Статус может принимать значение **Нет ошибок** или содержать информацию о типе ошибки работы компонента Endpoint Sensors.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

По ссылке с IP-адресом компьютера, на который установлен компонент Endpoint Sensors, вы также можете выбрать действие **Перейти к обнаружениям, отфильтрованным по этому значению**.

По ссылке с именем хоста, на который установлен компонент Endpoint Sensors, вы также можете выбрать действия:

- **Изолировать от сети**.
- **Найти события**.
- **Найти обнаружения**.

Просмотр таблицы Endpoint Sensors в режиме распределенного решения и multitenancy

Таблица хостов с компонентом Endpoint Sensors находится в разделе **Endpoint Sensors** окна веб-интерфейса программы.

Если вы используете режим распределенного решения и multitenancy и не используете интеграцию с KSC, в таблице содержится информация о компонентах Endpoint Sensors, подключенных к PCN и всем серверам SCN. В таблице могут отображаться следующие данные:

- **Хост** – имя хоста с компонентом Endpoint Sensors.

  По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Новое правило запрета**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Серверы** – имена серверов, к которым подключен хост с компонентом Endpoint Sensors.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Версия** – версия установленного компонента Endpoint Sensors.
- **Активность** – показатель активности компонента Endpoint Sensors. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в любой графе таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

По ссылке с IP-адресом компьютера, на который установлен компонент Endpoint Sensors, вы также можете

выбрать действие **Перейти к обнаружениям, отфильтрованным по этому значению**.

Просмотр информации о хосте

► *Чтобы просмотреть информацию о хосте, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Выберите хост, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- **Обнаружения** – ссылка, по которой открывается раздел **Обнаружения** с условием поиска, содержащим информацию о выбранном вами хосте.
- **События** – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим информацию о выбранном вами хосте.
- **Состояние** – состояние хоста с компонентом Endpoint Sensors.

  Хост может находиться в одном из следующих состояний:

  - **Онлайн**.
  - **Отключено**.
- **Хост** – имя хоста с компонентом Endpoint Sensors.

  По ссылке с именем хоста вы можете выбрать одно из следующих действий:

  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Отправить файл в Карантин**.
  - **Выполнить программу**.
  - **Новое правило запрета**.
  - **Изолировать от сети**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **IP** – IP-адрес компьютера, на который установлен компонент Endpoint Sensors.
- **ОС** – версия операционной системы, установленной на компьютере с компонентом Endpoint Sensors.
- **Защита** – состояние защиты хоста с компонентом Endpoint Sensors.
- **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и multitenancy.
- **Имя сервера** – имя сервера Central Node.
- **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.

- **Версия** – тип и версия установленного компонента Endpoint Sensors.
- **Состояние** – состояние компонента Endpoint Sensors.
- **Правила запрета**. По ссылке открывается таблица правил запрета, созданных по хешам файлов на этом хосте со следующей информацией:
  - **Тип**
  - **Имя**.
  - **Состояние**.
  - **Хеш**.
- **Задачи**. По ссылке открывается таблица задач, созданных для этого хоста со следующей информацией:
  - **Время создания**.
  - **Тип**.
  - **Имя**.
  - **Сведения**.
  - **Состояние**.

Фильтрация и поиск Endpoint Sensors по имени хоста

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по имени хоста, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **Хост** откройте окно настройки фильтрации.
4. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Sensors**.
5. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
6. В поле ввода укажите один или несколько символов имени хоста.
7. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
8. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.

9. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors, изолированных от сети

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors, изолированные от сети (стр. 294), выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.

2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:

   - **Central Node**.
   - **KSC**.

3. По ссылке **Хост** откройте окно настройки фильтрации.
4. Установите флажок **Показывать только изолированные Endpoint Sensors**.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по именам серверов PCN и SCN

Если вы используете режим распределенного решения и multitenancy, вы можете отфильтровать или найти хосты с компонентом Endpoint Sensors по именам серверов PCN и SCN, к которым подключены эти хосты.

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по именам серверов PCN и SCN, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.

2. По ссылке **Серверы** откройте окно настройки фильтрации.
3. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с компонентом Endpoint Sensors.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по IP-адресу компьютера

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по IP-адресу компьютера, на котором установлен компонент Endpoint Sensors, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **IP** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по версии операционной системы на компьютере

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по версии операционной системы, установленной на компьютере с компонентом Endpoint Sensors, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **ОС** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов версии операционной системы.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по версии компонента Endpoint Sensor

► *Чтобы отфильтровать или найти хосты с компонентом Endpoint Sensors по версии компонента Endpoint Sensors, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.

- **KSC**.

3. По ссылке **Версия** откройте окно настройки фильтрации.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов версии компонента Endpoint Sensors.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку  справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по их активности

► *Чтобы отфильтровать или найти компоненты Endpoint Sensors по их активности, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. По ссылке **Активность** откройте окно настройки фильтрации.
4. Установите флажки рядом с одним или несколькими показателями активности компонента Endpoint Sensors (стр. 211):
   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск Endpoint Sensors по наличию ошибок в работе компонента

Если вы не используете режим распределенного решения и multitenancy и используете отдельный сервер Central Node, вы можете отфильтровать или найти хосты с компонентом Endpoint Sensors по наличию ошибок в работе компонента.

► *Чтобы отфильтровать или найти хосты Endpoint Sensors по наличию ошибок в работе компонента, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица компьютеров с компонентом Endpoint Sensors.
2. По ссылке **С ошибкой** откройте окно настройки фильтрации.
3. В раскрывающемся списке выберите один из следующих вариантов:
   - Если вы хотите, чтобы в таблице отображались все хосты с компонентом Endpoint Sensors, выберите **Все**.
   - Если вы хотите, чтобы в таблице отображались только те хосты, на которых компонент Endpoint Sensors работает с ошибками, выберите **С ошибками**.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра компьютеров с компонентом Endpoint Sensors

► *Чтобы быстро создать фильтр хостов с компонентом Endpoint Sensors, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый

фильтр:

a. Наведите курсор мыши на ссылку с тем значением графы таблицы, которое вы хотите добавить в качестве условия фильтрации.

b. Нажмите на левую клавишу мыши.

   Откроется список действий над значением.

c. В открывшемся списке выберите одно из следующих действий:

   - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
   - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

4. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра Endpoint Sensors

► *Чтобы сбросить фильтр хостов с компонентом Endpoint Sensors по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.
2. Если режим распределенного решения и multitenancy (стр. 42) отключен, выберите один из следующих подразделов:
   - **Central Node**.
   - **KSC**.
3. Нажмите на кнопку справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице хостов с компонентом Endpoint Sensors отобразятся только хосты, соответствующие заданным вами условиям.

Настройка показателей активности Endpoint Sensors

Пользователи с ролью **Локальный администратор** и **Администратор** могут определить, какой период бездействия компонентов Endpoint Sensors считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности компонентов Endpoint Sensors. Просматривать показатели активности Endpoint Sensors могут все пользователи.

► *Чтобы настроить показатели активности компонентов Endpoint Sensors, выполните следующие действия:*

1. Войдите в веб-интерфейс программы под учетной записью **Локальный администратор** или **Администратор**.

2. В окне веб интерфейса программы выберите раздел **Параметры**, подраздел **Endpoint Sensors**.
3. В полях под названием раздела введите количество дней бездействия компьютеров с компонентом Endpoint Sensors, которое вы хотите отображать как **Предупреждение** и **Критическая**.
4. Нажмите на кнопку **Применить**.

Пользователи с правами **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** смогут увидеть настроенные вами показатели активности компонентов Endpoint Sensors в графе **Активность** таблицы хостов с компонентом Endpoint Sensors в разделе **Endpoint Sensors** окна веб-интерфейса программы.

Поддерживаемые интерпретаторы и процессы

Компонент Endpoint Sensors контролирует запуск скриптов следующими интерпретаторами:

- cmd.exe;
- reg.exe;
- regedit.exe;
- regedt32.exe;
- cscript.exe;
- wscript.exe;
- mmc.exe;
- msiexec.exe;
- mshta.exe;
- rundll32.exe;
- runlegacycplelevated.exe;
- control.exe;
- explorer.exe;
- regsvr32.exe;
- wwahost.exe;
- powershell.exe;
- java.exe и javaw.exe (только при запуске с опцией –jar);
- InstallUtil.exe;
- msdt.exe;
- python.exe;
- ruby.exe;
- rubyw.exe.

Информация о процессах, контролируемых компонентом Endpoint Sensor, представлена в таблице ниже.

Таблица 14. Процессы и расширения файлов, которые они открывают

Процесс	Расширения файлов
winword.exe	rtf doc dot docm docx dotx dotm docb
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

Сетевая изоляция хостов с компонентом Endpoint Sensors

Сетевая изоляция доступна для хостов с компонентом Endpoint Sensors версии 3.5 и 3.6.

При включении правила сетевой изоляции на хосте прерываются все текущие соединения, а также становится недоступно VPN-подключение.

Программа блокирует соединение изолированных хостов с сервером Active Directory. Если параметры операционной системы требуют подключения к службам Active Directory для авторизации, то пользователь изолированного хоста не сможет войти в систему.

Если администратор программы заменяет сертификат сервера с компонентом Central Node (стр. 188) при включенном правиле сетевой изоляции, то отключение правила становится недоступно.

Для корректной работы изолированного хоста рекомендуется выполнять следующие условия:

- Создать на хосте учетную запись локального администратора или сохранить данные доменной учетной записи в кеш перед включением правила сетевой изоляции.
- Не заменять сертификат и IP-адрес сервера с компонентом Central Node при включенном правиле сетевой изоляции.

Изолированным хостам доступны по сети следующие ресурсы:

- Сервер с компонентом Central Node.
- Источник обновлений баз программы (сервер обновлений "Лаборатории Касперского" или пользовательский источник).
- Серверы службы KSN.
- Хосты, добавленные в исключения правила сетевой изоляции.

Если соединение между изолированным хостом и сервером с компонентом Central Node отсутствует более 5 часов, правило сетевой изоляции автоматически отключается.

Создание правила сетевой изоляции

► *Чтобы создать правило сетевой изоляции, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.

2. Выберите хост, для которого вы хотите включить или отключить правило сетевой изоляции.

Откроется окно с информацией о хосте.

3. Нажмите на кнопку **Изолировать**.
4. В блоке параметров **Исключения для правила изоляции хоста** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящий/Исходящий**.
   - **Входящий**.
   - **Исходящий**.
5. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.
6. Если вы выбрали **Входящий** или **Исходящий**, в поле **Порты** введите порты подключения.
7. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия 4–6.
8. Нажмите на кнопку **Сохранить**.

Хост будет изолирован от сети.

Вы также можете создать правило сетевой изоляции по ссылке **Имя хоста** в информации о событии (стр. 270) и в информации об обнаружении (стр. 250).

Добавление исключения из правила сетевой изоляции

► *Чтобы добавить исключение в ранее созданное правило сетевой изоляции, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Выберите хост, изолированный от сети, для которого вы хотите создать исключение из правила сетевой изоляции.

   Откроется окно с информацией о хосте.
3. По ссылке **Добавить в исключения** раскройте блок параметров **Исключения для правила изоляции хоста**.
4. Выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящий/Исходящий**.
   - **Входящий**.
   - **Исходящий**.
5. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.
6. Если вы выбрали **Входящий** или **Исходящий**, в поле **Порты** введите порты подключения.
7. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия 4–6.
8. Нажмите на кнопку **Сохранить**.

Исключение из правила сетевой изоляции будет добавлено.

Отключение правила сетевой изоляции

Чтобы отключить правило сетевой изоляции, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Sensors**.

   Откроется таблица хостов с компонентом Endpoint Sensors.
2. Выберите хост, для которого вы хотите отключить правило сетевой изоляции.

   Откроется окно с информацией о хосте.
3. Нажмите на кнопу **Отключить изоляцию**.

   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.
5. В окне с информацией о хосте нажмите на кнопу **Закрыть**.

Правило сетевой изоляции хоста будет отключено.

Работа с задачами

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** могут работать с файлами и программами на хостах путем создания и удаления задач: **Завершить процесс**, **Выполнить программу**, **Получить файл**, **Удалить файл**, **Отправить файл в Карантин**, **Восстановить файл из Карантина**.

Задачи **Завершить процесс**, **Выполнить программу**, **Удалить файл**., **Отправить файл в Карантин**, **Восстановить файл из Карантина** могут быть одного из следующих типов:

- **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (если вы используете режим распределенного решения и multitenancy).
- **Глобальный** – созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232).

Задача **Получить файл** выполняется только на указанном хосте независимо от режима работы с программой.

Пользователи с ролью **Старший сотрудник службы безопасности** могут работать со всеми задачами в рамках тех организаций, к данным которых у них есть доступ (стр. 158).

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Максимальное время выполнение задачи составляет 24 часа. Если за это время задача не успела завершиться, ее выполнение останавливается.

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Задачи** окна веб-интерфейса программы. Вы можете просматривать все задачи или только задачи, созданные вами (текущим пользователем).

► *Чтобы включить отображение задач, созданных только текущим пользователем,*

включите переключатель **Только мои** в правом верхнем углу окна.

Отображение задач, созданных текущим пользователем, по умолчанию включено.

В таблице задач содержится следующая информация:

1. **Время создания** – дата и время создания задачи.
2. **Тип** – тип задачи по области распространения задачи.

   Задачи могут быть одного из следующих типов:

   - **Глобальный** – созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232).
   - **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на

хосты, подключенные к этому серверу SCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (если вы используете режим распределенного решения и multitenancy).

3. **Имя** – название задачи.

   Задача может быть иметь одно из следующих названий:

   - **Завершить процесс**.
   - **Выполнить программу**.
   - **Получить файл**.
   - **Удалить файл**.
   - **Отправить файл в Карантин**.
   - **Восстановить файл из Карантина**.

   По ссылке с названием типа задачи раскрывается список, в котором вы можете выбрать одно из следующих действий:

   - **Добавить в фильтр**.
   - **Исключить из фильтра**.
   - **Скопировать значение в буфер**.

4. **Сведения** – полный путь к файлу или потоку данных, для которого создана задача.

   По ссылке со сведениями о пути к файлу или потоку данных раскрывается список, в котором вы можете выбрать одно из следующих действий:

   - **Добавить в фильтр**.
   - **Исключить из фильтра**.
   - **Скопировать значение в буфер**.

5. **Серверы** – имя сервера с ролью PCN или SCN, на котором выполняется задача.

   Поле отображается только если вы используете режим распределенного решения и multitenancy.

6. **Хосты** – имя хоста, на котором выполняется задача.

   Поле отображается только если вы используете отдельный сервер Central Node.

7. **Автор** – имя пользователя, создавшего задачу.

   Если вы включили отображение задач, созданных только текущим пользователем, эта графа не будет отображаться.

8. **Состояние** – статус выполнения задачи.

   Задача может иметь один из следующих статусов:

   - **Ожидает**.
   - **В обработке**.
   - **Завершено**.

Просмотр информации о задаче

► *Чтобы просмотреть информацию о задаче, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Выберите задачу, информацию о которой вы хотите просмотреть.

Откроется окно с информацией о задаче.

Окно может содержать следующую информацию в зависимости от типа задачи:

- **Состояние** – статус выполнения задачи.
- **Описание** – описание задачи.
- **Путь к файлу** – путь к файлу или потоку данных.
- **SHA256** – SHA256-хеш файла, который вы хотите получить.
- **Команда** – команда запуска программы.
- **Рабочий каталог** – рабочий каталог программы.
- **Запущено от имени** – параметр запуска программы: от имени текущего пользователя или от имени локальной системы.
- **Автор** – имя пользователя, создавшего задачу.
- **Организация** – название организации, отображается только когда вы используете режим распределенного решения и multitenancy.
- **Время создания** – время создания задачи.
- **Время завершения** – время завершения задачи.
- **Отчет** – результат выполнения задачи на выбранных хостах.

Создание задачи завершения процесса

Если вы считаете, что запущенный на компьютере процесс может угрожать безопасности компьютера или локальной сети организации, вы можете завершить его.

► *Чтобы создать задачу завершения процесса, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Завершить процесс**.

   Откроется окно создания задачи.

3. Укажите следующие параметры:

   a. **Путь к файлу** – путь к файлу процесса, который вы хотите завершить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будут завершены только процессы указанного потока данных. Процессы остальных потоков этого файла будут выполняться.

b. **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, который вы хотите завершить. Поле не является обязательным.

c. **Описание** – описание задачи. Поле не является обязательным.

d. Если вы хотите, чтобы пользователю компьютера, на котором выполняется задача, отображалось уведомление о запуске задачи, справа от названия параметра **Уведомление** установите флажок **Показать пользователю уведомление о выполнении задачи**.

e. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения (стр. 42) и multitenancy.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача завершения процесса.

Создание задачи выполнения программы

Вы можете выполнить задачу запуска программы или выполнения команды.

Если при выполнении задачи файл стандартного вывода или файл вывода ошибок достигает размера 100 КБ, часть данных из файла удаляется. Файл будет содержать не все данные.

► *Чтобы создать задачу запуска программы или выполнения команды, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Выполнить программу**.

   Откроется окно создания задачи.

3. Укажите следующие параметры:

   a. Если вы хотите запустить программу от имени SYSTEM, в блоке параметров **Параметры** установите флажок **Запустить от имени SYSTEM**.

   По умолчанию флажок снят. Программа будет запущена от имени текущего пользователя.

   b. Выберите одно из следующих действий:

   - Если вы хотите запустить программу с помощью командной строки (cmd.exe) или выполнить команду, выберите вариант **Выполнить команду** и введите команду в поле **Команда**.
   - Если вы хотите запустить программу напрямую, выберите вариант **Запустить файл**, укажите

полный путь к файлу в поле **Путь к файлу** и ключи запуска в поле **Аргументы**.

Вы также можете указать путь к альтернативному потоку данных этого файла.

c. **Описание** – описание задачи. Поле не является обязательным.

d. **Рабочий каталог** – рабочий каталог программы, которую вы хотите запустить.

e. Если вы хотите, чтобы пользователю компьютера, на котором выполняется задача, отображалось уведомление о запуске задачи, справа от названия параметра **Уведомление** установите флажок **Показать пользователю уведомление о выполнении задачи**.

f. **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и multitenancy.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача запуска программы или выполнения команды.

Пример:

► *Чтобы полностью отключить сетевые интерфейсы хоста с помощью выполнения команды от имени текущего пользователя на всех хостах, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Выполнить программу**.

   Откроется окно создания задачи.

3. Укажите следующие параметры:

   a. В блоке параметров **Параметры** выберите вариант **Выполнить команду** и в поле **Команда** введите команду `netsh interface set interface <Имя интерфейса> admin=disable`.

   b. В поле **Описание** введите описание задачи.

   c. Выберите область применения задачи **Всех хостов**.

