kaspersky

Kaspersky Anti Targeted Attack Platform

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform

- Что нового
- О Kaspersky Threat Intelligence Portal
- Комплект поставки
- Аппаратные и программные требования
  - Требования к Kaspersky Endpoint Agent для Windows
  - Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform
  - Совместимость версий Kaspersky Endpoint Agent для Windows с программами EPP
  - Совместимость версий Kaspersky Endpoint Agent для Windows с другими программами
  - Требования к Kaspersky Endpoint Agent для Linux
  - Совместимость версий Kaspersky Endpoint Agent для Linux с версиями Kaspersky Anti Targeted Attack Platform
  - Совместимость версий Kaspersky Endpoint Agent для Linux с программами EPP
  - Совместимость версий Kaspersky Endpoint Agent для Linux с другими программами
  - Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform
- Ограничения текущей версии программы

О предоставлении данных

- Служебные данные программы
- Данные компонентов Central Node и Sensor
  - Данные трафика компонента Sensor
  - Данные в обнаружениях
  - Данные в событиях
  - Данные в отчетах
  - Данные об объектах в Хранилище и на карантине
- Данные компонента Sandbox
- Данные, пересылаемые между компонентами программы
- Данные в файлах трассировки программы
- Данные Kaspersky Endpoint Agent для Windows
  - Данные, получаемые от компонента Central Node
  - Данные в полях событий Windows Event Log программы Kaspersky Endpoint Agent
  - Данные в запросах Kaspersky Endpoint Agent для Windows к Kaspersky Anti Targeted Attack Platform
  - Служебные данные Kaspersky Endpoint Agent для Windows
  - Данные в файлах трассировки и дампов Kaspersky Endpoint Agent для Windows
  - Данные, отправляемые в "Лабораторию Касперского" при принятии условий Положения о KSN
  - Данные в обнаружениях и событиях
  - Данные в отчетах о выполнении задач
  - Данные о файлах, запрещенных к запуску
  - Данные, связанные с выполнением задач
- Данные Kaspersky Endpoint Agent для Linux
  - Данные в запросах Kaspersky Endpoint Agent для Linux к Kaspersky Anti Targeted Attack Platform
  - Служебные данные Kaspersky Endpoint Agent для Linux
  - Данные в файлах трассировки и дампов Kaspersky Endpoint Agent для Linux

Лицензирование программы
- О Лицензионном соглашении
- О лицензии
- О лицензионном сертификате
- О ключе
- О файле ключа
- Просмотр информации о лицензии и добавленных ключах
- Просмотр текста Лицензионного соглашения в веб-интерфейсе Central Node
- Просмотр текста Политики конфиденциальности в веб-интерфейсе Central Node
- Просмотр информации о стороннем коде, используемом в программе
- Просмотр текста Лицензионного соглашения в веб-интерфейсе Sandbox
- Просмотр текста Лицензионного соглашения на компьютере с Kaspersky Endpoint Agent
- Добавление ключа
- Замена ключа
- Удаление ключа
- Режимы работы программы в соответствии с лицензией

Архитектура программы
- Компонент Sensor
- Компонент Central Node
- Компонент Sandbox
- Компонент Kaspersky Endpoint Agent

Принцип работы программы

Распределенное решение и мультитенантность
- Сценарий перехода в режим распределенного решения и мультитенантности
- Изменения в параметрах программы при переходе в режим распределенного решения и мультитенантности
- Назначение серверу роли PCN
- Назначение серверу роли SCN
- Обработка запросов на подключение SCN к PCN
- Просмотр информации о тенантах, серверах PCN и SCN
- Добавление тенанта на сервере PCN
- Удаление тенанта на сервере PCN
- Изменение названия тенанта на сервере PCN
- Отключение SCN от PCN
- Изменения в параметрах программы при отключении SCN от PCN
- Вывод сервера SCN из эксплуатации

Руководство по масштабированию
- Типовые схемы развертывания и установки компонентов программы
  - Схема развертывания на два сервера
  - Схема развертывания на три сервера
  - Схема развертывания на четыре и более сервера
  - Схема развертывания функциональности KEDR с компонентом Sandbox
  - Схема развертывания функциональности KEDR без компонента Sandbox
- Калькулятор масштабирования
  - Расчеты для компонента Sensor
  - Расчеты для компонента Central Node
  - Расчеты для компонента Sandbox