4. Нажмите на кнопку **Добавить**.

   Выполняйте задачу для отключения каждого сетевого интерфейса.
   Сетевой интерфейс, соединяющий хост с компонентом Central Node, отключайте в последнюю очередь.

После успешного выполнения задачи сетевые интерфейсы хоста будут отключены.

Создание задачи получения файла

► *Чтобы создать задачу получения файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Получить файл**.

   Откроется окно создания задачи.

3. Укажите следующие параметры:

   a. **Путь к файлу** – путь к файлу, который вы хотите получить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае вы получите только указанный поток.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите получить. Поле не является обязательным.

      При указании этого параметра может быть получено более одного файла.

   c. Если вы хотите отказаться от проверки файла, снимите флажок **Отправить на проверку**.

      По умолчанию флажок установлен.

   d. **Описание** – описание задачи. Поле не является обязательным.

   e. **Хост** – имя хоста или IP-адрес сервера, с которого вы хотите получить файл.

4. Нажмите на кнопку **Добавить**.

Будет создана задача получения файла. Файл, полученный в результате выполнения задачи, будет помещен в Хранилище.

Если задача получения файла завершилась успешно, вы можете скачать полученный файл на ваш локальный компьютер.

► *Чтобы скачать полученный файл на локальный компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу получения файла, который вы хотите скачать.

3. В нижней части окна **Получить файл** нажмите на имя хоста или IP-адрес.

   Откроется окно с информацией о файле.

4. Нажмите на кнопку **Скачать**.

Файл будет сохранен на ваш локальный компьютер в папку загрузки браузера.

Создание задачи удаления файла

► *Чтобы создать задачу удаления файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Удалить файл**.

   Откроется окно создания задачи.

3. Укажите следующие параметры:

   a. **Путь к файлу** – путь к файлу, который вы хотите удалить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будет удален только указанный поток данных. Остальные потоки данных этого файла останутся без изменений.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите удалить. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

   d. Если вы хотите, чтобы пользователю компьютера, на котором выполняется задача, отображалось уведомление о запуске задачи, справа от названия параметра **Уведомление** установите флажок **Показать пользователю уведомление о выполнении задачи**.

   e. **Задача для** – область применения задачи:

      - Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
      - Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

        Этот вариант доступен только при включенном режиме распределенного решения и multitenancy.

      - Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создана задача удаления файла.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки хоста. Рекомендуется проверить успешность удаления файла после перезагрузки хоста.
Удаление файла с подключенного сетевого диска не поддерживается.

Создание задачи помещения файла в Карантин

Если вы считаете, что на компьютере находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив в Карантин.

► *Чтобы создать задачу помещения файла в Карантин, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Отправить файл в Карантин**.

   Откроется окно создания задачи.

3. Укажите следующие параметры:

   a. **Путь к файлу** – путь к файлу, который вы хотите поместить в Карантин.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите поместить в Карантин. Поле не является обязательным.

   c. Если вы хотите отказаться от проверки файла, снимите флажок **Отправить на проверку**.

      По умолчанию флажок установлен.

   d. **Описание** – описание задачи. Поле не является обязательным.

   e. Если вы хотите, чтобы пользователю компьютера, на котором выполняется задача, отображалось уведомление о запуске задачи, справа от названия параметра **Уведомление** установите флажок **Показать пользователю уведомление о выполнении задачи**.

   f. **Хост** – имена хостов, с которых вы хотите удалить файл, поместив его копию в Карантин.

4. Нажмите на кнопку **Добавить**.

Будет создана задача помещения файла в Карантин. В результате выполнения задачи файл будет удален с выбранных хостов и помещен в Карантин.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом Выполнено, но сам файл будет помещен в Карантин только после перезагрузки хоста. Рекомендуется проверить успешность выполнения задачи после перезагрузки хоста.

Создание задачи восстановления файла из Карантина

Если вы считаете, что изолированный ранее файл безопасен, вы можете восстановить его из Карантина на хост.

► *Чтобы создать задачу восстановления файла из Карантина, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Восстановить файл из Карантина**.

   Откроется окно создания задачи.

3. Укажите следующие параметры:

   a. **Описание** – описание задачи. Поле не является обязательным.

   b. Если вы хотите, чтобы пользователю компьютера, на котором выполняется задача, отображалось уведомление о запуске задачи, справа от названия параметра **Уведомление** установите флажок **Показать пользователю уведомление о выполнении задачи**.

c. **Поиск файлов** – имя файла, находящегося в Карантине.

4. Нажмите на кнопку **Добавить**.

Будет создана задача восстановления файла из Карантина.

После восстановления файла из Карантина на хост метаданные о файле останутся в таблице объектов, помещенных в Хранилище.

Создание копии задачи

► *Чтобы скопировать задачу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу, которую вы хотите скопировать.
3. Нажмите на кнопку **Скопировать**.

   Откроется окно создания задачи. Все параметры задачи будут скопированы.

4. Нажмите на кнопку **Добавить**.

Будет создана копия выбранной задачи.

Удаление задачи

Если вы удалите задачу в процессе ее выполнения, результат выполнения задачи может не сохраниться.
Если вы удалите успешно выполненную задачу скачивания файла, файл будет удален.

► *Чтобы удалить задачу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Откройте задачу, которую вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Задача будет удалена.

Фильтрация задач по времени создания

► *Чтобы отфильтровать задачи по времени их создания, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Время создания** откройте меню фильтрации задач.
3. Выберите один из следующих периодов отображения задач:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все созданные задачи.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за

предыдущий час.

- **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за предыдущий день.
- **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице задачи, созданные за указанный вами период.

4. Если вы выбрали период отображения задач **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения задач.
   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по типу

Если вы используете режим распределенного решения и multitenancy, вы можете отфильтровать задачи по их типу.

► *Чтобы отфильтровать задачи по их типу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Тип** откройте меню фильтрации задач.
3. Выберите один из следующих вариантов отображения задач:
   - **Все**, если вы хотите, чтобы отображались все задачи независимо от типа.
   - **Глобальный**, если вы хотите, чтобы отображались только задачи, созданные на сервере PCN. Действие этих задач распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232).
   - **Локальный**, если вы хотите, чтобы отображались только задачи, созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (если вы используете режим распределенного решения и multitenancy).

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени

► *Чтобы отфильтровать задачи по имени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Имя** откройте меню фильтрации задач.
3. Установите один или несколько флажков:
   - **Получить файл**.
   - **Завершить процесс**.
   - **Удалить файл**.
   - **Отправить файл в Карантин**.
   - **Восстановить файл**.
   - **Выполнить программу**.
4. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени и пути к файлу

Вы можете фильтровать задачи по показателю **Сведения** – имя и путь к файлу или потоку данных.

► *Чтобы отфильтровать задачи по имени и пути к файлу или потоку данных, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. По ссылке **Сведения** откройте окно настройки фильтрации задач.
3. В правом раскрывающемся списке выберите **Сведения**.
4. В левом раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
5. В поле ввода укажите один или несколько символов имени или пути к файлу.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по описанию

Вы можете фильтровать задачи по показателю **Описание** – описание задачи, которое было добавлено на этапе создания задачи.

► *Чтобы отфильтровать задачи по описанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Сведения** откройте окно настройки фильтрации задач.
3. В левом раскрывающемся списке выберите **Описание**.
4. В правом раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
5. В поле ввода укажите один или несколько символов имени или пути к файлу.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени сервера

Если вы используете режиме распределенного решения и multitenancy, вы можете отфильтровать задачи по серверам, на которые распространяется действие задач.

► *Чтобы отфильтровать задачи по серверам, на которые распространяется действие задач, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Серверы** откройте меню фильтрации задач.
3. Установите флажки рядом с именами тех серверов, задачи по которым вы хотите отобразить.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по имени пользователя, создавшего задачу

Фильтрация задач по имени пользователя, создавшего задачу, доступна только при отображении всех задач. Если вы включили отображение задач, созданных только текущим пользователем, фильтрация задач по имени пользователя недоступна.

► *Чтобы отфильтровать задачи по имени пользователя, создавшего задачу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Автор** откройте меню фильтрации задач.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации задач:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация задач по состоянию обработки

► *Чтобы отфильтровать задачи по состоянию их обработки пользователем, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Состояние** откройте меню фильтрации задач.
3. Установите один или несколько флажков:
   - **Ожидает**.
   - **В обработке**.
   - **Завершено**.
4. Нажмите на кнопку **Применить**.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра задач

► *Чтобы сбросить фильтр задач по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку  справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

   > Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице задач отобразятся только задачи, соответствующие заданным вами условиям.

Работа с политиками (правилами запрета)

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** могут управлять правилами запрета запуска файлов и процессов на выбранных хостах с помощью политик. Например, вы можете запретить запуск программ, использование которых считаете небезопасным, на выбранном хосте с компонентом Endpoint Sensors. Программа идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Вы можете создавать, удалять и изменять запреты.

Правила запрета могут быть следующих типов:

- **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (если вы используете режим распределенного решения и multitenancy).
- **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232).

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, редактировать, удалять, включать и отключать правила запрета в рамках тех организаций, к данным которых у них есть доступ (стр. 158).

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета.

Все изменения в правилах запрета применяются на хостах после установки авторизованного соединения с выбранными хостами. Если соединение с хостами отсутствует, на хостах продолжают действовать старые правила запрета. Изменения в правилах запрета не влияют на уже запущенные процессы.

Если попытка запуска файла будет совершена до запуска компонента Endpoint Sensors или после завершения работы компонента Endpoint Sensors на хосте, то запуск файла будет заблокирован. На компьютере пользователя отобразится уведомление о запрете запуска файла, когда компонент Endpoint Sensors будет запущен.

На каждый хеш файла можно создать только одно правило запрета.

Просмотр таблицы правил запрета

Таблица правил запрета находится в разделе **Политики** окна веб-интерфейса программы.

В таблице содержится следующая информация:

1. **Тип** – тип правила запрета. Правила запрета могут быть следующих типов:
   - **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232).
   - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется

только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (если вы используете режим распределенного решения и multitenancy).

2. **Имя** – имя правила запрета.
3. **Серверы** – имена серверов с ролью PCN или SCN, на которые распространяется правило запрета (если вы используете режим распределенного решения и multitenancy).

   Поле отображается только когда вы используете режим распределенного решения и multitenancy.
4. **Хосты** – имя сервера с компонентом Central Node, на хосты которого распространяется правило запрета.

   Поле отображается только когда вы используете отдельный сервер Central Node.
5. **Хеш файла** – алгоритм хеширования, применяющийся для идентификации файла.

   Идентификация файла может осуществляться по одному из следующих алгоритмов хеширования:

   - **MD5**.
   - **SHA256**.

   По ссылке с названием алгоритма хеширования раскрывается список, в котором вы можете посмотреть хеш файла, а также выбрать одно из следующих действий:

   - **Добавить в фильтр**.
   - **Исключить из фильтра**.
   - **Найти на Kaspersky Threat Intelligence Portal**.
   - **Найти на virustotal.com**.
   - **Найти события**.

     В результате выполнения этого действия откроется раздел **Поиск угроз** с событиями, уже отфильтрованными по выбранному вами хешу.
   - **Включить правило запрета**.
   - **Отключить правило запрета**.
   - **Удалить правило запрета**.
   - **Скопировать значение в буфер**.
6. **Состояние** – текущее состояние правила запрета.

   Правило запрета может находиться в одном из следующих состояний:

   - **Включено**.
   - **Отключено**.

Просмотр правила запрета

► *Чтобы просмотреть правило запрета, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Выберите правило запрета, которое вы хотите просмотреть.

Правило запрета содержит следующую информацию:

- **События** – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранное вами правило запрета.
- **Состояние** – текущее состояние правила запрета.

  Правило запрета может находиться в одном из следующих состояний:

  - **Включено**.
  - **Отключено**.
- Закладка **Сведения** со следующей информацией:
  - **MD5/SHA256** – хеш файла, запрещенного к запуску.
  - **Имя** – имя правила запрета или файла, запрещенного к запуску.
  - **Тип** – тип правила запрета. Правила запрета могут быть одного из следующих типов:
    - **Глобальный** – созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232).
    - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (если вы используете режим распределенного решения и multitenancy).
  - **Уведомление** – состояние параметра **Показать пользователю уведомление о выполнении задачи**.
  - **Запрет для** – список хостов, на которые распространяется правило запрета.

    Если запрет действует на всех хостах, отображается надпись **Всех хостов**.
- Закладка **Журнал изменений** содержит список изменений запрета: время изменения, имя пользователя, изменившего запрет, и действия над запретом.

Создание правила запрета

► *Чтобы создать правило запрета, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Нажмите на кнопку **Добавить**.

   Откроется окно создания правила запрета.
3. Укажите следующие параметры:
   a. **Состояние** – состояние правила запрета:
   b. Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
   c. Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.
   d. **MD5/SHA256 –** MD5- или SHA256-хеш файла или потока данных, запуск которого вы хотите запретить.

e. **Имя** – имя правила запрета.

f. Если вы хотите, чтобы программа выводила уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показать пользователю уведомление о выполнении задачи**.

g. **Запрет для** – область применения правила запрета:

- Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

  Этот вариант доступен только при включенном режиме распределенного решения и multitenancy.
- Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

4. Нажмите на кнопку **Добавить**.

Будет создан запрет на запуск файла.

Если вы установили флажок **Показать пользователю уведомление о выполнении задачи**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.

Включение и отключение запрета

► *Чтобы включить или отключить правило запрета, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. В строке с правилом запрета, которое вы хотите включить или отключить, в графе **Состояние** выполните одно из следующих действий:
   - Если вы хотите включить правило запрета, переведите переключатель в положение **Включено**.

     Выбранное вами правило запрета будет включено.
   - Если вы хотите отключить правило запрета, переведите переключатель в положение **Отключено**.

     Выбранное вами правило запрета будет отключено.

Удаление правила запрета

► *Чтобы удалить правило запрета, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. Нажмите на правило запрета, которое вы хотите удалить.

Откроется окно сведений о правиле запрета.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило запрета будет удалено.

Фильтрация запретов по имени

► *Чтобы отфильтровать запреты по их имени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. По ссылке **Имя** откройте меню фильтрации запретов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени запрета.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по типу

Если вы используете режим распределенного решения и multitenancy, вы можете отфильтровать правила запрета по их типу.

► *Чтобы отфильтровать правила запрета по их типу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. По ссылке **Тип** откройте меню фильтрации правил запрета.
3. Выберите один из следующих вариантов отображения правил запрета:
   - **Все**, если вы хотите, чтобы отображались все правила запрета независимо от типа.
   - **Глобальный**, если вы хотите, чтобы отображались только правила запрета, созданные на PCN. Действие этих правил запрета распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232).

- **Локальный**, если вы хотите, чтобы отображались только правила запрета, созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (если вы используете режим распределенного решения и multitenancy).

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация запретов по хешу файла

► *Чтобы отфильтровать запреты по хешу файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Хеш файла** откройте меню фильтрации запретов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов хеша файла.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация запретов по имени сервера

Если вы используете режим распределенного решения и multitenancy, вы можете отфильтровать правила запрета по серверам, на которые распространяется действие правил запрета.

► *Чтобы отфильтровать правила запрета по имени сервера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.
2. По ссылке **Серверы** откройте меню фильтрации правил запрета.

3. Установите флажки напротив тех серверов, по которым вы хотите отфильтровать правила запрета.
4. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил запрета

► *Чтобы сбросить фильтр правил запрета по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку справа от того заголовка графы таблицы правил запрета, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Работа с индикаторами компрометации и атаки

Kaspersky Anti Targeted Attack Platform использует для поиска угроз два типа индикаторов – *IOC* (Indicator of Compromise, или индикатор компрометации) и *IOA* (Indicator of Attack, или индикатор атаки).

Индикатор IOC – это набор данных о вредоносном объекте или действии. Kaspersky Anti Targeted Attack Platform использует IOC-файлы открытого стандарта описания индикаторов компрометации OpenIOC. IOC-файлы содержат набор индикаторов, при совпадении с которыми программа считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

Индикатор IOA – это правило (далее также "IOA-правило"), содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Kaspersky Anti Targeted Attack Platform проверяет базу событий (стр. 263) программы и отмечает события, которые совпадают с поведением, описанным в IOA-правилах. При проверке используется технология *потокового сканирования*, при которой объекты, загружаемые из сети, проверяются непрерывно в режиме реального времени.

IOA-правила, сформированные специалистами "Лаборатории Касперского", обновляются вместе с базами программы. Они не отображаются в интерфейсе программы и не могут быть отредактированы. Вы можете добавлять пользовательские IOA-правила (стр. 332) в виде IOC-файлов открытого стандарта описания OpenIOC, а также создавать IOA-правила на основе условий поиска по базе событий (стр. 268).

Сравнительные характеристики индикаторов IOC и IOA приведены в таблице ниже.

Таблица 15. Сравнительные характеристики индикаторов IOC и IOA

Сравнительная характеристика	IOC	IOA
Область проверки	Компьютеры с компонентом Endpoint Sensors	База событий программы
Механизм проверки	Периодическое сканирование	Потоковое сканирование
Предустановленные индикаторы от специалистов "Лаборатории Касперского"	Нет	Есть
Возможность добавить в белый список	Нет	Есть

Если вы используете режим распределенного решения и multitenancy, в разделе отображаются данные по выбранной вами организации (стр. 232).

IOC-проверка событий

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут использовать IOC-файлы для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и обнаружений, а также для проверки локальных компьютеров с установленным компонентом Endpoint Sensors.

В зависимости от режима работы программы и сервера, на который загружаются IOC-файлы, загруженные IOC-файлы могут быть одного из следующих типов:

- **Локальный** – загруженные на сервер SCN. По этим IOC-файлам производится проверка событий на этом сервере SCN. Проверяемые события относятся к организации, в рамках которой пользователь

работает в веб-интерфейсе программы (стр. 232) (в режиме распределенного решения и multitenancy).

- **Глобальный** – загруженные на сервер PCN. По этим IOC-файлам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (в режиме распределенного решения и multitenancy).

Пользователи с ролью **Старший сотрудник службы безопасности** могут управлять проверкой событий по IOC-файлам: добавлять, изменять, удалять и скачивать IOC-файлы на компьютер, включать и отключать проверку событий по IOC-файлам, а также управлять параметрами проверки объектов.

Пользователи с ролью **Сотрудник службы безопасности** могут только просматривать информацию об IOC-файлах и скачивать IOC-файлы на компьютер.

Если вы работаете с событиями, уже обнаруженными программой ранее, повторное совпадение данных этих событий с индикаторами компрометации не всегда свидетельствует о возможном обнаружении.