Установка и первоначальная настройка программы
Подготовка к установке компонентов программы
Подготовка IT-инфраструктуры к установке компонентов программы
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для приема сообщений по протоколу POP3
Подготовка IT-инфраструктуры к интеграции с почтовым сервером для отправки сообщений по протоколу SMTP
Подготовка виртуальной машины к установке компонента Sandbox
Порядок установки и настройки компонентов программы
Установка компонента Sandbox
Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 2. Выбор диска для установки компонента Sandbox
Шаг 3. Назначение имени хоста
Шаг 4. Выбор управляющего сетевого интерфейса в списке
Шаг 5. Назначение адреса и маски сети управляющего интерфейса
Шаг 6. Добавление адресов DNS-серверов
Шаг 7. Настройка статического сетевого маршрута
Шаг 8. Настройка минимальной длины пароля администратора Sandbox
Шаг 9. Создание учетной записи администратора Sandbox
Развертывание компонентов Central Node и Sensor в виде кластера
Развертывание сервера хранения данных
Шаг 1. Выбор роли сервера
Шаг 2. Выбор режима развертывания
Шаг 3. Выбор диска для установки компонента
Шаг 4. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 5. Выбор маски сети для адресации серверов кластера
Шаг 6. Выбор маски сети для адресации компонентов программы
Шаг 7. Выбор кластерного сетевого интерфейса
Шаг 8. Выбор внешнего сетевого интерфейса
Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов
Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере
Создание учетной записи администратора
Аутентификация сервера в кластере
Шаг 11. Добавление адресов DNS-серверов
Шаг 12. Выбор дисков для Ceph-хранилища
Развертывание обрабатывающего сервера
Шаг 1. Выбор роли сервера
Шаг 2. Выбор режима развертывания
Шаг 3. Выбор диска для установки компонента
Шаг 4. Просмотр Лицензионного соглашения и Политики конфиденциальности
Шаг 5. Выбор маски сети для адресации серверов кластера
Шаг 6. Выбор маски сети для адресации компонентов программы
Шаг 7. Выбор кластерного сетевого интерфейса
Шаг 8. Выбор внешнего сетевого интерфейса
Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов
Шаг 10. Аутентификация сервера в кластере
Шаг 11. Настройка получения зеркалированного трафика со SPAN-портов
Шаг 12. Добавление адресов DNS-серверов

Установка компонентов Central Node и Sensor на сервере

Шаг 1. Выбор роли сервера

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности

Шаг 3. Выбор диска для установки компонента

Шаг 4. Выделение диска для базы данных компонента Targeted Attack Analyzer

Шаг 5. Выбор маски сети для адресации серверов кластера

Шаг 6. Выбор внешнего сетевого интерфейса

Шаг 7. Выбор способа получения IP-адресов для сетевых интерфейсов

Шаг 8. Создание учетной записи администратора

Шаг 9. Добавление адресов DNS-серверов

Шаг 10. Настройка получения зеркалированного трафика со SPAN-портов

Шаг 11. Настройка синхронизации времени с NTP-сервером

Установка компонента Sensor на отдельном сервере

Шаг 1. Выбор роли сервера

Шаг 2. Просмотр Лицензионного соглашения и Политики конфиденциальности

Шаг 3. Выбор диска для установки компонента

Шаг 4. Выбор внешнего сетевого интерфейса

Шаг 5. Подключение к серверу с компонентом Central Node

Шаг 6. Создание учетной записи администратора

Настройка параметров масштабирования программы

Настройка интеграции Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent

Настройка доверенного соединения Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent

Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

Настройка соединения с сервером Sensor без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

Настройка соединения с сервером Sensor с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

Скачивание TLS-сертификата сервера Central Node на компьютер

Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform

Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent

Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание криптоконтейнера

Загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform

Просмотр таблицы TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Фильтрация и поиск TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Удаление TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка криптоконтейнера в Kaspersky Endpoint Agent

Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor
Включение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor
Авторизация компонента Sensor на сервере Central Node
Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor
Загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor
Скачивание TLS-сертификата сервера Sensor на компьютер
Настройка интеграции и доверенного соединения с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent
Начало работы с программой
Начало работы в веб-интерфейсе для управления масштабированием
Начало работы в веб-интерфейсе программы под учетной записью локального администратора
Начало работы в меню администратора программы
Начало работы с программой в режиме Technical Support Mode
Управление учетными записями администраторов и пользователей программы
Создание учетной записи администратора веб-интерфейса программы
Создание учетной записи пользователя веб-интерфейса программы
Настройка отображения таблицы учетных записей пользователей
Просмотр таблицы учетных записей пользователей
Фильтрация учетных записей
Сброс фильтра учетных записей
Изменение прав доступа учетной записи пользователя веб-интерфейса программы
Включение и отключение учетной записи администратора или пользователя веб-интерфейса программы
Изменение пароля учетной записи администратора или пользователя программы
Изменение пароля своей учетной записи
Аутентификация с помощью доменных учетных записей
Создание keytab-файла
Настройка интеграции с Active Directory
Отключение интеграции с Active Directory
Участие в Kaspersky Security Network и использование Kaspersky Private Security Network
Просмотр Положения о KSN и настройка участия в KSN
Включение использования KPSN
Настройка подключения к локальной репутационной базе KPSN
Настройка сохранения информации в локальную репутационную базу KPSN
Отказ от участия в KSN и использования KPSN
Работа с компонентом Sandbox через веб-интерфейс
Обновление баз компонента Sandbox
Запуск обновления баз вручную
Выбор источника обновления баз
Включение и отключение использования прокси-сервера для обновления баз
Настройка параметров соединения с прокси-сервером для обновления баз
Настройка соединения компонентов Sandbox и Central Node
Обработка запросов на подключение от серверов Central Node в веб-интерфейсе Sandbox
Настройка сетевых интерфейсов компонента Sandbox
Настройка параметров DNS
Настройка параметров управляющего сетевого интерфейса

Настройка параметров сетевого интерфейса для доступа обрабатываемых объектов в интернет
Добавление, изменение и удаление статических сетевых маршрутов
Обновление системы Sandbox
Установка даты и времени системы Sandbox
Установка и настройка образов операционных систем и программ для работы компонента Sandbox
Загрузка ISO-образов операционных систем и программ для работы компонента Sandbox
Создание виртуальных машин с образами операционных систем и программ для работы компонента Sandbox
Установка виртуальных машин с образами операционных систем и программ для работы компонента Sandbox
Удаление всех виртуальных машин, ожидающих установки
Установка максимального количества одновременно запускаемых виртуальных машин
Загрузка журнала системы Sandbox на жесткий диск
Экспорт параметров Sandbox
Импорт параметров Sandbox
Перезагрузка сервера Sandbox
Выключение сервера Sandbox
Изменение пароля учетной записи администратора Sandbox
Администратору: работа в веб-интерфейсе программы
Интерфейс Kaspersky Anti Targeted Attack Platform
Мониторинг работы программы
О виджетах и схемах расположения виджетов
Выбор тенанта и сервера для работы в разделе Мониторинг
Добавление виджета на текущую схему расположения виджетов
Перемещение виджета на текущей схеме расположения виджетов
Удаление виджета с текущей схемы расположения виджетов
Сохранение схемы расположения виджетов в PDF
Настройка периода отображения данных на виджетах
Мониторинг приема и обработки входящих данных
Мониторинг очередей обработки данных модулями и компонентами программы
Мониторинг обработки данных компонентом Sandbox
Просмотр состояния работоспособности модулей и компонентов программы
Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса программы
Настройка даты и времени сервера
Генерация или загрузка TLS-сертификата сервера
Скачивание TLS-сертификата сервера на компьютер
Назначение DNS-имени сервера
Настройка параметров DNS
Настройка параметров сетевого интерфейса
Настройка сетевого маршрута для использования по умолчанию
Настройка параметров соединения с прокси-сервером
Настройка параметров соединения с почтовым сервером
Выбор операционных систем для проверки объектов в Sandbox
Управление компонентом Sensor
Просмотр таблицы серверов с компонентом Sensor
Обработка запроса на подключение от компонента Sensor
Настройка максимального размера проверяемого файла
Настройка получения зеркалированного трафика со SPAN-портов
Настройка интеграции с почтовым сервером по протоколу SMTP