Просмотр таблицы IOC-файлов

Таблица IOC-файлов содержит информацию об IOC-файлах, используемых для проверки на компьютерах с компонентом Endpoint Sensors, и находится в разделе **IOC/IOA-анализ**, подразделе **IOC-проверка** окна веб-интерфейса программы.

В таблице IOC-файлов содержится следующая информация:

1.  – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

   Степень важности может иметь одно из следующих значений:

   - – низкая важность.
   -  – средняя важность.
   -  – высокая важность.
2. **Тип** – тип загруженного IOC-файла в зависимости от режима работы программы и сервера, на который загружен IOC-файл. IOC-файлы могут быть одного из следующих типов:

   - **Глобальный** – загруженные на сервер PCN. По этим IOC-файлам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (в режиме распределенного решения и multitenancy).
   - **Локальный** –загруженные на сервер SCN. По этим IOC-файлам производится проверка событий на этом сервере SCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (в режиме распределенного решения и multitenancy).
3. **Имя** – имя IOC-файла.
4. **Серверы** – имя сервера с компонентом Central Node, на котором производится проверка событий по этому IOC-файлу.

5. **Автоматическая проверка** – использование IOC-файла при автоматической проверке событий.

   Проверка событий с использованием этого IOC-файла может находиться в одном из следующих состояний:

   - **Включено**.
   - **Отключено**.

Просмотр информации об IOC-файле

► *Чтобы просмотреть информацию об IOC-файле, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOC-проверка**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об IOC-файле.

Окно содержит следующую информацию:

- **Найти обнаружения**. По ссылке открывается раздел **Обнаружения** с условием фильтрации, содержащим выбранный вами IOC-файл.
- **Найти события**. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный вами IOC-файл.
- **Скачать**. По ссылке открывается окно скачивания IOC-файла.
- **Автоматическая проверка** – использование IOC-файла при автоматической проверке событий.

  Проверка событий с использованием этого IOC-файла может находиться в одном из следующих состояний:

  - **Включено**.
  - **Отключено**.
- **Имя** – имя IOC-файла.
- **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

  Степень важности может иметь одно из следующих значений:

  - – низкая важность.
  -  – средняя важность.
  -  – высокая важность.
- **Область применения**. Отображает название организации и имена серверов, к которым относятся события, проверяемые по этому IOC-файлу (в режиме распределенного решения и multitenancy).
- **XML**. Отображает содержимое IOC-файла в формате XML.

Загрузка IOC-файла

IOC-файлы со свойствами UserItem для доменных пользователей не поддерживаются.

► *Чтобы загрузить IOC-файл, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOC-проверка**.

   Откроется таблица IOC-файлов.
2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла на вашем локальном компьютере.
3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.
4. Укажите следующие параметры:
   a. **Автоматическая проверка** – использование IOC-файла при автоматической проверке событий:
      - **Включено**.
      - **Отключено**.
   b. **Имя** – имя IOC-файла.
   c. **Важность** – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла:
      - **Низкая**.
      - **Средняя**.
      - **Высокая**.
   d. **Область применения** – название организации и имена серверов, на которых вы хотите проверять события по этому IOC-файлу (в режиме распределенного решения и multitenancy).
5. Нажмите на кнопку **Сохранить**.

IOC-файл будет загружен в формате XML.

Скачивание IOC-файла на компьютер

Вы можете скачать ранее загруженный IOC-файл на компьютер.

► *Чтобы скачать IOC-файл на компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOC-проверка**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, который вы хотите скачать.

   Откроется окно с информацией об IOC-файле.
3. В зависимости от параметров вашего браузера, по ссылке **Скачать** сохраните файл в папку по умолчанию или укажите папку для сохранения файла.

IOC-файл будет сохранен на компьютер в папку загрузки браузера.

Включение и отключение автоматического использования IOC-файла при проверке событий

Вы можете включить или отключить автоматическое использование IOC-файла при проверке событий.

► *Чтобы включить или отключить автоматическое использование IOC-файла при проверке событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOC-проверка**.

   Откроется таблица IOC-файлов.
2. В строке с IOC-файлом, использование которого вы хотите включить или отключить, в графе **Автоматическая проверка** переведите переключатель в одно из следующих положений:
   - **Включено**.
   - **Отключено**.
3. Нажмите на кнопку **Сохранить**.

Автоматическое использование IOC-файла при проверке событий будет включено или отключено.

Удаление IOC-файла

► *Чтобы удалить IOC-файл, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOC-проверка**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, который вы хотите удалить.

   Откроется окно с информацией об IOC-файле.
3. Нажмите на кнопку **Удалить**.

IOC-файл будет удален.

Поиск результатов IOC-проверки

► *Чтобы найти и просмотреть результаты IOC-проверки, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOC-проверка**.

   Откроется таблица IOC-файлов.
2. Выберите IOC-файл, для которого вы хотите просмотреть результаты проверки.

   Откроется окно с информацией об IOC-файле.
3. Выполните одно из следующих действий:
   - Если вы хотите просмотреть обнаружения, найденные с помощью IOC-файла, по ссылке **Найти обнаружения** перейдите в базу обнаружений.

     Откроется новая закладка браузера с таблицей найденных обнаружений.
   - Если вы хотите просмотреть события, найденные с помощью IOC-файла, по ссылке **Найти события** перейдите в базу событий.

     Откроется новая закладка браузера с таблицей найденных событий.

Фильтрация и поиск IOC-файлов

► *Чтобы отфильтровать или найти IOC-файлы по требуемым критериям, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOC-проверка**.

   Откроется таблица IOC-файлов.
2. Выполните следующие действия в зависимости от критерия фильтрации:
   - **По степени важности**
   - **По имени файла**
   - **По имени сервера**
   - **По состоянию IOC-файлов**

В таблице IOC-фалов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра IOC-файлов

► *Чтобы сбросить фильтр IOC-файлов по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOC-проверка**.

   Откроется таблица IOC-файлов.
2. Нажмите на кнопку справа от того заголовка графы таблицы IOC-файлов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице IOC-фалов отобразятся только IOC-файлы, соответствующие заданным вами условиям.

Настройка расписания IOC-проверки

Вы можете настроить расписание IOC-проверки компьютеров, на которых установлен компонент Endpoint Sensors.

► *Чтобы настроить расписание IOC-проверки, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Расписание IOC-проверки**.
2. В раскрывающихся списках **Время запуска** выберите время начала проверки.
3. В раскрывающемся списке **Ограничение по времени** выберите ограничение по времени выполнения

проверки.

Если проверка не завершится за указанное время, некоторые события могут быть не найдены.

4. Нажмите на кнопку **Сохранить**.

Новое расписание IOC-проверки начнет действовать сразу после сохранения изменений. Результаты IOC-проверки будут отображаться в таблице обнаружений.

Поддерживаемые индикаторы компрометации OpenIOC

Kaspersky Anti Targeted Attack Platform поддерживает индикаторы компрометации открытого стандарта OpenIOC, приведенные в таблице ниже.

Таблица 16. Поддерживаемые индикаторы компрометации

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
FileItem/FileName	Нет значения.
FileItem/Md5sum	Нет значения.
FileItem/FilePath	Не поддерживается раскрытие user-specific переменных окружения. Например, `%APPDATA%`, `%UserName%`.
FileItem/SizeInBytes	Нет значения.
RegistryItem/KeyPath	Нет значения.
RegistryItem/Path	Не поддерживаются сканирование user-specific ключей через HKEY_CURRENT_USER и HKEY_CLASSES_ROOT для неавторизованных пользователей.
RegistryItem/Value	Нет значения.
FileItem/PEInfo/PETimeStamp	Нет значения.
FileItem/FullPath	Не поддерживается раскрытие user-specific переменных окружения. Например, `%APPDATA%`, `%UserName%`.
PortItem/remoteIP	Нет значения.
FileItem/PEInfo/DetectedAnomalies/string	Поддерживается только checksum_is_zero.
FileItem/FileExtension	Нет значения.
DnsEntryItem/RecordName	Нет значения.
ProcessItem/name	Нет значения.
RegistryItem/ValueName	Нет значения.
RegistryItem/Text	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
ServiceItem/name	Нет значения.
FileItem/PEInfo/Exports/ExportedFunctions/string	Нет значения.
FileItem/PEInfo/Exports/DllName	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/OriginalFilename	Нет значения.
FileItem/PEInfo/ImportedModules/Module/ImportedFunctions/string	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileDescription	Нет значения.
ProcessItem/arguments	Нет значения.
PortItem/remotePort	Нет значения.
DnsEntryItem/RecordData/IPv4Address	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/InternalName	Нет значения.
FileItem/PEInfo/Exports/NumberOfFunctions	Нет значения.
FileItem/PEInfo/DigitalSignature/SignatureExists	Нет значения.
ProcessItem/SectionList/MemorySection/Name	Нет значения.
FileItem/PEInfo/Type	Нет значения.
ProcessItem/path	Нет значения.
PortItem/localPort	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/CompanyName	Нет значения.
ProcessItem/SectionList/MemorySection/Md5sum	Нет значения.
DnsEntryItem/Host	Нет значения.
PortItem/protocol	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductName	Нет значения.
ServiceItem/description	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Name	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Language	Нет значения.
ServiceItem/descriptiveName	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Language	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalCopyright	Нет значения.
FileItem/PEInfo/ImportedModules/Module/Name	Нет значения.
ServiceItem/serviceDLL	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileVersion	Нет значения.
FileItem/PEInfo/Sections/Section/Name	Нет значения.
FileItem/PEInfo/DigitalSignature/SignatureVerified	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
ServiceItem/path	Нет значения.
FileItem/PEInfo/Subsystem	Нет значения.
FileItem/Sha256sum	Нет значения.
RegistryItem/Type	Нет значения.
FileItem/PEInfo/DigitalSignature/CertificateSubject	Нет значения.
EventLogItem/EID	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Type	Нет значения.
VolumeItem/Name	Нет значения.
EventLogItem/source	Нет значения.
PortItem/state	Нет значения.
UserItem/Username	Сканируются только локальные пользователи. Сканирование доменных пользователей не поддерживается.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductVersion	Нет значения.
DnsEntryItem/RecordType	Нет значения.
VolumeItem/VolumeName	Нет значения.
PortItem/localIP	Нет значения.
ProcessItem/parentpid	Нет значения.
FileItem/PEInfo/DigitalSignature/CertificateIssuer	Нет значения.
ProcessItem/SectionList/MemorySection/Protection	Нет значения.
ProcessItem/SectionList/MemorySection/Sha256sum	Нет значения.
FileItem/PEInfo/Exports/ExportsTimeStamp	Нет значения.
ProcessItem/Username	Нет значения.
ServiceItem/status	Нет значения.
ArpEntryItem/CacheType	Нет значения.
ArpEntryItem/IPv4Address	Нет значения.
ArpEntryItem/Interface	Нет значения.
ArpEntryItem/PhysicalAddress	Нет значения.
DnsEntryItem/DataLength	Нет значения.
DnsEntryItem/Flags	Нет значения.
DnsEntryItem/RecordData/Host	Нет значения.
DnsEntryItem/RecordName	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
DnsEntryItem/TimeToLive	Нет значения.
VolumeItem/ActualAvailableAllocationUnits	Нет значения.
VolumeItem/BytesPerSector	Нет значения.
VolumeItem/CreationTime	Нет значения.
VolumeItem/DevicePath	Нет значения.
VolumeItem/DriveLetter	Нет значения.
VolumeItem/FileSystemFlags	Нет значения.
VolumeItem/FileSystemName	Нет значения.
VolumeItem/IsMounted	Нет значения.
VolumeItem/SectorsPerAllocationUnit	Нет значения.
VolumeItem/SerialNumber	Нет значения.
VolumeItem/TotalAllocationUnits	Нет значения.
VolumeItem/Type	Нет значения.
UserItem/LastLogin	Нет значения.
UserItem/SecurityID	Нет значения.
UserItem/SecurityType	Нет значения.
UserItem/description	Нет значения.
UserItem/disabled	Нет значения.
UserItem/fullname	Нет значения.
UserItem/homedirectory	Нет значения.
UserItem/lockedout	Нет значения.
UserItem/passwordrequired	Нет значения.
UserItem/scriptpath	Нет значения.
UserItem/userpasswordage	Нет значения.
PortItem/CreationTime	Нет значения.
PortItem/path	Нет значения.
PortItem/pid	Нет значения.
PortItem/process	Нет значения.
EventLogItem/log	Нет значения.
EventLogItem/index	Нет значения.
EventLogItem/user	Нет значения.
EventLogItem/genTime	Нет значения.

Индикатор компрометации OpenIOC	Ограничения в реализации (если имеются)
EventLogItem/machine	Нет значения.
EventLogItem/CorrelationActivityId	Нет значения.
EventLogItem/CorrelationRelatedActivityId	Нет значения.
EventLogItem/ExecutionProcessId	Нет значения.
EventLogItem/ExecutionThreadId	Нет значения.
RegistryItem/Hive	Не поддерживаются сканирование user-specific ключей через HKEY_CURRENT_USER и HKEY_CLASSES_ROOT для неавторизованных пользователей.
ServiceItem/pid	Нет значения.
ServiceItem/type	Нет значения.
ServiceItem/startedAs	Нет значения.
ServiceItem/arguments	Нет значения.
ServiceItem/mode	Нет значения.
ProcessItem/pid	Нет значения.
ProcessItem/startTime	Нет значения.
ProcessItem/SectionList/MemorySection/RegionSize	Нет значения.
ProcessItem/SectionList/MemorySection/RegionStart	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Comments	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalTrademarks	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/PrivateBuild	Нет значения.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/SpecialBuild	Нет значения.
FileItem/PEInfo/BaseAddress	Нет значения.
FileItem/PEInfo/Exports/NumberOfNames	Нет значения.
FileItem/PEInfo/ImportedModules/Module/NumberOfFunctions	Нет значения.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Size	Нет значения.
FileItem/PEInfo/Sections/ActualNumberOfSections	Нет значения.
FileItem/PEInfo/Sections/NumberOfSections	Нет значения.
FileItem/PEInfo/Sections/Section/SizeInBytes	Нет значения.

IOA-анализ событий

Программа анализирует события с помощью IOA-правил. Специалисты "Лаборатории Касперского" предоставляют набор IOA-правил, содержащих примеры наиболее частых подозрительных действий в системе пользователя. Кроме того, пользователи могут создавать свои IOA-правила.

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** могут управлять IOA-правилами: добавлять (стр. 332), удалять (стр. 334), включать и отключать правила (стр. 331), а также добавлять IOA-правила "Лаборатории Касперского" в белый список (стр. 336). Пользователи с ролями **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности** могут использовать IOA-правила для поиска признаков целевых атак (стр. 337), зараженных и возможно зараженных объектов в базе событий и обнаружений, а также просматривать таблицу IOA-правил (стр. 330) и информацию об IOA-правилах (стр. 330).

Различия между пользовательскими правилами и правилами "Лаборатории Касперского" представлены в таблице ниже.

Таблица 17. Сравнительные характеристики IOA-правил

Сравнительная характеристика	Пользовательские правила	Правила "Лаборатории Касперского"
Наличие рекомендаций по реагированию на событие	Нет	Есть Вы можете посмотреть рекомендации в информации об обнаружении (стр. 252)
Соответствие технике в базе MITRE ATT&CK	Нет	Есть Вы можете посмотреть описание техники по классификации MITRE в информации об обнаружении (стр. 252)
Отображение в таблице IOA-правил (стр. 330)	Да	Нет
Способ отключить проверку базы по этому правилу	Отключить правило (стр. 331)	Добавить правило в белый список (стр. 336)
Возможность удалить или добавить правило	Вы можете удалить (стр. 334) или добавить правило (стр. 332) в веб-интерфейсе программы	Правила обновляются вместе с базами программы и не могут быть удалены пользователем
Поиск результатов IOA-анализа (стр. 337)	По ссылкам **Обнаружения** и **События** в окне с информацией об IOA-правиле (стр. 330)	По ссылкам **Обнаружения** и **События** в окне с информацией об обнаружении (стр. 250)

В зависимости от режима работы программы и сервера, на котором создаются IOA-правила, пользовательские IOA-правила могут быть одного из следующих типов:

- **Локальный** – созданные на сервере SCN. По этим IOA-правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (в режиме распределенного решения и multitenancy).
- **Глобальный** – созданные на сервере PCN. По этим IOA-правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые

события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (в режиме распределенного решения и multitenancy).

Просмотр таблицы IOA-правил

Таблица IOA-правил содержит информацию об IOA-правилах, используемых для проверки базы событий, и находится в разделе **IOC/IOA-анализ**, подразделе **IOA-анализ** окна веб-интерфейса программы.

В таблице IOA-правил содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOA-правила.

   Степень важности может иметь одно из следующих значений:

   - – **Низкая**.
   -  – **Средняя**.
   -  – **Высокая**.
2. **Тип** – тип правила в зависимости от роли сервера, на котором оно создано, в режиме распределенного решения и multitenancy (стр. 42):
   - **Глобальный** – правило создано на сервере PCN.
   - **Локальный** – правило создано на сервере SCN.
3. **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:
   - **Высокая**.
   - **Средняя**.
   - **Низкая**.

   Чем выше надежность, тем меньше вероятность ложных срабатываний
4. **Имя** – название правила.
5. **Серверы** – имя сервера с компонентом Central Node, на котором применяется правило.
6. **Создавать обнаружения** – требование сохранять информацию об обнаружении на основе совпадения события из базы с критериями правила.
   - **Включено** – для события создается запись в таблице обнаружений с указанием технологии IOA.
   - **Отключено** – не отображается в таблице обнаружений.
7. **Состояние** – использование правила при проверке базы событий:
   - **Включено** – правило используется.
   - **Отключено** – правило не используется.

Просмотр информации об IOA-правиле

► *Чтобы просмотреть информацию об IOA-правиле, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

Откроется таблица IOA-правил.

2. Выберите IOA-правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об IOA-правиле.

Окно содержит следующую информацию:

- **События**. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим выбранное вами IOA-правило.
- **Обнаружения**. По ссылке открывается раздел **Обнаружения** с условием фильтрации, содержащим выбранное вами IOA-правило.
- **IOA ID** По ссылке открывается идентификатор, присваиваемый программой каждому правилу.

  Изменение идентификатора недоступно. Вы можете скопировать идентификатор по кнопке **Скопировать значение в буфер**.
- **Состояние** – использование правила при проверке базы событий.

На закладке **Сведения** отображается следующая информация:

- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Описание** – любая дополнительная информация о правиле, которую вы указали.
- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, указанная пользователем при добавлении правила.
- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, заданный пользователем при добавлении правила.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Глобальный** – созданные на сервере PCN. По этим IOA-правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (в режиме распределенного решения и multitenancy).
  - **Локальный** – созданные на сервере SCN. По этим IOA-правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к организации, в рамках которой пользователь работает в веб-интерфейсе программы (стр. 232) (в режиме распределенного решения и multitenancy).
- **Область применения** – имена серверов с компонентом Central Node, на которых применяется правило.

На закладке **Запрос** отображается исходный код запроса, по которому осуществляется проверка. По ссылке с текстом запроса вы можете перейти в раздел **Поиск угроз** и просмотреть все события по заданным критериям поиска (стр. 241).

Включение и отключение использования IOA-правила

Вы можете включить или отключить использование одного или нескольких правил, а также всех правил сразу.

► *Чтобы включить или отключить использование IOA-правила при проверке базы событий,*

выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.

2. В строке с нужным IOA-правилом в графе **Состояние** включите или выключите переключатель.

Использование IOA-правила при проверке базы событий будет включено или отключено.

► *Чтобы включить или отключить использование всех или нескольких IOA-правил при проверке событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.

2. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками граф.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование всех правил.

Использование выбранных пользовательских IOA-правил при проверке событий будет включено или отключено.

Эти изменения не влияют на работу IOA-правил "Лаборатории Касперского". Если вы не хотите использовать при проверке IOA-правило "Лаборатории Касперского", вам требуется добавить его в белый список (стр. 336).

Добавление IOA-правила

► *Чтобы добавить IOA-правило, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.

2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла на вашем локальном компьютере.

3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

   Откроется окно **Новое IOA-правило**.

   По ссылке **События** вы можете просмотреть список угроз в базе событий, соответствующих заданным в файле критериям.

4. Включите или выключите переключатель **Состояние** для использования правила при проверке базы событий.
5. В поле **Имя** введите имя правила.
6. В поле **Описание** введите любую дополнительную информацию о правиле.
7. В раскрывающемся списке **Важность** выберите степень важности, которая будет присвоена

обнаружению, произведенному с использованием этого IOA-правила:

- **Низкая**.
- **Средняя**.
- **Высокая**.

8. В раскрывающемся списке **Надежность** выберите уровень надежности этого правила, по вашей оценке:
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.
9. В блоке параметров **Область применения** установите флажки напротив тех серверов, на которых вы хотите применить правило.
10. На закладке **Запрос** проверьте заданные условия поиска. Если требуется, внесите изменения.
11. Нажмите на кнопку **Сохранить**.

IOA-правило будет добавлено.

Вы также можете добавить IOA-правило, сохранив условия поиска (стр. 268) по базе событий в разделе **Поиск угроз**.

Изменение IOA-правила

Вы можете изменять только пользовательские IOA-правила. Изменение правил "Лаборатории Касперского" недоступно.

При работе в режиме распределенного решения и multitenancy вы можете изменять только те IOA-правила, которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно изменение только правил, созданных на PCN. В веб-интерфейсе SCN доступно изменение только правил, созданных на SCN.

► *Чтобы изменить IOA-правило, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.
2. Выберите IOA-правило, которое вы хотите изменить.

   Откроется окно с информацией об IOA-правиле.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Сохранить**.

Параметры IOA-правила будут изменены.

Удаление IOA-правила

Вы можете удалить одно или несколько правил, а также все правила сразу.

При работе в режиме распределенного решения вы можете удалять только те IOA-правила, которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно удаление только правил, созданных на PCN. В веб-интерфейсе SCN доступно удаление только правил, созданных на SCN.

► *Чтобы удалить IOA-правило, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.
2. Выберите IOA-правило, которое вы хотите удалить.

   Откроется окно с информацией об IOA-правиле.
3. Нажмите на кнопку **Удалить**.

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

IOA-правило будет удалено.

► *Чтобы удалить все или несколько IOA-правил, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.
2. Установите флажки слева от правил, которые вы хотите удалить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками граф.

   В нижней части окна отобразится панель управления.
3. Нажмите на кнопку **Удалить**.

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

Выбранные пользовательские IOA-правила будут удалены.

Вы не можете удалить IOA-правила "Лаборатории Касперского". Если вы не хотите использовать при проверке IOA-правило "Лаборатории Касперского", вам требуется добавить его в белый список (стр. 336).

Просмотр белого списка IOA

► *Чтобы просмотреть белый список IOA-правил,*

в окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **Белый список IOA**.

Отобразится таблица IOA-правил, добавленных в белый список. Вы можете фильтровать правила по

ссылкам в названии граф.

В таблице IOA-правил содержится следующая информация:

1.  – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOA-правила.

   Степень важности может иметь одно из следующих значений:

   - – **Низкая**.
   -  – **Средняя**.
   -  – **Высокая**.
2. **Тип** – тип правила в зависимости от роли сервера, на котором оно создано, в режиме распределенного решения и multitenancy (стр. 42):
   - **Глобальный** – правило создано на сервере PCN.
   - **Локальный** – правило создано на сервере SCN.
3. **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:
   - **Высокая**.
   - **Средняя**.
   - **Низкая**.

   Чем выше надежность, тем меньше вероятность ложных срабатываний
4. **Имя** – название правила.
5. **Серверы** – имя сервера с компонентом Central Node, на котором применяется правило.

Просмотр информации об IOA-правиле в белом списке

► *Чтобы просмотреть информацию об IOA-правиле, добавленном в белый список, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **Белый список IOA**.

   Отобразится таблица IOA-правил, добавленных в белый список.
2. Выберите IOA-правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **IOA-правило**. По ссылке открывается окно с описанием техники MITRE, соответствующей этому правилу, рекомендациям по реагированию на событие и данными о вероятности ложных срабатываний.
- **ID** – идентификатор, присваиваемый программой каждому правилу.
- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, по оценке специалистов "Лаборатории Касперского".

- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, по оценке специалистов "Лаборатории Касперского".
- **Применить к серверам*** – список организаций и серверов, на которых применяется IOA-правило, добавленное в белый список.

Добавление IOA-правила в белый список

Добавление в белый список доступно только для IOA-правил "Лаборатории Касперского". Если вы не хотите применять при проверке базы событий пользовательское IOA-правило, вы можете отключить это правило (стр. 331) или удалить его (стр. 334).

► *Чтобы добавить IOA-правило в белый список из раздела **Обнаружения**, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке в графе **Технологии** откройте окно настройки фильтрации.
3. В левом раскрывающемся списке выберите **Содержит**.
4. В правом раскрывающемся списке выберите **(IOA) IOA-анализ**.
5. Нажмите на кнопку **Применить**.

   В таблице отобразятся обнаружения, выполненные на основе IOA-правил.
6. Выберите обнаружение, для которого в графе **Обнаружено** отображается название нужного IOA-правила.

   Откроется окно с информацией об обнаружении.
7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.
8. Нажмите на кнопку **Добавить в белый список**.

   Откроется окно с информацией о правиле.
9. Нажмите на кнопку **Добавить**.

IOA-правило будет добавлено в белый список. Это правило не будет применяться при проверке базы событий.

► *Чтобы добавить IOA-правило в белый список из раздела **Поиск угроз**, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.
2. Задайте условия поиска и нажмите на кнопку **Найти**.

   Отобразится список серверов, на которых были обнаружены события по заданным критериям.
3. Выберите нужный сервер.

4. Выберите событие в таблице с результатами поиска.

   Откроется окно с информацией о событии.

5. Перейдите по ссылке в поле **Имя IOA**.

   Откроется окно с информацией об обнаружении.

6. Нажмите на кнопку **Добавить в белый список**.

   Откроется окно с информацией о правиле.

7. Нажмите на кнопку **Добавить**.

IOA-правило будет добавлено в белый список. Это правило не будет применяться при проверке базы событий.

Удаление IOA-правила из белого списка

Вы можете удалить из белого списка одно или несколько правил, а также все правила сразу.

► *Чтобы удалить IOA-правило из белого списка, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**, подраздел **Белый список IOA**.

   Откроется таблица IOA-правил, добавленных в белый список.

2. Выберите IOA-правило, которое вы хотите удалить из белого списка.

   Откроется окно с информацией об IOA-правиле.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

IOA-правило будет удалено из белого списка. Правило будет применяться при проверке базы событий.

► *Чтобы удалить все или несколько IOA-правил из белого списка, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC-проверка**, подраздел **Белый список IOA**.

   Откроется таблица IOA-правил, добавленных в белый список.

2. Установите флажки напротив правил, которые вы хотите удалить из белого списка.

   Вы можете выбрать все правила, установив флажок в строке с заголовками граф.

3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные IOA-правила будут удалены из белого списка. Правила будут применяться при проверке базы событий.

Поиск результатов IOA-анализа

► *Чтобы найти и просмотреть результаты IOA-анализа по пользовательским правилам,*

выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.

2. Выберите IOA-правило, для которого вы хотите просмотреть результаты проверки.

   Откроется окно с информацией об IOA-правиле.

3. Выполните одно из следующих действий:

   - Если вы хотите просмотреть обнаружения, найденные с помощью IOA-правила, по ссылке **Обнаружения** перейдите в базу обнаружений.

     Откроется новая закладка браузера с таблицей найденных обнаружений.

   - Если вы хотите просмотреть события, найденные с помощью IOA-правила, по ссылке **События** перейдите в базу событий.

     Откроется новая закладка браузера с таблицей найденных событий.

► *Чтобы найти и просмотреть результаты IOA-анализа по правилам "Лаборатории Касперского", выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке в графе **Технологии** откройте окно настройки фильтрации.
3. В левом раскрывающемся списке выберите **Содержит**.
4. В правом раскрывающемся списке выберите **(IOA) IOA-анализ**.
5. Нажмите на кнопку **Применить**.

   В таблице отобразятся обнаружения, выполненные на основе IOA-правил.

6. Выберите обнаружение, для которого в графе **Обнаружено** отображается название нужного IOA-правила.

   Откроется окно с информацией об обнаружении.

7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.
8. Выполните одно из следующих действий:

   - Если вы хотите просмотреть обнаружения, найденные с помощью IOA-правила, по ссылке **Обнаружения** перейдите в базу обнаружений.

     Откроется новая закладка браузера с таблицей найденных обнаружений.

   - Если вы хотите просмотреть события, найденные с помощью IOA-правила, по ссылке **События** перейдите в базу событий.

     Откроется новая закладка браузера с таблицей найденных событий.

Фильтрация и поиск IOA-правил

► *Чтобы отфильтровать или найти IOA-правила по требуемым критериям, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.

2. Выполните следующие действия в зависимости от критерия фильтрации:
   - **По степени важности**
   - **По типу правила**
   - **По уровню надежности**
   - **По названию правила**
   - **По имени сервера**
   - **По созданию обнаружений на основе правила**
   - **По состоянию правила**

В таблице IOA-правил отобразятся только IOA-правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра IOA-правил

► *Чтобы сбросить фильтр IOA-правил по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **IOC/IOA-анализ**, подраздел **IOA-анализ**.

   Откроется таблица IOA-правил.

2. Нажмите на кнопку  справа от того заголовка графы таблицы IOA-правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице IOA-правил отобразятся только IOA-правила, соответствующие заданным вами условиям.

Работа с объектами в Хранилище

Вы можете поместить копии объектов, которые хотите проверить, в специальное Хранилище.

Хранилище расположено на сервере Central Node.

Если вы используете режим распределенного решения и multitenancy, Хранилище расположено на серверах PCN и SCN. В веб-интерфейсе сервера PCN отображается информация о Хранилище всех подключенных SCN в рамках тех организаций, к данным которых у пользователя есть доступ (стр. 158).

Пользователь с ролью **Старший сотрудник службы безопасности** может поместить копии объектов в Хранилище с помощью задачи **Получить файл** или загрузив объект в Хранилище вручную (стр. 343) на том сервере PCN или SCN, с которым он работает в рамках тех организаций, к данным которых у него есть доступ (стр. 158).

Пользователь с ролью **Сотрудник службы безопасности** может работать только с файлами, полученными в результате выполнения задач, которые он сам создал на том сервере PCN или SCN, с которым он работает в рамках тех организаций, к данным которых у него есть доступ (стр. 158).

Если вы считаете объект опасным, вы можете поместить его в Карантин.

Карантин – это специальная область Хранилища, предназначенная для хранения файлов, которые могут нанести вред компьютерам или локальной сети организации. Вы можете переместить файлы с хоста в Карантин для проверки перед удалением или восстановлением в случае отсутствия угрозы.

При отправке объекта в Карантин выполняется его перемещение, а не копирование: объект удаляется с хоста и сохраняется в Карантине.

Вы можете управлять объектами в Хранилище: удалять, скачивать, загружать, отправлять на проверку, а также фильтровать списки объектов.

Kaspersky Anti Targeted Attack Platform отображает объекты в Хранилище в виде таблицы объектов.

По умолчанию максимальный объем Хранилища (помимо Карантина) составляет 10 ГБ. Как только объем Хранилища превышает заданное по умолчанию пороговое значение, программа начинает удалять из Хранилища самые старые копии объектов. Когда объем Хранилища снова становится меньше порогового значения, программа прекращает удалять копии объектов из Хранилища. Информация о степени заполненности Хранилища отображается в разделе **Хранилище**, подразделе **Объем**.

Максимальный объем Карантина составляет 10 ГБ. Если объем Карантина превысит заданное по умолчанию пороговое значение, вы не сможете помещать в него новые объекты, пока не удалите часть старых объектов. Информация о степени заполненности Карантина отображается в разделе **Хранилище**, подразделе **Объем** в верхней части окна веб-интерфейса программы.

Максимальный объем файла, который можно поместить в Карантин, составляет 100 МБ.

Реальный размер файла может быть больше видимого размера файла из-за метаданных, необходимых для восстановления файла из Карантина. При помещении в Карантин учитывается реальный размер файла. Зашифрованные файлы могут передаваться в расшифрованном виде (в зависимости от параметров шифрования), сжатые файлы передаются в исходном виде.

Просмотр таблицы объектов, помещенных в Хранилище

Таблица объектов, помещенных в Хранилище, находится в разделе **Хранилище**, подразделе **Файлы**.

В таблице объектов, помещенных в Хранилище, содержится следующая информация:

1. **Тип** – расположение объекта в Хранилище.

   Возможны следующие типы объектов:

   -  – объект не помещен в Карантин;
   -  – объект помещен в Карантин;
   -  – объект загружен пользователем.
2. **Объект** – информация об объекте. Например, имя файла или путь к файлу.
3. **Результаты проверки** – результат проверки объекта.

   Результат проверки отображается в виде одного из следующих значений:

   - **Не обнаружено** – в результате проверки программа не обнаружила признаков целевой атаки, возможно зараженных объектов или подозрительной активности.
   - **С ошибкой** – проверка объекта завершилась с ошибкой.
   - **Выполняется** – проверка объекта еще не завершилась.
   - **Не выполнялась** – объект не был отправлен на проверку.
   - **Обнаружено** – в результате проверки программа обнаружила признаки целевой атаки, возможно зараженный объект или подозрительную активность.
4. **Серверы** – имя сервера Central Node, PCN или SCN. К этому серверу подключен хост, с которого получен объект.
5. **Адрес источника** – IP-адрес или имя хоста, с которого получен объект, или имя учетной записи пользователя, загрузившего объект.
6. **Время** – дата и время помещения объекта в Хранилище.

Просмотр информации об объекте в Хранилище

► *Чтобы просмотреть информацию об объекте в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. В таблице выберите объект, информацию о котором вы хотите посмотреть.

Откроется окно сведений об объекте.

В окне содержится следующая информация:

- **Имя файла** – имя файла.

  По ссылке рядом с **Имя файла** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **SHA256** – SHA256-хеш файла.

  По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на Kaspersky Threat Intelligence Portal**.
  - **Найти на virustotal.com**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- **Время** – время помещения объекта в Хранилище.
- **Время загрузки** – время загрузки для объектов, загруженных пользователем вручную.
- **Организация** – название организации, к которой относится сервер Central Node, PCN или SCN.
- **Сервер** – имя сервера Central Node, PCN или SCN. К этому серверу подключен хост, с которого получен объект.
- **Хост** – имя хоста, с которого получен объект.
- **Имя пользователя** – имя учетной записи пользователя, загрузившего объект в Хранилище вручную.
- **Результаты проверки** – результат проверки объекта программой.

Скачивание объектов из Хранилища

Если вы считаете объект в Хранилище безопасным, вы можете скачать его на локальный компьютер.

Скачивание зараженных объектов может угрожать безопасности вашего локального компьютера.

► *Чтобы скачать объект из Хранилища, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В правой части строки с именем объекта, который вы хотите скачать, нажмите на кнопку 

Объект будет сохранен на ваш локальный компьютер в папку загрузки браузера. Файл загружается в формате ZIP-архива, защищенного паролем infected.

Загрузка объектов в Хранилище

Если вам требуется запустить проверку определенного объекта, вы можете загрузить этот объект в Хранилище и отправить его на проверку (стр. 343).

► *Чтобы загрузить объект в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. В правом верхнем углу окна нажмите на кнопу **Загрузить**.

   Откроется окно выбора файла.

3. Выберите объект, который вы хотите загрузить в Хранилище, и нажмите на кнопку **Open**.

Объект будет загружен в Хранилище и отобразится в таблице объектов.

Проверка объектов из Хранилища

Вы можете проверить объекты, помещенные в Хранилище, компонентом Central Node с помощью технологий Anti-Malware Engine и YARA, а также компонентом Sandbox.

Рекомендуется отправлять объекты из Хранилища на проверку в следующих случаях:

- проверка при помещении в Хранилище была отключена;
- базы программы были обновлены;
- объект был загружен в Хранилище вручную.

► *Чтобы отправить объект из Хранилища на проверку, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

Откроется таблица объектов.

2. Нажмите на объект, который вы хотите проверить.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Проверить**.

Запустится проверка объекта.

После завершения проверки объекта его статус отобразится в таблице объектов.

Удаление объектов из Хранилища

► *Чтобы удалить объект из Хранилища, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. Нажмите на объект, который вы хотите удалить.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Объект будет удален из Хранилища.

Фильтрация объектов в Хранилище по типу объекта

► *Чтобы отфильтровать объекты в Хранилище по их типу, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Тип** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:
   - **Файл в Хранилище**, если вы хотите, чтобы программа отображала в таблице объекты, содержащиеся в Хранилище, но не помещенные в Карантин.
   - **Файл в Карантине**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Карантин.
   - **Файл загружен**, если вы хотите, чтобы программа отображала в таблице объекты, загруженные пользователем вручную.
4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по описанию объекта

► *Чтобы отфильтровать объекты в Хранилище по описанию объекта, выполните*

следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Объект** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих вариантов:
   - **Путь к файлу**.
   - **MD5**.
   - **SHA256**.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
   - **Равняется**.
   - **Не равняется**.
   - **Соответствует шаблону**.
   - **Не соответствует шаблону**.
5. В поле ввода укажите один или несколько символов описания объекта.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по результатам проверки

► *Чтобы отфильтровать объекты в Хранилище по результатам проверки этих объектов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.
2. По ссылке **Результаты проверки** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:
   - **Не обнаружено**.
   - **С ошибкой**.
   - **Выполняется**.
   - **Не выполнялась**.