Настройка TLS-шифрования соединений с почтовым сервером по протоколу SMTP
Включение интеграции с прокси-сервером по протоколу ICAP
Настройка интеграции с почтовым сервером по протоколу POP3
Управление кластером
Просмотр таблицы серверов кластера
Добавление сервера в кластер
Увеличение дискового пространства сервера хранения
Вывод серверов из эксплуатации
Удаление сервера из кластера
Включение и выключение кластера
Уведомления о максимальной загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor
Настройка максимального допустимого значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor
Настройка соединения с протоколом SNMP
Описание объектов MIB Kaspersky Anti Targeted Attack Platform
Работа с информацией о хостах с Kaspersky Endpoint Agent
Выбор тенанта для работы в разделе Endpoint Agents
Просмотр таблицы хостов с Kaspersky Endpoint Agent на отдельном сервере Central Node
Просмотр таблицы хостов с Kaspersky Endpoint Agent в режиме распределенного решения и мультитенантности
Просмотр информации о хосте
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по имени хоста
Фильтрация и поиск хостов с Kaspersky Endpoint Agent, изолированных от сети
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по именам серверов PCN и SCN
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по IP-адресу компьютера
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по версии операционной системы на компьютере
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по версии Kaspersky Endpoint Agent
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по их активности
Быстрое создание фильтра хостов с Kaspersky Endpoint Agent
Сброс фильтра хостов с Kaspersky Endpoint Agent
Настройка показателей активности Kaspersky Endpoint Agent
Поддерживаемые интерпретаторы и процессы
Настройка интеграции с компонентом Sandbox
Просмотр таблицы серверов с компонентом Sandbox
Создание запроса на подключение к серверу с компонентом Sandbox
Включение и отключение соединения с компонентом Sandbox
Удаление соединения с компонентом Sandbox
Настройка интеграции с внешними системами
Просмотр таблицы внешних систем
Обработка запроса от внешней системы
Удаление внешней системы из списка разрешенных к интеграции
Настройка приоритета обработки трафика от почтовых сенсоров
Настройка интеграции с Kaspersky Managed Detection and Response
Включение интеграции с MDR
Отключение интеграции с MDR
Замена конфигурационного файла MDR

Настройка интеграции с SIEM-системой
Включение и отключение записи информации в удаленный журнал
Настройка основных параметров интеграции с SIEM-системой
Загрузка TLS-сертификата
Включение и отключение TLS-шифрования соединения с SIEM-системой
Содержание и свойства syslog-сообщений об обнаружениях
Управление журналом активности
Включение и отключение записи информации в журнал активности
Скачивание файла журналов активности
Содержание и свойства CEF-сообщений о действиях пользователей в веб-интерфейсе
Обновление баз программы
Выбор источника обновления баз
Запуск обновления баз вручную
Создание списка паролей для архивов
Сотруднику службы безопасности: работа в веб-интерфейсе программы
Интерфейс Kaspersky Anti Targeted Attack Platform
Выбор тенанта для работы в веб-интерфейсе программы
Мониторинг работы программы
О виджетах и схемах расположения виджетов
Добавление виджета на текущую схему расположения виджетов
Перемещение виджета на текущей схеме расположения виджетов
Удаление виджета с текущей схемы расположения виджетов
Сохранение схемы расположения виджетов в PDF
Настройка периода отображения данных на виджетах
Настройка масштаба отображения виджетов
Основные принципы работы с виджетами типа "Обнаружения"
Просмотр состояния работоспособности модулей и компонентов программы
Просмотр таблицы обнаружений
Настройка отображения таблицы обнаружений
Фильтрация, сортировка и поиск обнаружений
Фильтрация обнаружений по наличию статуса VIP
Фильтрация и поиск обнаружений по времени
Фильтрация обнаружений по степени важности
Фильтрация и поиск обнаружений по категориям обнаруженных объектов
Фильтрация и поиск обнаружений по полученной информации
Фильтрация и поиск обнаружений по адресу источника
Фильтрация и поиск обнаружений по адресу назначения
Фильтрация и поиск обнаружений по имени сервера
Фильтрация и поиск обнаружений по названию технологии
Фильтрация и поиск обнаружений по состоянию их обработки пользователем
Сортировка обнаружений в таблице
Быстрое создание фильтра обнаружений
Сброс фильтра обнаружений
Просмотр обнаружений
Просмотр информации об обнаружении
Общая информация об обнаружении любого типа
Информация в блоке Информация об объекте