- **Обнаружено**.

4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по имени сервера Central Node, PCN или SCN

► *Чтобы отфильтровать объекты в Хранилище по имени сервера Central Node, PCN или SCN, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Серверы** откройте меню фильтрации объектов.
3. Установите один или несколько флажков напротив тех серверов, по которым вы хотите отфильтровать объекты в Хранилище.
4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов в Хранилище по источнику объекта

► *Чтобы отфильтровать объекты в Хранилище по источнику, с которого они были получены, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Адрес источника** откройте меню фильтрации объектов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации объектов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов IP-адреса, имени хоста или имени учетной записи пользователя, загрузившего объект вручную.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку  и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация объектов по времени помещения в Хранилище

► *Чтобы отфильтровать объекты по времени помещения в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. По ссылке **Время** откройте меню фильтрации объектов.
3. Выберите один из следующих периодов отображения объектов:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все помещенные в Хранилище объекты.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище за указанный вами период.
4. Если вы выбрали период отображения объектов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения объектов.
   b. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра объектов в Хранилище

► *Чтобы сбросить фильтр объектов в Хранилище по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

   Откроется таблица объектов.

2. Нажмите на кнопку  справа от того заголовка графы таблицы объектов в Хранилище, условия фильтрации по которому вы хотите сбросить.

Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Просмотр используемого места в Хранилище и Карантине

Информация о степени заполненности Хранилища и Карантина находится в разделе **Хранилище**, подразделе **Объем**.

В таблице содержится следующая информация:

1. **Сервер** – имя сервера Central Node, PCN или SCN. К этому серверу подключены хосты, с которых получены объекты в Хранилище.
2. **Используемое место** – объем используемого места в Хранилище и Карантине.

По умолчанию максимальный объем Хранилища (помимо Карантина) составляет 10 ГБ. Как только объем Хранилища превышает заданное по умолчанию пороговое значение, программа начинает удалять из Хранилища самые старые копии объектов. Когда объем Хранилища снова становится меньше порогового значения, программа прекращает удалять копии объектов из Хранилища.

Максимальный объем Карантина составляет 10 ГБ. Если объем Карантина превысит заданное по умолчанию пороговое значение, вы не сможете помещать в него новые объекты, пока не удалите часть старых объектов.

Работа с отчетами

При работе в веб-интерфейсе программы пользователи **Старший сотрудник службы безопасности** могут управлять отчетами об обнаружениях программы: создавать шаблоны отчетов (стр. 349), создавать отчеты по шаблону (стр. 351), просматривать и удалять отчеты и шаблоны отчетов.

Отчет формируется на основе выборки обнаружений за указанный период. Если вы используете режим распределенного решения и multitenancy, выборка данных осуществляется также по организации и серверам этой организации.

Управление шаблонами отчетов и отчетами доступно во всех режимах работы программы в соответствии с лицензией.

Выполняйте действия по созданию отчета в следующем порядке:

a. **Создайте шаблон отчета (стр. 349).**

b. **Создайте отчет на основе шаблона (стр. 351).**

Создание шаблона

При создании шаблона отчета вам нужно указать всю информацию, которую вы хотите отображать в отчете: имя отчета, его описание, наличие таблицы, графика или изображения. Также вы можете выбрать данные, которые вы хотите отображать в отчете и задать расположение элементов отчета. Создание отчета (стр. 351) в разделе **Отчеты**, подразделе **Созданные отчеты** интерфейса позволяет только выбрать шаблон для создания отчета и период отображения данных.
Создавайте новый шаблон отчета для каждой выборки данных.

► *Чтобы создать шаблон, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Нажмите на кнопку **Добавить**.

   Откроется окно создания шаблона. Окно содержит тело отчета и конструктор отчета в плавающем окне. Вы можете перемещать конструктор отчета по рабочей области окна веб-интерфейса.

3. В поле **Имя отчета** в правом верхнем углу окна введите имя, которое вы хотите присвоить отчетам, создаваемым по этому шаблону. Например, **Обнаружения по технологии**.

   Это имя отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов на этом шаблоне.

4. Вместо текста **Заголовок отчета** введите имя отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять имя отчета, вы можете стереть текст **Заголовок отчета** и оставить этот раздел отчета пустым.

   Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.

5. Вместо текста **Описание отчета** введите описание отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять описание отчета, вы можете стереть текст **Описание отчета** и оставить этот раздел отчета пустым.

Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.

6. Используя конструктор отчета, добавьте один или несколько элементов отчета:
   - **Таблица**.
   - **Диаграмма**.
   - **Изображение**.
7. Если вы выбрали добавление изображения, откроется окно **Изображение**. Выполните следующие действия:
   a. Нажмите на кнопку **Загрузить**.
   b. Загрузите изображение. Например, вы можете загрузить логотип вашей организации.
   c. В списке справа от кнопки загрузки выберите выравнивание изображения на странице отчета: **По левому краю**, **По правому краю** или **По центру**.
   d. Нажмите на кнопку **Применить**.
8. Если вы выбрали добавление диаграммы, откроется окно **Диаграмма по свойствам обнаружений**. Выполните следующие действия:
   a. В поле **Имя** введите имя диаграммы. Например, **Топ 5 обнаружений по технологии**. Вы также можете оставить поле пустым.
   b. В списке **Источник данных** выберите свойство обнаружения, по которому вы хотите создать диаграмму. Например, **Технологии**.
   c. В поле **Количество секторов** укажите максимальное количество секторов диаграммы. При создании отчета программа выберет наиболее часто встречающиеся данные. Например, если вы указали 5 секторов и хотите создать диаграмму по технологии, программа покажет диаграмму по 5 технологиям, выполнившим наибольшее количество обнаружений. Технологии, выполнившие наименьшее количество обнаружений, не отобразятся на диаграмме.

      Нажмите на кнопку **Применить**.
9. Если вы выбрали добавление таблицы, откроется окно **Таблица обнаружений**. Выполните следующие действия:
   a. В поле **Доступные столбцы** двойным щелчком мыши выберите свойства обнаружений, которые вы хотите добавить в таблицу отчета.

      Выбранные свойства переместятся в поле **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.

      Например, если в поле **Выбранные столбцы** вы переместили свойства **Технологии, Обнаружено** и **Время создания**, в таблице созданного отчета отобразятся технологии, выполнившие обнаружения, список обнаруженных объектов и время создания обнаружений.
   b. Если вы хотите отфильтровать обнаружения по свойству **Состояние**, установите флажки рядом с теми состояниями обработки обнаружений пользователем, данные по которым вы хотите отображать в отчете.
   c. Если вы хотите отфильтровать обнаружения по свойству **Технологии**, установите флажки рядом с теми названиями модулей и компонентов программы, данные по которым вы хотите отображать в отчете.
   d. Если вы хотите отфильтровать обнаружения по свойству **Важность**, установите флажки рядом с теми степенями важности обнаружений, данные по которым вы хотите отображать в отчете.
   e. Если вы хотите отфильтровать обнаружения по статусу **Статус VIP**, в списке выберите **VIP**. В

отчете отобразятся только обнаружения со статусом VIP.

f. Нажмите на кнопку **Применить**.

10. Нажмите на кнопку **Сохранить** в правом верхнем углу окна.

Будет создан новый шаблон.

Создание отчета по шаблону

► *Чтобы создать отчет по шаблону, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Новый отчет**.

3. Выполните следующие действия:

   a. В раскрывающемся списке **Шаблон** выберите один из шаблонов для создания отчета.

   b. В блоке параметров **Период** выберите один из следующих вариантов:

   - **Прошедший час**, если вы хотите, чтобы отчет содержал информацию о работе программы за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы отчет содержал информацию о работе программы за предыдущий день.
   - **Прошедшие 7 дней**, если вы хотите, чтобы отчет содержал информацию о работе программы за предыдущую неделю.
   - **Прошедшие 30 дней**, если вы хотите, чтобы отчет содержал информацию о работе системы за предыдущий месяц.
   - **Пользовательский**, если вы хотите, чтобы отчет содержал информацию о работе системы за указанный вами период.

4. Если вы выбрали период отображения информации о работе программы **Пользовательский**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода, за который будет создан отчет.

   b. Нажмите на кнопку **Применить**.

5. Если вы используете режим распределенного решения и multitenacy, в блоке параметров **Серверы** установите флажки напротив тех организаций и серверов, данные по которым вы хотите отображать в отчете.

6. Нажмите на кнопку **Создать**.

Созданный отчет отобразится в таблице отчетов. Вы можете загрузить отчет для просмотра (стр. 352) на вашем компьютере.

Просмотр таблицы шаблонов и отчетов

Шаблоны и отчеты отображаются в разделе **Отчеты** окна веб-интерфейса программы.

В подразделе **Созданные отчеты** отображается таблица отчетов. Таблица содержит следующую информацию:

- **Время создания** – дата и время создания отчета.
- **Имя отчета** – имя отчета, созданного по шаблону.
- **Серверы** – имя сервера с компонентом Central Node, на котором создан отчет (если вы используете режим распределенного решения и multitenancy).
- **Период** – период, за который создан отчет.
- **Автор** – имя пользователя, создавшего отчет.

В подразделе **Шаблоны** отображается таблица шаблонов. Таблица содержит следующую информацию:

- **Время создания** – дата и время создания шаблона.
- **Время обновления** – дата и время последнего изменения шаблона.
- **Имя отчета** – имя шаблона.
- **Автор** – имя пользователя, создавшего шаблон.

Просмотр отчета

► *Чтобы просмотреть отчет, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. Выберите отчет, который вы хотите просмотреть.

Отчет откроется в новой вкладке вашего браузера.

Скачивание отчета на локальный компьютер

► *Чтобы скачать отчет на ваш компьютер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. В строке с отчетом, который вы хотите просмотреть, нажмите на значок  .

   Отчет будет сохранен в формате HTML на ваш локальный компьютер в папку загрузки браузера.

   Для просмотра отчета вы можете использовать любую программу для просмотра HTML-файлов (например, браузер).

Изменение шаблона

► *Чтобы изменить шаблон, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Выберите шаблон, который вы хотите изменить.

   Откроется окно изменения шаблона.

3. Вы можете изменить следующие параметры:

   - **Имя отчета** – имя отчета, которое отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов по этому шаблону.
   - **Заголовок отчета** – имя отчета, которое отобразится в отчете после создания отчета.

     Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
   - **Описание отчета** – описание отчета, которое отобразится в отчете после создания отчета.

     Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
   - **Изображение**. Вы можете загрузить или удалить изображение.
   - **Диаграмма**. Вы можете изменить следующие параметры диаграммы:
     - **Имя**.
     - **Источник данных**.
     - **Количество секторов**.

     Нажмите на кнопку **Применить**.
   - **Таблица**. Вы можете изменить следующие параметры таблицы:
     - **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.
     - **Состояние**.
     - **Технологии**.
     - **Важность**.
     - **Статус VIP**.

4. Выберите один из следующих способов сохранения шаблона:

   - Если вы хотите применить изменения к текущему шаблону, нажмите на кнопку **Сохранить**.

     Шаблон будет изменен.
   - Если вы хотите создать новый шаблон, введите имя и нажмите на кнопку **Сохранить как**.

     > Имя нового шаблона не должно совпадать с именем уже существующего шаблона.

     Новый шаблон будет сохранен.

Фильтрация шаблонов по имени

► *Чтобы отфильтровать шаблоны по имени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. По ссылке **Имя отчета** откройте меню фильтрации шаблонов.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени шаблона.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по имени пользователя, создавшего шаблон

► *Чтобы отфильтровать шаблоны по имени пользователя, создавшего шаблон, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.
2. По ссылке **Автор** откройте меню фильтрации шаблонов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации шаблонов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Фильтрация шаблонов по времени создания

► *Чтобы отфильтровать шаблоны отчетов по времени создания, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.
2. По ссылке **Время создания** откройте меню фильтрации шаблонов.
3. Выберите один из следующих периодов отображения шаблонов:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все созданные шаблоны.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные

за предыдущий час.

- **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные за предыдущий день.
- **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице шаблоны, созданные за указанный вами период.

4. Если вы выбрали период отображения шаблонов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения шаблонов.
   b. Нажмите на кнопку **Применить**.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Сброс фильтра шаблонов

► *Чтобы сбросить фильтр шаблонов по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Нажмите на кнопку справа от того заголовка графы таблицы шаблонов, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице шаблонов отобразятся только шаблоны, соответствующие заданным вами условиям.

Удаление шаблона

► *Чтобы удалить шаблон, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Установите флажок в строке с шаблоном, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранный вами шаблон будет удален.

Фильтрация отчетов по времени создания

► *Чтобы отфильтровать отчеты по времени их создания, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Время создания** откройте меню фильтрации отчетов.
3. Выберите один из следующих периодов отображения отчетов:
   - **Все**, если вы хотите, чтобы программа отображала в таблице все созданные отчеты.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице отчеты, созданные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице отчеты, созданные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице отчеты, созданные за указанный вами период.
4. Если вы выбрали период отображения отчетов **Пользовательский диапазон**, выполните следующие действия:
   a. В открывшемся календаре укажите даты начала и конца периода отображения отчетов.
   b. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени

► *Чтобы отфильтровать отчеты по имени, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Имя отчета** откройте меню фильтрации отчетов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:
   - **Содержит**.
   - **Не содержит**.
4. В поле ввода укажите один или несколько символов имени отчета.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени сервера с компонентом Central Node

► *Чтобы отфильтровать отчеты по имени сервера с компонентом Central Node, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Серверы** откройте меню фильтрации отчетов.
3. Установите флажки напротив тех серверов, по которым вы хотите отфильтровать отчеты.
4. Нажмите на кнопку **Применить**.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Фильтрация отчетов по имени пользователя, создавшего отчет

► *Чтобы отфильтровать отчеты по имени пользователя, создавшего отчет, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. По ссылке **Автор** откройте меню фильтрации отчетов.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации отчетов:
   - **Содержит**.
   - **Не содержит**.
4. Введите один или несколько символов имени пользователя.
5. Если вы хотите добавить условие фильтрации в фильтр, нажмите на кнопку  под списком операторов фильтрации и повторите действия по вводу условий фильтрации.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Сброс фильтра отчетов

► *Чтобы сбросить фильтр отчетов по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. Нажмите на кнопку справа от того заголовка графы таблицы отчетов, условия фильтрации по которому вы хотите сбросить.

Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отчетов отобразятся только отчеты, соответствующие заданным вами условиям.

Удаление отчета

► *Чтобы удалить отчет о работе программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.
2. Установите флажок в строке с отчетом, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

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

Выбранный отчет будет удален.

Отправка уведомлений

Вы можете настроить отправку уведомлений на один или несколько адресов электронной почты.

В программе доступны уведомления об обнаружениях и о проблемах в работе программы.

Просмотр таблицы правил для отправки уведомлений

Правила для отправки уведомлений отображаются в разделе **Параметры**, подразделе **Отправка уведомлений** окна веб-интерфейса программы.

Таблица правил для отправки уведомлений содержит следующую информацию:

-  – тип правила для отправки уведомлений.

  Возможны следующие типы правил:

  -  – правило для отправки уведомления об обнаружениях;
  -  – правило для отправки уведомления о работе компонентов программы.
- **Тема** – тема сообщения с уведомлением.
- **Кому** – адреса электронной почты, на которые отправляются уведомления.
- **Состояние** – состояние правила для отправки уведомления.

Создание правила для отправки уведомлений об обнаружениях

► *Чтобы создать правило для отправки уведомлений об обнаружениях, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило отправки уведомлений**.
3. В поле **Кому** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.

   Вы можете ввести несколько адресов электронной почты через запятую.
4. В поле **Тема** введите тему сообщения с уведомлением.
5. Если вы хотите, чтобы программа подставляла важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.
6. В поле **Тип уведомления** выберите **Обнаружения**.
7. В раскрывающемся списке **Важность обнаружения** выберите минимальное значение важности обнаружений, о которых вы хотите настроить отправку уведомлений.

   Например, вы можете настроить отправку уведомлений об обнаружениях только высокой степени важности или только средней и высокой степени важности.

8. В поле **Адрес источника или назначения** введите IP-адрес и маску сети, если вы хотите настроить отправку уведомлений об обнаружениях, связанных с определенным IP-адресом или адресом подсети источника или назначения.
9. В поле **Email** введите адрес электронной почты, если вы хотите настроить отправку уведомлений об обнаружениях, связанных с определенным адресом отправителя или получателя сообщений электронной почты.
10. В блоке параметров **Компоненты** установите флажки рядом с названиями одной или нескольких технологий, если вы хотите настроить отправку уведомлений об обнаружениях, выполненных определенными технологиями.
11. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений об обнаружениях будет добавлено в список правил.

Создание правила для отправки уведомлений о работе компонентов программы

► *Чтобы создать правило для отправки уведомлений о работе компонентов программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило отправки уведомлений**.
3. В поле **Кому** введите один или несколько адресов электронной почты, на которые вы хотите настроить отправку уведомлений.

   Вы можете ввести несколько адресов электронной почты через запятую.
4. В поле **Тема** введите тему сообщения с уведомлением.
5. Если вы хотите, чтобы программа подставляла важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.
6. В поле **Тип уведомления** выберите **Работа программы**.
7. В блоке параметров **Компоненты** установите флажки рядом с названиями тех функциональных областей программы, о которых вы хотите получать уведомления.
8. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений о работе компонентов программы будет добавлено в список правил.

Включение и отключение правила для отправки уведомлений

► *Чтобы включить или отключить правило для отправки уведомлений об обнаружениях, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. В строке с правилом для отправки уведомлений, которое вы хотите включить или отключить, в графе

Состояние выполните одно из следующих действий:

- Включите переключатель, если вы хотите включить правило.
- Выключите переключатель, если вы хотите отключить правило.

Состояние правила для отправки уведомлений об обнаружениях будет изменено.

Изменение правила для отправки уведомлений

► *Чтобы изменить правило для отправки уведомлений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. В списке правил для отправки уведомлений выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило отправки уведомлений**.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Сохранить**.

Правило для отправки уведомлений будет изменено.

Удаление правила для отправки уведомлений

► *Чтобы удалить правило для отправки уведомлений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. Установите флажок слева от названия каждого правила, которое вы хотите удалить.

   Если вы хотите удалить все правила, установите флажок над списком.
3. Нажмите на кнопку **Удалить** в нижней части окна.
4. В окне подтверждения нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Фильтрация и поиск правил отправки уведомлений по типу правила

► *Чтобы отфильтровать или найти правила отправки уведомлений по типу правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. В таблице правил для отправки уведомлений нажмите на значок  .