- Информация в блоке Информация об обнаружении
- Информация в блоке Результаты проверки
- Информация в блоке Правило IDS
- Информация в блоке Сетевое событие
- Результаты проверки в Sandbox
- Результаты IOC-проверки
- Информация в блоке Хосты
- Информация в блоке Журнал изменений
- Отправка данных об обнаружении

Рекомендации по обработке обнаружений
- Рекомендации по обработке AM-обнаружений
- Рекомендации по обработке TAA-обнаружений
- Рекомендации по обработке SB-обнаружений
- Рекомендации по обработке IOC-обнаружений
- Рекомендации по обработке YARA-обнаружений
- Рекомендации по обработке IDS-обнаружений

Действия пользователей над обнаружениями
- Назначение обнаружений определенному пользователю
- Отметка о завершении обработки одного обнаружения
- Отметка о завершении обработки обнаружений
- Изменение статуса VIP обнаружений
- Добавление комментария к обнаружению

Поиск угроз по базе событий
- Поиск событий в режиме исходного кода
- Поиск событий в режиме конструктора
- Сортировка событий в таблице
- Изменение условий поиска событий
- Поиск событий по результатам их обработки в программах EPP
- Загрузка IOC-файла и поиск событий по условиям, заданным в IOC-файле
- Создание правила TAA (IOA) на основе условий поиска событий

Информация о событиях
- Просмотр таблицы событий
- Настройка отображения таблицы событий
- Просмотр информации о событии
- Информация о событиях в дереве событий
  - Просмотр информации о родительском процессе в дереве событий
  - Просмотр информации о событиях, инициированных родительским процессом, в дереве событий
  - Просмотр информации о хосте в дереве событий
- Рекомендации по обработке событий
  - Выполнение рекомендации по изоляции хоста
  - Выполнение рекомендации по запрету запуска файла
  - Выполнение рекомендации по созданию задачи
- Информация о событии Запущен процесс
- Информация о событии Завершен процесс
- Информация о событии Загружен модуль
- Информация о событии Удаленное соединение
- Информация о событии Правило запрета

Информация о событии Заблокирован документ
Информация о событии Изменен файл
Информация о событии Журнал событий ОС
Информация о событии Изменение в реестре
Информация о событии Прослушан порт
Информация о событии Загружен драйвер
Информация о событии Обнаружение
Информация о событии Результат обработки обнаружения
Информация о событии Интерпретированный запуск файла
Информация о событии AMSI-проверка
Информация о событии Интерактивный ввод команд в консоли
Работа с информацией о хостах с Kaspersky Endpoint Agent
Просмотр таблицы хостов с Kaspersky Endpoint Agent на отдельном сервере Central Node
Настройка отображения таблицы хостов с Kaspersky Endpoint Agent
Просмотр информации о хосте
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по имени хоста
Фильтрация и поиск хостов с Kaspersky Endpoint Agent, изолированных от сети
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по именам серверов PCN и SCN
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по IP-адресу компьютера
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по версии операционной системы на компьютере
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по версии Kaspersky Endpoint Agent
Фильтрация и поиск хостов с Kaspersky Endpoint Agent по их активности
Быстрое создание фильтра хостов с Kaspersky Endpoint Agent
Сброс фильтра хостов с Kaspersky Endpoint Agent
Настройка показателей активности Kaspersky Endpoint Agent
Поддерживаемые интерпретаторы и процессы
Сетевая изоляция хостов с Kaspersky Endpoint Agent
Создание правила сетевой изоляции
Добавление исключения из правила сетевой изоляции
Удаление правила сетевой изоляции
Ограничения, действующие при сетевой изоляции
Автоматическая отправка файлов с хостов с Kaspersky Endpoint Agent на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского"
Включение и отключение автоматической отправки файлов с хостов с Kaspersky Endpoint Agent на проверку компоненту Sandbox
Работа с задачами
Просмотр таблицы задач
Просмотр информации о задаче
Создание задачи получения файла
Создание задачи сбора форензики
Создание задачи получения ключа реестра
Создание задачи получения метафайлов NTFS
Создание задачи получения дампа памяти процесса
Создание задачи получения образа диска
Создание задачи получения дампа оперативной памяти
Создание задачи завершения процесса
Создание задачи проверки хостов с помощью правил YARA