   Откроется окно настройки фильтрации.
3. Выберите один из следующих вариантов:

- **Все**.
- **Обнаружения**.
- **Работа программы**.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по теме уведомлений

► *Чтобы отфильтровать или найти правила отправки уведомлений по теме уведомлений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. По ссылке **Тема** откройте окно настройки фильтрации.
3. Введите один или несколько символов темы уведомлений.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по адресу электронной почты

► *Чтобы отфильтровать или найти правила отправки уведомлений по адресу электронной почты, на который они отправляются, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. По ссылке **Кому** откройте окно настройки фильтрации.
3. Введите один или несколько символов адреса электронной почты.
4. Нажмите на кнопку **Применить**.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск правил отправки уведомлений по их состоянию

► *Чтобы отфильтровать или найти правила отправки уведомлений по их состоянию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. По ссылке **Состояние** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом со значениями состояний:
   - **Включено**.
   - **Отключено**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил отправки уведомлений

► *Чтобы сбросить фильтр правил отправки уведомлений по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Отправка уведомлений**.
2. Нажмите на кнопку справа от того заголовка графы таблицы правил отправки уведомлений, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице правил отправки уведомлений отобразятся только правила, соответствующие заданным вами условиям.

Работа с правилами присвоения обнаружениям статуса VIP

Вы можете создавать, импортировать и экспортировать список правил присвоения обнаружениям статуса VIP. Обнаружения со статусом VIP доступны только пользователям с ролью **Старший сотрудник службы безопасности**.

Вы можете создавать правила одного из следующих типов:

- **IP**. Новым обнаружениям, связанным с этим IP-адресом компьютера, будет присвоен статус VIP.
- **Имя хоста**. Новым обнаружениям, связанным с этим именем хоста, будет присвоен статус VIP.
- **Email**. Новым обнаружениям, связанным с этим адресом электронной почты, будет присвоен статус VIP.

Добавление правила присвоения статуса VIP

► *Чтобы добавить правило присвоения обнаружениям статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Добавить**.

   Откроется окно добавления правила.
3. В раскрывающемся списке **Тип правила** выберите один из следующих типов правила:
   - **IP**, если вы хотите добавить правило для IP-адреса компьютера.
   - **Имя хоста**, если вы хотите добавить правило для имени хоста.
   - **Email**, если вы хотите добавить правило для адреса электронной почты.
4. В поле **Значение** введите нужное значение.

   Например, если в списке **Тип правила** вы выбрали **Email**, в поле **Значение** введите адрес электронной почты, для которого вы хотите добавить правило.
5. В поле **Описание** введите дополнительную информацию, если необходимо.
6. Нажмите на кнопку **Добавить**.

Правило будет добавлено. Новым обнаружениям, связанным с добавленным IP-адресом, именем хоста или адресом электронной почты, будет присвоен статус VIP.

Удаление правила присвоения статуса VIP

► *Чтобы удалить правило присвоения обнаружениям статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Установите флажок слева от каждого правила, которое вы хотите удалить из списка.
3. Если вы хотите удалить все правила, установите флажок над списком.

4. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Изменение правила присвоения статуса VIP

► *Чтобы изменить правило присвоения обнаружениям статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Выберите правило, которое вы хотите изменить.

   Откроется окно изменения правила.

3. Внесите необходимые изменения в поля **Тип правила**, **Значение**, **Описание**.
4. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Импорт списка правил присвоения статуса VIP

► *Чтобы импортировать список правил присвоения обнаружениям статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Нажмите на кнопку **Импортировать**.

   Отобразится подтверждение импорта списка.

   Импортированный список правил присвоения обнаружениям статуса VIP заменит текущий список правил присвоения обнаружениям статуса VIP.

3. Нажмите на кнопку **Да**.

   Откроется окно выбора файлов.

4. Выберите файл формата JSON со списком правил, которые вы хотите импортировать, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Список будет импортирован.

Экспорт списка правил присвоения статуса VIP

► *Чтобы экспортировать список правил присвоения статуса VIP, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Экспортировать**.

Список правил присвоения статуса VIP будет экспортирован в файл формата JSON.

Фильтрация и поиск по типу правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по типу правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Тип правила** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом с типами правил:
   - **IP**.
   - **Имя хоста**.
   - **Email**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по значению правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по значению правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Значение** откройте окно настройки фильтрации.
3. Введите один или несколько символов значения правила.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по описанию правила присвоения статуса VIP

► *Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по описанию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Описание** откройте окно настройки фильтрации.
3. Введите один или несколько символов описания.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил присвоения статуса VIP

► *Чтобы сбросить фильтр правил присвоения обнаружениям статуса VIP по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Нажмите на кнопку справа от того заголовка графы таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным вами условиям.

Работа с YARA-правилами

В качестве баз модуля YARA используются файлы YARA-правил.

Вы можете создавать свои YARA-правила и добавлять файл YARA-правил в Kaspersky Anti Targeted Attack Platform через веб-интерфейс программы.

Подробнее о создании и обновлении YARA-правил версии 3.7.0 и выше см. в документации YARA-правил или

на веб-сайте http://yararules.com/.

Загрузка YARA-правил

► *Чтобы загрузить YARA-правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **YARA-правила**.
2. Нажмите на кнопку **Загрузить**.

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

   Окно выбора файлов закроется.

Отобразится следующая информация о загруженных YARA-правилах:

- **Размер файла** – размер файла YARA-правил.
- **Время загрузки** – дата и время последней загрузки файла YARA-правил.

Обновление YARA-правил

► *Чтобы обновить YARA-правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **YARA-правила**.
2. Нажмите на кнопку **Заменить**.

   Откроется окно выбора файлов.
3. Выберите файл YARA-правил, которым вы хотите заменить текущий файл, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Загруженный файл YARA-правил заменит предыдущий файл.

Удаление YARA-правил

► *Чтобы удалить YARA-правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **YARA-правила**.
2. Нажмите на кнопку **Удалить**.

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

YARA-правила будут удалены.

Работа с белым списком

Вы можете создавать, импортировать и экспортировать *белый список* – список данных, которые Kaspersky Anti Targeted Attack Platform будет считать безопасными и не будет отображать в таблице обнаружений (стр. 238). Вы можете включать следующие данные в белый список:

- **MD5**.
- **Формат**.
- **Маска URL**.
- **Email**.
- **Маска подсети**.
- **User Agent**.

Добавление записи в белый список

► *Чтобы добавить запись в белый список, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белый список**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
3. В раскрывающемся списке **Тип правила** выберите один из следующих критериев добавления записи в белый список:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Email**.
   - **Маска подсети**.
   - **User Agent**.
4. Если вы выбрали **Формат**, в раскрывающемся списке **Значение** выберите формат файла, который вы хотите добавить.

   Например, вы можете выбрать формат **MSOfficeDoc**.
5. Если вы выбрали **MD5**, **Маска URL**, **Email**, **User Agent** или **Маска подсети**, в поле **Значение** введите значение соответствующего критерия, которое вы хотите добавить в белый список:
   - Если вы выбрали **MD5**, в поле **Значение** введите MD5-хеш файла.
   - Если вы выбрали **Маска URL**, в поле **Значение** введите маску URL-адреса.

     При формировании маски вы можете использовать следующие специальные символы:

     * – любая последовательность символов.

Пример:

Если вы введете маску `*abc*`, программа будет считать безопасным любой URL-адрес, содержащий последовательность `abc`. Например, `www.example.com/download_virusabc`

? – любой один символ.

Пример:

Если вы введете маску `example_123?.com`, программа будет считать безопасным любой URL-адрес, содержащий заданную последовательность символов и любой символ, следующий за `3`. Например, `example_1234.com`

В случае, если символы `*` и `?` входят в состав полного URL-адреса, добавляемого в белый список, необходимо при вводе этого адреса использовать символ `\` – отмена одного из следующих за ним символов `*` или `?`, `\`.

Пример:

В качестве доверенного адреса необходимо добавить следующий URL-адрес:
`www.example.com/download_virus/virus.dll?virus_name=`

Чтобы программа не восприняла `?` как специальный символ формирования маски, нужно поставить перед `?` знак `\`.

URL-адрес, добавляемый в белый список, будет выглядеть следующим образом:
`www.example.com/download_virus/virus.dll\?virus_name=`

- Если вы выбрали **Email**, в поле **Значение** введите адрес электронной почты.
- Если вы выбрали **User Agent**, в поле **Значение** введите заголовок User agent HTTP-запросов, содержащий информацию о браузере.
- Если вы выбрали **Маска подсети**, в поле **Значение** введите маску подсети. Например, 255.255.255.0

В полях **Маска URL** и **Email** Вы можете указывать доменные имена, содержащие символы кириллицы. В этом случае указанный адрес будет преобразован в Punycode и обработан в соответствии с параметрами программы.

6. Нажмите на кнопку **Добавить**.

Запись будет добавлена в белый список.

Удаление записи из белого списка

► *Чтобы удалить одну или несколько записей из белого списка, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белый список**.
2. Установите флажок слева от каждой записи, которую вы хотите удалить из белого списка.

Если вы хотите удалить все записи, установите флажок над списком.

3. В правом верхнем углу окна нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные записи будут удалены из белого списка.

Изменение записи в белом списке

► *Чтобы изменить запись в белом списке, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белый список**.
2. Выберите запись, которую вы хотите изменить.

   Откроется окно **Изменить правило**.

3. Внесите необходимые изменения в поля **Тип правила** и **Значение**.
4. Нажмите на кнопку **Сохранить**.

   Запись будет изменена.

Импорт белого списка

Импортированный белый список заменит текущий белый список.

► *Чтобы импортировать белый список, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белый список**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Импортировать**.

   Отобразится окно подтверждения действия.

3. Нажмите на кнопку **Да**.

   Откроется окно выбора файлов.

4. Выберите файл формата JSON с белым списком, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Белый список будет импортирован. Импортированный белый список заменит текущий белый список.

Экспорт белого списка

► *Чтобы экспортировать белый список, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белый список**.

2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Экспортировать**.

Файл в формате JSON с экспортированным белым списком будет сохранен в папку загрузки браузера на вашем компьютере.

Фильтрация и поиск записей в белом списке по типу правила

► *Чтобы отфильтровать или найти записи в белом списке по типу правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белый список**.
2. По ссылке **Тип правила** откройте окно настройки фильтрации.
3. Установите один или несколько флажков рядом с типами правил, по которым вы хотите отфильтровать записи:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Email**.
   - **Маска подсети**.
   - **User Agent**.
4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В белом списке отобразятся только записи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск записей в белом списке по значению правил

► *Чтобы отфильтровать или найти записи в белом списке по значению правил, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белый список**.
2. По ссылке **Значение** откройте окно настройки фильтрации.
3. Введите один или несколько символов значения.
4. Нажмите на кнопку **Применить**.

В белом списке отобразятся только записи, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра записей в белом списке

► *Чтобы сбросить фильтр записей в белом списке по одному или нескольким условиям фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Белый список**.
2. Нажмите на кнопку справа от того заголовка графы таблицы записей в белом списке, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В белом списке отобразятся только записи, соответствующие заданным вами условиям.

Создание списка паролей для архивов

Программа не проверяет архивы, защищенные паролем. Вы можете создать список наиболее часто встречающихся паролей для архивов, которые используются при обмене файлами в вашей организации. В этом случае при проверке архива программа будет проверять пароли из списка. Если какой-либо из паролей подойдет, архив будет разблокирован и проверен.

Список паролей, заданный в параметрах программы, также передается на сервер с компонентом Sandbox.

► *Чтобы создать список паролей для архивов, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пароли к архивам**.
2. В поле **Пароли к архивам** введите пароли, которые программа будет использовать для архивов, защищенных паролем.

   Вводите каждый пароль с новой строки. Вы можете ввести до 50 паролей.
3. Нажмите на кнопку **Применить**.

Список паролей для архивов будет создан. При проверке файлов формата PDF, а также файлов программ Microsoft Word, Excel, PowerPoint, защищенных паролем, программа будет подбирать пароли из заданного списка.

Создание резервной копии и восстановление программы

Вы можете создать резервную копию Kaspersky Anti Targeted Attack Platform, а затем восстановить программу из резервной копии.

Если вы не используете режим распределенного решения и multitenancy и используете отдельный сервер Central Node, вы можете создать резервную копию данных этого сервера Central Node.

Если вы используете режим распределенного решения и multitenancy, вы можете:

1. Создать резервную копию данных PCN.
2. Создать резервную копию данных SCN. При восстановлении данных из резервной копии SCN роль сервера изменится с SCN на отдельный сервер Central Node.

Выполняйте действия по созданию резервной копии программы на том сервере, резервную копию данных которого вы хотите создать.

В Kaspersky Anti Targeted Attack Platform могут содержаться данные пользователей и другая конфиденциальная информация. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность этих данных самостоятельно при создании резервной копии программы, замене оборудования, на которое установлена программа, и в прочих случаях, когда может потребоваться удаление данных без возможности восстановления. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за доступ к данным, хранящимся на серверах программы.

Вы можете создать резервную копию следующих данных:

- Базы данных программы (базы обнаружений, задач, политик, наличия у обнаружений статуса VIP, белых списков, уведомлений).
- Карантина.
- Базы обнаружений, выполненных при повторной проверке (rescan).
- Артефактов Sandbox.
- Параметров Central Node или PCN:
  - Если вы используете отдельный сервер Central Node, создается резервная копия параметров Central Node.
  - Если вы используете режим распределенного решения и multitenancy и работаете на сервере PCN, создается резервная копия параметров PCN.
  - Если вы используете режим распределенного решения и multitenancy и работаете на сервере SCN, вы можете создать резервную копию SCN, но при восстановлении данных из резервной копии роль сервера изменится с SCN на отдельный сервер Central Node.

Вы можете очистить директорию перед созданием резервной копии программы.

Перед восстановлением программы из резервной копии на сервере Central Node или PCN, на котором вы выполняете восстановление программы, происходит очистка:

- Базы данных программы (базы обнаружений, задач, политик, наличия у обнаружений статуса VIP, белых списков, уведомлений).
- Карантина.
- Базы обнаружений, выполненных при повторной проверке (rescan).
- Артефактов Sandbox.
- Параметров Central Node или PCN.

Таблица 18. Состав и объем данных, экспортируемых для создания резервной копии программы

Максимальный объем данных	Тип данных	Экспортируемые данные	Режим работы с программой
4 ГБ	Параметры Central Node Базы данных программы на Central Node (база обнаружений, задачи, политики, наличие у обнаружений статуса VIP, белые списки, уведомления).	Параметры Central Node – по выбору. Базы данных программы – по умолчанию.	Отдельный сервер Central Node.
4 ГБ	Параметры PCN.	По выбору.	Режим распределенного решения и multitenancy.
4 ГБ	Параметры PCN.	По выбору. Как для отдельного сервера Central Node.	Режим распределенного решения и multitenancy.
4 ГБ	Базы данных программы на PCN (база обнаружений, задачи, политики, наличие у обнаружений статуса VIP, белые списки, уведомления).	По умолчанию.	Режим распределенного решения и multitenancy.
300 ГБ	Карантин.	По выбору.	Все режимы.
300 ГБ	Артефакты Sandbox.	По выбору.	Все режимы.
300 ГБ	База обнаружений, выполненных при повторной проверке (rescan).	По выбору.	Все режимы.
Нет	База Targeted Attack Analyzer.	По умолчанию (данные HBase).	Все режимы.

Максимальный объем данных	Тип данных	Экспортируемые данные	Режим работы с программой
Нет	База событий.	Нет.	Все режимы.

Файлы, которые в момент создания резервной копии программы находились в очереди на проверку, не экспортируются.

Создание резервной копии программы из меню администратора программы

► *Чтобы создать резервную копию Kaspersky Anti Targeted Attack Platform, выполните следующие действия в меню администратора сервера (стр. 151):*

1. В списке разделов меню администратора программы выберите раздел **System administration**.
2. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
3. В списке действий выберите **Backup/Restore settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup/Restore settings**.
5. В списке действий выберите **New**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup settings**.
7. Нажмите на кнопку **Back up**.

Резервная копия Kaspersky Anti Targeted Attack Platform будет создана на сервере.

Загрузка файла с резервной копией программы с сервера Central Node или PCN на жесткий диск компьютера

Рекомендуется сохранять файлы с резервной копией программы на жесткий диск вашего компьютера.

► *Чтобы загрузить файл с резервной копией программы на жесткий диск вашего компьютера, выполните команду в интерфейсе командной строки операционной системы Linux на вашем компьютере:*

```
scp <имя учетной записи для работы в меню администратора и в консоли управления сервером>@<IP-адрес сервера>:<имя файла с резервной копией программы вида settings-<дата и время создания резервной копии>.tar.gz>
```

Пример:

Команда для загрузки на жесткий диск вашего компьютера архива с резервной копией программы, созданной на сервере Central Node с IP-адресом 10.0.0.10 под учетной записью admin 10 апреля 2019 года в 10 часов 00 минут 00 секунд:

```
scp admin@10.0.0.10:settings-20190410-100000.tar.gz
```

Файл с резервной копией программы будет сохранен на жесткий диск вашего компьютера в текущую директорию.

Загрузка файла с резервной копией программы с вашего компьютера на сервер Central Node

► *Чтобы загрузить файл с резервной копией программы с жесткого диска вашего компьютера на сервер, выполните следующую команду в режиме Technical Support Mode:*

```
scp <имя файла с резервной копией программы вида settings-<дата и время создания резервной копии>.tar.gz> <имя учетной записи для работы в меню администратора и в консоли управления сервером>@<IP-адрес сервера>:
```

Пример:

Команда для загрузки архива с резервной копией программы, созданной 10 апреля 2019 года в 10 часов 00 минут 00 секунд, на сервер Central Node с IP-адресом 10.0.0.10 под учетной записью admin:

```
scp settings-20190410-100000.tar.gz admin@10.0.0.10:
```

Файл с резервной копией программы будет загружен на сервер Central Node в текущую директорию.

Восстановление программы из резервной копии через меню администратора программы

Для восстановления Kaspersky Anti Targeted Attack Platform из резервной копии необходимо предварительно создать резервную копию текущего состояния программы (стр. 376) и загрузить ее на жесткий диск вашего компьютера. В случае сбоя при восстановлении программы или необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией программы.

► *Чтобы восстановить Kaspersky Anti Targeted Attack Platform из уже созданной ранее резервной копии, выполните следующие действия в меню администратора (стр. 151) сервера:*

1. В списке разделов меню администратора программы выберите раздел **System administration**.
2. Нажмите на клавишу **ENTER**.

Откроется окно выбора действий.

3. В списке действий выберите **Backup/Restore settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup/Restore settings**.
5. В списке файлов с резервными копиями программы выберите файл, из которого вы хотите восстановить программу.

   Если нужного файла нет в списке, вам необходимо загрузить файл с резервной копией программы на сервер.
6. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
7. В списке действий выберите **Restore <имя файла с резервной копией программы>**.
8. Нажмите на клавишу **ENTER**.

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

Kaspersky Anti Targeted Attack Platform будет восстановлена из файла с резервной копией программы.

Создание резервной копии программы в режиме Technical Support Mode

► *Чтобы создать резервную копию Kaspersky Anti Targeted Attack Platform, выполните следующую команду в режиме Technical Support Mode (стр. 152) сервера:*

```
/opt/kaspersky/apt-base/bin/ie_kata.sh
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Таблица 19. Параметры команды для создания резервной копии Kaspersky Anti Targeted Attack Platform

Обязательный параметр	Параметр	Описание
Да	`-b <path>`	Создать файл с резервной копией программы по указанному пути, где <path> – абсолютный или относительный путь к директории, в которой создается файл с резервной копией программы.
Нет	`-q`	Сохранить файлы в Карантине.
Нет	`-a`	Сохранить файлы, ожидающие повторной проверки (rescan).
Нет	`-s`	Сохранить артефакты Sandbox.
Нет	`-n`	Сохранить параметры Central Node или PCN.

Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Если дополнительные параметры не указаны, резервная копия Kaspersky Anti Targeted Attack Platform будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, белые списки, уведомления).

Все файлы с резервной копией программы сохраняются в один TAR-архив. Имя файла архива: data_kata_ddmmyyyyhhMM, где ddmmyyyy – дата, hhMM – часы и минуты создания резервной копии программы. Имя базы данных резервной копии программы – KATA3.6.sql для резервной копии программы версии 3.6.

Пример:

Команда для создания резервной копии программы со всеми параметрами:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh -b <path> -q -a -s -n -l <filepath>
```

Восстановление программы из резервной копии в режиме Technical Support Mode

► *Чтобы восстановить Kaspersky Anti Targeted Attack Platform из резервной копии, выполните следующую команду в режиме Technical Support Mode (стр. 152) сервера:*

```
/opt/kaspersky/apt-base/bin/ie_kata.sh
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

Таблица 20. Параметры команды для восстановления Kaspersky Anti Targeted Attack Platform из резервной копии

Обязательный параметр	Параметр	Описание команды
Да	`-r <path>`	Восстановить данные из файла с резервной копией программы, где <path> – абсолютный или относительный путь к директории, в которой находится файл.

Нет	`-c <path>`	Очистить директорию до начала восстановления программы по указанному пути, где <path> – абсолютный или относительный путь к директории, в которой создается файл для обновления программы. Также после выполнения этой команды программа проверяет наличие свободного места на диске.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Пример:

Команда для восстановления программы из резервной копии со всеми параметрами:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh -r <path> - c <path> -l <filepath>
```

Обновление Kaspersky Anti Targeted Attack Platform

Вы можете обновить Kaspersky Anti Targeted Attack Platform с версии 3.5 до версии 3.6.

Вы также можете устанавливать пакеты обновлений программы, выпускаемые "Лабораторией Касперского".

Если вы не используете режим распределенного решения и multitenancy и используете отдельный сервер Central Node, вы можете обновить программу на сервере Central Node.

Если вы используете режим распределенного решения и multitenancy:

1. Вы можете обновить программу на сервере PCN. После обновления программы сервер PCN будет относиться к той же организации, к которой он относился до обновления.
2. Если вы хотите обновить программу на сервере SCN, перед обновлением измените роль сервера с SCN на отдельный сервер Central Node.

   Программа обновится на отдельном сервере Central Node.

   После обновления программы вы сможете назначить серверам роль SCN и выбрать организацию, к которой относится сервер SCN (стр. 48).
3. После обновления программы всем пользователям с ролью Администратор по умолчанию предоставляется доступ к веб-интерфейсу сервера PCN и всех серверов SCN.

   Если до обновления программы вы настраивали доступ каждого пользователя к веб-интерфейсам SCN индивидуально, вы можете настроить его повторно (стр. 158).

   После обновления всем пользователям с ролью Старший сотрудник службы безопасности и Сотрудник службы безопасности по умолчанию предоставляется доступ к веб-интерфейсу сервера PCN и всех серверов SCN.

   Если до обновления программы вы настраивали доступ каждого пользователя к веб-интерфейсам SCN индивидуально, вы можете настроить его повторно (стр. 158). Для этого выполните следующие действия в веб-интерфейсе сервера PCN:

   1. Добавьте необходимые организации. (стр. 50)
   2. Настройте доступ учетных записей пользователей с ролью Старший сотрудник службы безопасности и Сотрудник службы безопасности к этим организациям и серверам. (стр. 158)
   3. Удалите все SCN, временно отключенные от PCN него при обновлении (стр. 51).
   4. Повторно подключите к PCN все необходимые SCN (стр. 48).

      При этом программа предложит вам выбрать организацию для каждого сервера SCN.

   Доступ пользователей к веб-интерфейсам SCN будет настроен.

Выполняйте действия по обновлению программы на том сервере, на котором вы хотите обновить данные.

В Kaspersky Anti Targeted Attack Platform могут содержаться данные пользователей и другая конфиденциальная информация. Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность этих данных самостоятельно при обновлении программы и в прочих случаях, когда может потребоваться удаление данных без возможности восстановления. Администратор Kaspersky Anti Targeted Attack Platform несет ответственность за доступ к данным, хранящимся на серверах программы.

Таблица 21. Состав и объем данных, сохраняемых при обновлении программы с версии 3.5 до версии 3.6

Максимальный объем данных	Тип данных	Данные, сохраняемые при обновлении
4 ГБ	Параметры Central Node. Базы данных программы на Central Node (база обнаружений, задачи, политики, наличие у обнаружений статуса VIP, белые списки, уведомления).	Все данные, кроме: • параметров интеграции с сенсорами, • ключей, • схем расположения графиков в разделе **Мониторинг**.
4 ГБ	Параметры PCN.	Все данные, кроме: • параметров интеграции с сенсорами, • ключей, • схем расположения графиков в разделе **Мониторинг**.
4 ГБ	Базы данных программы на PCN (база обнаружений, задачи, политики, наличие у обнаружений статуса VIP, белые списки, уведомления).	Все данные.
300 ГБ	Карантин.	Все данные.
300 ГБ	Артефакты Sandbox.	Все данные.
300 ГБ	База обнаружений, выполненных при повторной проверке (rescan).	Все данные.
Нет	База Targeted Attack Analyzer.	Все данные.
Нет	База событий.	Нет.

Файлы, которые в момент обновления Kaspersky Anti Targeted Attack Platform до версии 3.6 находились в очереди на проверку, не сохраняются.

Обновление программы с версии 3.5 до версии 3.6

Перед обновлением программы с версии 3.5 до версии 3.6 рекомендуется предварительно создать резервную копию текущего состояния программы (стр. 376) и загрузить ее на жесткий диск вашего компьютера из меню администратора программы. В случае сбоя при обновлении программы или необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией программы.

► *Чтобы обновить программу с версии 3.5 до версии 3.6, выполните следующие действия на сервере Central Node:*

1. Запустите образ диска с компонентами Central Node и Sensor Kaspersky Anti Targeted Attack Platform версии 3.6. Образ диска входит в комплект поставки программы (стр. 22).

   Запустится мастер установки.

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

   Откроется окно начала установки программы.

3. Нажмите на кнопку **OK**.

   Откроется окно выбора языка для просмотра Лицензионного соглашения и Политики конфиденциальности.

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

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

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

5. Нажмите на клавишу **ENTER**.

   Откроется окно с текстом Лицензионного соглашения.

6. Ознакомьтесь с Лицензионным соглашением.

7. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept the terms**.

   Откроется окно с текстом Политики конфиденциальности.

8. Ознакомьтесь с Политикой конфиденциальности.

9. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **I accept the terms**.

   Откроется окно **Select device**.

10. В окне **Select device** в списке дисков выберите диск, на котором установлена программа версии 3.5.

11. Нажмите на клавишу **ENTER**.

    Откроется окно **Select action**.

12. В списке действий выберите **Upgrade**.

13. Нажмите на клавишу **ENTER**.

    Откроется окно с предупреждением о том, что на диске уже установлена программа версии 3.5 и что

вы можете обновить программу до новой версии.

14. Нажмите на кнопку **Upgrade**.

Kaspersky Anti Targeted Attack Platform версии 3.6 будет установлена на сервер Central Node. Сервер перезагрузится. Параметры программы, доступные для обновления программы с версии 3.5 до версии 3.6, будут применены.

После обновления программы необходимо заново добавить лицензионные ключи (стр. 90).

Установка пакетов обновления программы

Когда "Лаборатория Касперского" выпускает обновления программы, вы можете устанавливать пакеты обновлений программы.

Перед установкой пакетов обновления программы рекомендуется предварительно создать резервную копию текущего состояния программы (стр. 376) и загрузить ее на жесткий диск вашего компьютера из меню администратора программы. В случае сбоя при установке пакета обновления программы или необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией программы.

► *Чтобы загрузить архив с пакетом обновления программы на сервер с компонентом Central Node, выполните следующие действия:*

1. Войдите в консоль управления сервера с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

   Отобразится меню администратора программы.
3. В меню администратора программы выберите режим Technical Support Mode.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно подтверждения входа в режим Technical Support Mode.
5. Выберите **Yes** и нажмите на клавишу **ENTER**.
6. Выполните команду

   ```
   scp <имя пакета обновления программы>.ktgz <имя пользователя с правами администратора сервера Central Node>@<IP-адрес сервера с компонентом Central Node>
   ```

   Например, вы можете выполнить команду `apt-system-3.6.0-tr-patch-122.ktgz admin@10.10.10.1`

Вы можете перейти к установке пакета обновления программы.

► *Чтобы установить пакет обновления программы, выполните следующие действия:*

1. Войдите в консоль управления сервера с компонентом Central Node по протоколу SSH или через терминал.
2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

   Отобразится меню администратора программы.
3. В меню администратора программы выберите пункт **System administration**.
4. Нажмите на клавишу **ENTER**.

   Отобразится окно выбора действия.

5. Выберите **Install patch** и нажмите на клавишу **ENTER**.

   Отобразится окно со списком пакетов обновлений программы, доступных к установке.

6. Выберите пакет обновления программы, который вы хотите установить, и нажмите на клавишу **ENTER**.

   Отобразится окно выбора действия.

7. Выберите действие **Validate and install <имя пакета обновления программы>.ktgz** и нажмите на клавишу **ENTER**.

   Пакет обновления программы будет установлен. Потребуется перезагрузка сервера.

8. Выберите **Go back** и нажмите на клавишу **ENTER**.

   Отобразится меню администратора программы.

9. В меню администратора программы выберите пункт **Reboot the machine** и нажмите на клавишу **ENTER**.

   Сервер с компонентом Central Node перезагрузится.

Установка пакета обновления программы будет завершена.

Взаимодействие с внешними системами по API

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с внешними системами для проверки хранящихся в них файлов (стр. 388), а также для предоставления внешним системам доступа к информации обо всех обнаружениях программы (стр. 392).

Взаимодействие внешних систем с Kaspersky Anti Targeted Attack Platform осуществляется с помощью интерфейса API. Вызовы методов API доступны только для авторизованных внешних систем (стр. 387).

Сценарий взаимодействия внешней системы с Kaspersky Anti Targeted Attack Platform

Рекомендуется использовать следующий сценарий взаимодействия внешней системы с программой:

a. **Авторизация внешней системы**

Администратору необходимо создать запрос на интеграцию внешней системы (стр. 387) с программой. После этого администратор программы должен обработать запрос в веб-интерфейсе Kaspersky Anti Targeted Attack Platform (стр. 215).

b. **Вызов метода `POST` для запуска проверки (стр. 388)**

c. **Вызов метода `GET` для получения результатов проверки (стр. 389)**

Интерфейс API является асинхронным, то есть Kaspersky Anti Targeted Attack Platform выполняет проверку объектов не в момент обращения внешней системы, а в фоновом режиме. Поэтому для получения результатов проверки требуется периодически отправлять запрос от внешней системы с помощью метода `GET`. Рекомендуемая периодичность отправки запроса 1 раз в минуту.

Вы также можете настроить отправку уведомлений (стр. 359) об обнаруженных объектах в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

d. **Вызов метода `DELETE` для удаления результатов проверки (стр. 390)**

Вы можете удалить результаты проверки указанного объекта или всех объектов.

e. **Запрос информации обо всех обнаружениях Kaspersky Anti Targeted Attack Platform**

Вы можете получить информацию обо всех обнаружениях Kaspersky Anti Targeted Attack Platform, а не только о тех объектах, которые хранятся во внешней системе. При формировании запроса вы можете использовать фильтры для получения информации об объектах, удовлетворяющих заданным критериям.

Создание запроса на интеграцию внешней системы с Kaspersky Anti Targeted Attack Platform

Для начала работы с API внешняя система должна пройти авторизацию на сервере Kaspersky Anti Targeted Attack Platform. Для этого необходимо создать запрос на интеграцию.

► *Чтобы создать запрос на интеграцию внешней системы с Kaspersky Anti Targeted Attack*

Platform, выполните следующие действия:

1. Сгенерируйте уникальный идентификатор внешней системы для обращения к API.
2. Сгенерируйте сертификат сервера внешней системы.

   При замене сертификата необходимо повторно пройти авторизацию.

3. Вызовите любой метод с указанием идентификатора (`sensorId`).

Запрос на интеграцию внешней системы отобразится в веб-интерфейсе Kaspersky Anti Targeted Attack Platform (стр. 215). Обратитесь к администратору программы для обработки запроса.

API для проверки объектов внешних систем

Kaspersky Anti Targeted Attack Platform предоставляет HTTPS REST интерфейс проверки объектов, хранящихся во внешних системах.

Работа с кластером

Если внешняя система представляет собой несколько серверов, объединенных в кластер, рекомендуется использовать один идентификатор (`sensorId`) для всех серверов. В этом случае в веб-интерфейсе Kaspersky Anti Targeted Attack Platform будет отображаться один запрос на интеграцию (стр. 215) для всей системы. При необходимости разграничить получение результатов проверки по отдельным серверам вы можете назначить каждому серверу уникальный идентификатор экземпляра (`sensorInstanceId`).

Ограничения

В конфигурационном файле Kaspersky Anti Targeted Attack Platform установлены максимально допустимое количество запросов на проверку объектов от внешних систем и максимально допустимый размер проверяемого объекта.

Если превышено максимально допустимое количество одновременных запросов на проверку объектов, Kaspersky Anti Targeted Attack Platform перестает обрабатывать дальнейшие запросы до тех пор, пока количество запросов на проверку объектов не станет меньше максимально допустимого. До этого времени выдается код возврата 429. Необходимо повторить запрос на проверку позже.

Если превышен максимально допустимый размер объекта, Kaspersky Anti Targeted Attack Platform не проверяет этот объект. При вызове метода `POST` выдается код возврата 413. Вы можете узнать максимально допустимый размер объекта, просмотрев список фильтров с помощью метода `GET` (стр. 391).

Проверка объектов

Для проверки объектов используется метод `POST`.

Синтаксис

```
POST "<URL-адрес сервера с компонентом Central
Node>/sensors/<sensorId>/scans"
```

Пример

```
curl -X POST
"https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-5800
6b8f6056/scans?sensorInstanceId" -H "accept: application/json" -H
"Content-Type: multipart/form-data" -F "objectType=file" -F
"content=@sample.yaml;type=application/x-yaml" -F
"scanId=52e27edc-9aa8-4f37-8b5a-789d334e062a
```

Параметры

Параметр	Тип	Описание
`sensorId`	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensorInstanceId`	string	Уникальный идентификатор экземпляра внешней системы. Экземплярами внешней системы считаются также серверы, объединенные в кластер. Параметр не является обязательным.
`objectType`	string	Тип проверяемого объекта. Возможное значения параметра: `file`.
`content`	file	Содержимое проверяемого объекта.
`scanId`	string	Уникальный идентификатор проверки. Если этот параметр не указан, просмотр результатов проверки недоступен.

Возвращаемое значение

Код возврата	Описание
`200`	Проверка выполнена успешно.
`401`	Требуется авторизация.
`429`	Превышено количество запросов. Повторите запрос позднее.
`500`	Внутренняя ошибка сервера. Повторите запрос позднее.

Просмотр результатов проверки

Для просмотра результатов проверки используется метод `GET`.

Синтаксис

```
GET "<URL-адрес сервера с компонентом Central
Node>/sensors/<sensorId>/scans/state"
```

Пример

```
curl -X GET
"https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-5800
6b8f6056/scans/state?sensorInstanceId=instance1&state=detected,notdetected,er
ror,timeout" -H "accept: application/json"
```

Параметры

Параметр	Тип	Описание
`sensorId`	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensorInstanceId`	string	Уникальный идентификатор экземпляра внешней системы. Если этот параметр не указан, отображаются результаты проверки для всех экземпляров.
`state`	array (тип элементов string)	Статус проверки объекта. При указании этого параметра результаты проверки будут отфильтрованы по статусу. Указывайте несколько статусов через запятую. Возможны следующие значения параметра: • `detected`; • `notdetected`; • `processing`; • `error`.

Возвращаемое значение

Код возврата	Описание
`200`	Проверка выполнена успешно.
`204`	Нет содержимого.
`404`	Не найдены результаты проверки по указанному идентификатору.
`500`	Внутренняя ошибка сервера. Повторите запрос позднее.

Удаление результатов проверки

Для удаления результатов проверки используется метод `DELETE`.

Синтаксис

```
DELETE "<URL-адрес сервера с компонентом Central
Node>/sensors/<sensorId>/scans/<scanId>"
```

Пример

```
curl -X DELETE
"https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-5800
6b8f6056/scans/52e27edc-9aa8-4f37-8b5a-789d334e062a" -H "accept:
application/json"
```

Параметры

Параметр	Тип	Описание
sensorId	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
scanId	string	Уникальный идентификатор проверки. Если этот параметр не задан, будут удалены результаты проверки всех объектов.

Возвращаемое значение

Код возврата	Описание
200	Проверка выполнена успешно.
401	Требуется авторизация.
404	Не найдены результаты проверки по указанному идентификатору.
500	Внутренняя ошибка сервера. Повторите запрос позднее.

Просмотр фильтров

Для просмотра фильтров используется метод GET.

Синтаксис

```
GET "<URL-адрес сервера с компонентом Central
Node>/sensors/<sensorId>/scans/filters"
```

Пример

```
curl -X GET
"https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-5800
6b8f6056/scans/filters" -H "accept: application/json"
```

Параметры

Параметр	Тип	Описание
sensorId	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.