- Создание задачи управления службами
- Создание задачи выполнения программы
- Создание задачи удаления файла
- Создание задачи помещения файла на карантин
- Создание задачи восстановления файла из карантина
- Создание копии задачи
- Удаление задач
- Фильтрация задач по времени создания
- Фильтрация задач по типу
- Фильтрация задач по имени
- Фильтрация задач по имени и пути к файлу
- Фильтрация задач по описанию
- Фильтрация задач по имени сервера
- Фильтрация задач по имени пользователя, создавшего задачу
- Фильтрация задач по состоянию обработки
- Сброс фильтра задач

Работа с политиками (правилами запрета)
- Просмотр таблицы правил запрета
- Настройка отображения таблицы правил запрета
- Просмотр правила запрета
- Создание правила запрета
- Импорт правил запрета
- Включение и отключение правила запрета
- Включение и отключение предустановок
- Удаление правил запрета
- Фильтрация правил запрета по имени
- Фильтрация правил запрета по типу
- Фильтрация правил запрета по хешу файла
- Фильтрация правил запрета по имени сервера
- Сброс фильтра правил запрета

Работа с пользовательскими правилами
- Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз
- Работа с пользовательскими правилами IOC
  - Просмотр таблицы IOC-файлов
  - Просмотр информации об IOC-файле
  - Загрузка IOC-файла
  - Скачивание IOC-файла на компьютер
  - Включение и отключение автоматического использования IOC-файла при проверке хостов
  - Удаление IOC-файла
  - Поиск обнаружений по результатам IOC-проверки
  - Поиск событий по IOC-файлу
  - Фильтрация и поиск IOC-файлов
  - Сброс фильтра IOC-файлов
  - Настройка расписания IOC-проверки
- Работа с пользовательскими правилами TAA (IOA)
  - Просмотр таблицы правил TAA (IOA)
  - Создание правила TAA (IOA) на основе условий поиска событий

Импорт правила TAA (IOA)
Просмотр информации о правиле TAA (IOA)
Поиск обнаружений и событий, в которых сработали правила TAA (IOA)
Фильтрация и поиск правил TAA (IOA)
Сброс фильтра правил TAA (IOA)
Включение и отключение использования правил TAA (IOA)
Изменение правила TAA (IOA)
Удаление правил TAA (IOA)
Работа с пользовательскими правилами IDS
Импорт пользовательского правила IDS
Просмотр информации о пользовательском правиле IDS
Включение и отключение использования правила IDS при проверке событий
Настройка важности обнаружений, выполненных по пользовательскому правилу IDS
Замена пользовательского правила IDS
Скачивание файла пользовательского правила IDS на компьютер
Удаление пользовательского правила IDS
Работа с пользовательскими правилами YARA
Просмотр таблицы правил YARA
Импорт правил YARA
Настройка отображения таблицы правил YARA
Просмотр информации о правиле YARA
Фильтрация и поиск правил YARA
Сброс фильтра правил YARA
Включение и отключение использования правил YARA
Удаление правил YARA
Работа с объектами в Хранилище и на карантине
Просмотр таблицы объектов, помещенных в Хранилище
Просмотр информации об объекте, загруженном в Хранилище через веб-интерфейс
Просмотр информации об объекте, помещенном в Хранилище по задаче получения файла
Просмотр информации об объекте, помещенном в Хранилище по задаче получения данных
Скачивание объектов из Хранилища
Загрузка объектов в Хранилище
Отправка объектов из Хранилища на проверку
Удаление объектов из Хранилища
Фильтрация объектов в Хранилище по типу объекта
Фильтрация объектов в Хранилище по описанию объекта
Фильтрация объектов в Хранилище по результатам проверки
Фильтрация объектов в Хранилище по имени сервера Central Node, PCN или SCN
Фильтрация объектов в Хранилище по источнику объекта
Фильтрация объектов по времени помещения в Хранилище
Сброс фильтра объектов в Хранилище
Просмотр таблицы объектов, помещенных на карантин на компьютерах с Kaspersky Endpoint Agent
Просмотр информации об объекте на карантине
Восстановление объекта из карантина
Получение копии объекта на карантине на сервер Kaspersky Anti Targeted Attack Platform
Удаление информации об объекте, помещенном на карантин, из таблицы
Фильтрация информации об объектах, помещенных на карантин, по типу объекта