Возвращаемое значение

Код возврата	Описание
200	Проверка выполнена успешно.
401	Требуется авторизация.
500	Внутренняя ошибка сервера. Повторите запрос позднее.

API для получения внешними системами информации об обнаружениях программы

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для доступа внешних систем к информации обо всех обнаружениях программы, а не только о результатах проверки объектов, хранящихся в этих внешних системах.

Вы можете указать в параметрах запроса фильтры, чтобы получить информацию только о тех обнаружениях, которые удовлетворяют требуемым условиям.

При появлении новых обнаружений программа не отправляет информацию о них автоматически на основе предыдущих запросов. Для получения актуальной информации требуется отправить повторный запрос.

Особенности работы в распределенном решении

Если программа работает в режиме распределенного решения, то внешняя система может проходить процедуру авторизации только на сервере SCN. Авторизация на сервере PCN недоступна.

В таком случае внешняя система не может получить информацию обо всех обнаружениях, зарегистрированных в инфраструктуре, за одно обращение. Это ограничение связано с тем, что общая база данных, содержащая записи обо всех обнаружениях инфраструктуры, хранится на сервере PCN. Для получения информации обо всех обнаружениях внешней системе потребуется обращаться к каждому серверу SCN отдельно.

Запрос информации об обнаружениях

Для получения информации об обнаружениях программы используется метод GET.

Синтаксис

```
curl -X GET "<URL-адрес сервера с компонентом Central
Node>/sensors/<sensorId>/detects?<параметры>"
```

Пример

Пример:

```
curl -X GET
"https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-5
8006b8f6056/detects?detect_type=am,sb&limit=100&token=7b226f6666736574223a
20307d" -H "accept: application/json"
```

Параметры

Параметр	Тип	Описание
`sensorId`	String	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`detect_type`	Array	Технология, с помощью которой выполнено обнаружение. Возможно указать несколько технологий через запятую. Возможные значения: • `am` – Anti-Malware Engine; • `sb` – Sandbox; • `yara` – YARA; • `url_reputation` – URL Reputation; • `ids` – Intrusion Detection System; • `taa` – Targeted Attack Analyzer. Если параметр не указан, предоставляется информация обо всех обнаружениях.
`limit`	Integer	Количество объектов, информация о которых будет предоставлена в ответ на запрос. Допустимые значения: целые числа от 1 до 10000. По умолчанию установлено значение `1000`.
`token`	String	Идентификатор запроса. При указании этого параметра в повторном запросе не отображается информация об обнаружениях, полученная в предыдущих запросах. Это позволяет избежать дублирования информации об одних и тех же обнаружениях при повторных запросах. Если этот параметр не указан, предоставляется информация обо всех обнаружениях.

Возвращаемое значение

Код возврата	Описание
`200`	Операция выполнена успешно.
`400`	Ошибка ввода параметров.
`429`	Превышено количество запросов.
`401`	Требуется авторизация.
`500`	Внутренняя ошибка сервера. Повторите запрос позднее.

Состав передаваемых данных

Информация, передаваемая о каждом обнаружении, представлена в таблице ниже.

Таблица 22. Состав передаваемых данных об обнаружении

Параметр	Значение	Описание
`alertID`	Целочисленное значение.	Идентификатор обнаружения.
`eventTimeStamp`	Дата и время.	Время события.
`detectTimestamp`	Дата и время.	Время занесения информации об обнаружении в базу Kaspersky Anti Targeted Attack Platform.
`importance`	Одно из следующих значений: • `high`; • `medium`; • `low`.	Важность обнаружения.
`objectSource`	Одно из следующих значений: • `web`; • `mail`; • `endpoint`; • `external`; • `dns`.	Источник обнаруженного объекта.
`technology`	Одно из следующих значений: • `am` – Anti-Malware Engine; • `sb` – Sandbox; • `yara` – YARA; • `url_reputation` – URL Reputation; • `ids` – Intrusion Detection System; • `taa` – Targeted Attack Analyzer.	Технология, с помощью которой обнаружен объект.
`objectType`	Одно из следующих значений: • `file`. • `URL`. • `host` (для удаленных доменов или хостов).	Тип обнаруженного объекта.
`object`	Зависит от типа обнаруженного объекта.	Данные об обнаруженном объекте (стр. 395).

Параметр	Значение	Описание
detection	Зависит от технологии, с помощью которой обнаружен объект.	Данные о найденных угрозах (стр. 397).
details	Зависит от источника обнаруженного объекта.	Данные об окружении обнаруженных объектов (стр. 399).

Данные об обнаруженных объектах

Состав передаваемых данных об обнаруженных объектах в зависимости от типа объекта приведен в таблице ниже.

Таблица 23. Данные об обнаруженных объектах

	Параметр	Тип данных	Описание	Пример
file	processedObject.MD5	MD5	MD5-хеш файла или составного объекта, переданного на проверку.	1839a1e9621c58dadf782e131df3821f
	processedObject.SHA256	SHA256	SHA256-хеш файла или составного объекта, переданного на проверку.	7bbfc1d690079b0c591e146c4294305da1cee857e12db40f4318598fdb503a47
	processedObject.fileName	String	Имя файла или составного объекта, переданного на проверку.	EICAR-CURE.com
	processedObject.fileType	String	Тип файла или составного объекта, переданного на проверку.	GeneralTxt

	Параметр	Тип данных	Описание	Пример
	processedObject.fileSize	Integer	Размер файла или составного объекта, переданного на проверку, в байтах.	184
	detectedObject.MD5	MD5	MD5-хеш файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза.	1839a1e9621c58dadf782e131df3821f
	detectedObject.fileName	String	Имя файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза.	EICAR-CURE.com
	detectedObject.fileSize	Integer	Размер файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза, в байтах.	184
URL	detectedObject	String	URL-адрес обнаруженного объекта.	http://example.com/link

	Параметр	Тип данных	Описание	Пример
host	detectedObject	Array	Список доменов, к которым относятся обнаруженные объекты. • Для технологии TAA указывается только один домен. • Для технологии URL, а также для объектов с параметром objectSource=dns список может содержать несколько доменов.	example.org, example.net

Данные о найденных угрозах

Состав передаваемых данных о найденных угрозах в зависимости от технологии, с помощью которой выполнено обнаружение, приведен в таблице ниже.

Таблица 24. Данные о найденных угрозах

Технология	Параметр	Описание	Тип данных	Пример

Технология	Параметр	Описание	Тип данных	Пример
Одна из следующих технологий: • Anti-Malware Engine. • YARA. • Intrusion Detection System.	`detect`	Список найденных угроз.	Array	`HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic`
	`dataBaseVersion`	Версия баз, с помощью которых проверен файл.	Integer	`201811190706`
Sandbox	`detect`	Список найденных угроз.	Array	`HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic`
	`image`	Имя образа виртуальной машины, на которой был проверен файл.	String	`Win7`
	`dataBaseVersion`	Версия баз в следующем формате: `<версия баз программы, с помощью которых проверен файл> / <версия баз модуля IDS>`.	Integer	`201902031107/ 201811190706`

Технология	Параметр	Описание	Тип данных	Пример
URL Reputation	`detect`	Список категорий URL Reputation для обнаруженного объекта (для объектов типа `URL` или `host`).	Array	`Phishing host, Malicious host, Botnet C&C(Backdoor.Win32.Mokes)`
Targeted Attack Analyzer	`detect`	Название обнаружения модуля TAA.	Единственно возможное значение: `Suspicious remote host activity`	`Suspicious remote host activity`

Данные об окружении обнаруженных объектов

Состав передаваемых данных об окружении обнаруженных объектов в зависимости от источника объекта приведен в таблице ниже.

Таблица 25. Данные об окружении обнаруженных объектов

Источник объекта	Параметр	Описание	Тип данных	Пример
web	sourceIP	IP-адрес компьютера, установившего соединение.	IP address	192.0.2.0
	sourceHostname	Имя компьютера, установившего соединение.	String	example.com
	destinationIp	IP-адрес компьютера, с которым установлено соединение.	IP address	198.51.100.0
	destinationPort	Порт компьютера, с которым установлено соединение.	Integer	3128

Источник объекта	Параметр	Описание	Тип данных	Пример
	URL	URL-адрес интернет-ресурса, к которому выполнено обращение. Для обнаружений, выполненных технологией IDS, этот параметр отсутствует. Для обнаружений, выполненных технологией URL, этот параметр совпадает с параметром detectedObject.	String	https://example.com:443/
	method	Метод HTTP-запроса.	String	Connect
	referrer	URL-адрес, на который была выполнена переадресация.	String	https://example.com:443/

Источник объекта	Параметр	Описание	Тип данных	Пример
	agentString	Заголовок User agent из HTTP-запроса, содержащий название и версию клиентского приложения.	String	Mozilla/4.0
mail	mailFrom	Адрес электронной почты отправителя.	String	sender@example.com
	mailTo	Список адресов электронной почты получателей через запятую.	Array	recipient1@example.com, recipient2@example.com
	subject	Тема сообщения.	String	'You are the winner'
	messageId	ID сообщения электронной почты.	String	1745028736.156014.1542897410859.JavaMail.svc_jira_pool@hqconflapp2
• endpoint • external	hostName	Имя компьютера, на котором выполнено обнаружение.	String	computername.example.com

Источник объекта	Параметр	Описание	Тип данных	Пример
	IP	IP-адрес компьютера, на котором выполнено обнаружение.	IP address	198.51.100.0
dns	sourceIp	IP-адрес компьютера, инициировавшего соединение по протоколу DNS.	IP address	192.0.2.0
	destinationIp	IP-адрес компьютера, с которым установлено соединение по протоколу DNS (как правило, DNS-сервера).	IP address	198.51.100.0
	destinationPort	Порт компьютера, с которым установлено соединение по протоколу DNS (как правило, DNS-сервера).	Integer	3128

Источник объекта	Параметр	Описание	Тип данных	Пример
	dnsMessageType	Тип DNS-сообщения: • Request. • Response.	String	Request
	dnsRequestType	Один из следующих типов записи DNS-запроса: • A. • AAA. • CNAME. • MX.	String	MX
	domainToBeResolved	Имя домена из DNS-запроса.	String	example.com

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2b) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

Глоссарий

A

Advanced persistent threat (APT)

Сложная целевая атака на IT-инфраструктуру организации с одновременным использованием различных методов проникновения в сеть, закрепления в сети и получения регулярного доступа к конфиденциальным данным.

Anti-Malware Engine

Ядро программы. Выполняет проверку файлов и объектов на вирусы и другие программы, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.

B

Backdoor-программа

Программа, которую злоумышленники устанавливают на взломанном компьютере для того, чтобы повторно получать доступ к этому компьютеру.

C

Central Node

Компонент программы. Выполняет проверку данных, исследование поведения объектов, а также публикацию результатов исследования в веб-интерфейс программы.

CSRF-атака

Cross-Site Request Forgery (также "XSRF-атака"). Атака на пользователей веб-сайтов, использующая уязвимости HTTP-протокола. Атака позволяет производить действия от имени авторизованного пользователя уязвимого веб-сайта. Например, от имени авторизованного пользователя уязвимого веб-сайта злоумышленник может тайно отправлять запрос на сервер сторонней платежной системы для перевода денег на счет злоумышленника.

E

Endpoint Sensors

Компонент программы. Устанавливается на отдельные компьютеры, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft Windows. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

I

ICAP-данные

Данные, полученные по протоколу ICAP (Internet Content Adaptation Protocol). Протокол позволяет фильтровать и изменять данные HTTP-запросов и HTTP-ответов. Например, производить антивирусную проверку данных, блокировать спам, запрещать доступ к персональным ресурсам. В качестве ICAP-клиента обычно выступает прокси-сервер, который взаимодействует с ICAP-сервером, используя протокол ICAP. Kaspersky Anti Targeted Attack Platform получает данные с прокси-сервера вашей организации после их обработки на ICAP-сервере.

Intrusion Detection System

Модуль программы. Выполняет проверку интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации.

IOA

Indicator of Attack (индикатор атаки). Описание подозрительного поведения объектов в IT-инфраструктуре организации, которое может являться признаком целевой атаки на эту организацию.

IOA-правило

Один признак подозрительного поведения объекта в IT-инфраструктуре организации, при совпадении с которым Kaspersky Anti Targeted Attack Platform считает событие обнаружением. IOA-правило содержит описание признака атаки и рекомендации по противодействию.

IOC

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

Файл, содержащий набор индикаторов IOC, при совпадении с которыми Kaspersky Anti Targeted Attack Platform считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

K

Kaspersky Anti Targeted Attack Platform

Решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "*APT*").

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Secure Mail Gateway

Решение, предназначенное для защиты входящей и исходящей электронной почты от вредоносных объектов и спама, а также выполняющее контентную фильтрацию сообщений. Решение позволяет развернуть виртуальный почтовый шлюз и интегрировать его в существующую почтовую инфраструктуру организации. На виртуальном почтовом шлюзе предустановлена операционная система, почтовый сервер и антивирусная программа "Лаборатории Касперского".

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

KATA

Kaspersky Anti Targeted Attack. Функциональный блок программы Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту периметра IT-инфраструктуры предприятия.

KEDR

Kaspersky Endpoint Detection and Response. Функциональный блок программы Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту компьютеров локальной сети организации.

M

MITM-атака

Man in The Middle (человек посередине). Атака на IT-инфраструктуру организации, при которой злоумышленник перехватывает канал связи между двумя точками доступа, ретранслирует и при необходимости изменяет связь между этими точками доступа.

Multitenancy

Режим работы, при котором программа может использоваться для защиты инфраструктуры нескольких организаций одновременно.

N

NTP-сервер

Сервер точного времени, использующий протокол Network Time Protocol.

O

Open IOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе

XML и содержащий свыше 500 различных индикаторов компрометации.

S

Sandbox

Компонент программы. Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации.

Sensor

Компонент программы. Выполняет прием данных.

SIEM-система

Система Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

SPAN

Switch Port Analyzer. Технология зеркалирования трафика с одного порта на другой.

Syslog

Стандарт отправки и записи сообщений о происходящих в системе событиях, используемый на платформах UNIX™ и GNU/Linux.

T

Targeted Attack Analyzer

Модуль программы. Выполняет статистический анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации. Выполняет поиск признаков сетевой активности, на которую пользователю Kaspersky Anti Targeted Attack Platform рекомендуется обратить внимание, а также признаков целевых атак на IT-инфраструктуру организации.

TLS-шифрование

Шифрование соединения между двумя серверами, обеспечивающее защищенную передачу данных между серверами сети Интернет.

Y

YARA

Модуль программы. Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями Kaspersky Anti Targeted Attack Platform.

YARA-правила

Общедоступная классификация вредоносных программ, содержащая сигнатуры признаков целевых атак и вторжений в IT-инфраструктуру организации, по которым Kaspersky Anti Targeted Attack Platform производит проверку файлов и объектов.

A

Альтернативный поток данных

Потоки данных файловой системы NTFS (alternate data streams), предназначенные для размещения дополнительных атрибутов или информации к файлу.

Каждый файл в файловой системе NTFS представляет собой набор потоков (streams). В основном потоке находится содержимое файла. Остальные (альтернативные) потоки предназначены для размещения метаинформации. Потоки можно создавать, удалять, сохранять отдельно, переименовывать и даже запускать как процесс.

Альтернативные потоки могут использоваться злоумышленниками для скрытой передачи или получения данных с компьютера.

Атака "нулевого дня"

Атака на IT-инфраструктуру организации, использующая уязвимости "нулевого дня" в программном обеспечении, которые становятся известны злоумышленникам до момента выпуска производителем программного обеспечения обновления, содержащего исправления.

B

Вредоносные веб-адреса

Веб-адреса ресурсов, распространяющих вредоносное программное обеспечение.

Д

Дамп

Содержимое рабочей памяти процесса или всей оперативной памяти системы в определенный момент времени.

З

Зеркалированнный трафик

Копия трафика, перенаправляемая с одного порта коммутатора на другой порт этого же коммутатора (локальное зеркалирование) или на удаленный коммутатор (удаленное зеркалирование). Администратор сети может настроить, какую часть трафика зеркалировать для передачи в Kaspersky Anti Targeted Attack Platform.

Л

Лицензионное соглашение

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

Локальная репутационная база KPSN

База данных репутаций объектов (файлов или URL-адресов), которая хранится на сервере Kaspersky Private Security Network, а не на серверах Kaspersky Security Network. Управление локальными репутационными базами осуществляется администратором KPSN.

П

Пропускная способность канала связи

Наибольшая возможная в данном канале связи скорость передачи информации.

Р

Распределенное решение

Двухуровневая иерархия серверов с установленными компонентами Central Node, в которой выделяется главный сервер управления – *Primary Central Node (PCN)* и подчиненные серверы – *Secondary Central Node (SCN)*.

С

Сигнатура

Код в базах систем защиты информации, содержащий описание известных угроз.

Статус VIP

Статус обнаружений с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователям с ролью **Сотрудник службы безопасности**.

Т

Техника MITRE

База знаний MITRE ATT&CK https://attack.mitre.org/ (Adversarial Tactics, Techniques & Common Knowledge – Тактики, техники и общеизвестные знания о злоумышленниках) содержит описание поведения злоумышленников, основанное на анализе реальных атак. Представляет собой структурированный список известных техник злоумышленников в виде таблицы.

Трассировка

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

У

Угрозы нового поколения

Угрозы IT-инфраструктуре организации, способные перезаписывать, изменять, зашифровывать или искажать свои коды так, чтобы невозможно было обнаружить совпадение с сигнатурой в системе защиты информации.

Уязвимость "нулевого дня"

Уязвимость в программном обеспечении, обнаруженная злоумышленниками до момента выпуска производителем программного обеспечения обновления, содержащего исправленный код программы.

Ф

Фишинговые URL-адреса

URL-адреса ресурсов, занимающихся получением неправомерного доступа к конфиденциальным данным пользователей. Как правило, целью фишинга является кража различных финансовых данных.

Ц

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top

Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com

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.

AMD – товарный знак Advanced Micro Devices, Inc.

Apple и Safari – товарные знаки Apple Inc.

Citrix и XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

ESET и ESET NOD32 – товарные знаки или зарегистрированные товарные знаки ESET, spol. s r.o.

Android и Google Chrome – товарные знаки Google, Inc.

FusionCompute, FusionSphere и HUAWEI являются зарегистрированными товарными знаками Huawei Technologies Co., Ltd в Китае и других странах.

Intel 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.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Active Directory, Excel, Hyper-V, Power Point, Microsoft, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS – товарный знак компании Red Hat, Inc.

Red Hat Enterprise Linux – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

Trend Micro – товарный знак компании Trend Micro.

VMware ESXi и VMware vSphere – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.