Фильтрация информации об объектах, помещенных на карантин, по описанию объекта
Фильтрация информации об объектах, помещенных на карантин, по имени хоста
Фильтрация информации об объектах, помещенных на карантин, по времени
Сброс фильтра информации об объектах на карантине
Работа с отчетами
Просмотр таблицы шаблонов и отчетов
Создание шаблона
Создание отчета по шаблону
Просмотр отчета
Скачивание отчета на локальный компьютер
Изменение шаблона
Фильтрация шаблонов по имени
Фильтрация шаблонов по имени пользователя, создавшего шаблон
Фильтрация шаблонов по времени создания
Сброс фильтра шаблонов
Удаление шаблона
Фильтрация отчетов по времени создания
Фильтрация отчетов по имени
Фильтрация отчетов по имени сервера с компонентом Central Node
Фильтрация отчетов по имени пользователя, создавшего отчет
Сброс фильтра отчетов
Удаление отчета
Работа с правилами присвоения обнаружениям статуса VIP
Просмотр таблицы правил присвоения статуса VIP
Создание правила присвоения статуса VIP
Удаление правила присвоения статуса VIP
Изменение правила присвоения статуса VIP
Импорт списка правил присвоения статуса VIP
Экспорт списка правил присвоения статуса VIP
Фильтрация и поиск по типу правила присвоения статуса VIP
Фильтрация и поиск по значению правила присвоения статуса VIP
Фильтрация и поиск по описанию правила присвоения статуса VIP
Сброс фильтра правил присвоения статуса VIP
Работа со списком исключений из проверки
Просмотр таблицы данных, исключенных из проверки
Добавление правила исключения из проверки
Удаление правила исключения из проверки
Изменение правила, добавленного в исключения из проверки
Экспорт списка данных, исключенных из проверки
Фильтрация правил в списке исключений из проверки по критерию
Поиск правил в списке исключений из проверки по значению
Сброс фильтра правил в списке исключений из проверки
Работа с IDS-исключениями
Просмотр таблицы правил IDS, добавленных в исключения
Добавление правила IDS в исключения
Редактирование описания правила IDS, добавленного в исключения
Удаление правил IDS из исключений

Работа с ТАА-исключениями
Просмотр таблицы правил ТАА (IOA), добавленных в исключения
Добавление правила ТАА (IOA) в исключения
Просмотр правила ТАА (IOA), добавленного в исключения
Удаление правил ТАА (IOA) из исключений
Создание списка паролей для архивов
Просмотр параметров сервера
Просмотр таблицы серверов с компонентом Sandbox
Просмотр таблицы серверов с компонентом Sensor
Просмотр таблицы внешних систем
Отправка уведомлений
Просмотр таблицы правил для отправки уведомлений
Создание правила для отправки уведомлений об обнаружениях
Создание правила для отправки уведомлений о работе компонентов программы
Включение и отключение правила для отправки уведомлений
Изменение правила для отправки уведомлений
Удаление правила для отправки уведомлений
Фильтрация и поиск правил отправки уведомлений по типу правила
Фильтрация и поиск правил отправки уведомлений по теме уведомлений
Фильтрация и поиск правил отправки уведомлений по адресу электронной почты
Фильтрация и поиск правил отправки уведомлений по их состоянию
Сброс фильтра правил отправки уведомлений
Управление программой Kaspersky Endpoint Agent для Windows
Установка и удаление Kaspersky Endpoint Agent
Подготовка к установке Kaspersky Endpoint Agent
Установка Kaspersky Endpoint Agent
Локальная установка и удаление Kaspersky Endpoint Agent
Установка Kaspersky Endpoint Agent с помощью Мастера установки
Удаление Kaspersky Endpoint Agent с помощью Мастера установки и удаления
Установка, восстановление и удаление программы с помощью командной строки
Установка Kaspersky Endpoint Agent с помощью Kaspersky Security Center
Создание инсталляционного пакета Kaspersky Endpoint Agent
Создание задачи удаленной установки Kaspersky Endpoint Agent
Установка средств администрирования Kaspersky Endpoint Agent
Установка и обновление плагина управления Kaspersky Endpoint Agent
Установка и обновление веб-плагина управления Kaspersky Endpoint Agent
Обновление предыдущей версии Kaspersky Endpoint Agent
Восстановление Kaspersky Endpoint Agent
Изменения в системе после установки Kaspersky Endpoint Agent
Активация Kaspersky Endpoint Agent
Управление активацией Kaspersky Endpoint Agent
Функциональные ограничения после окончания срока действия лицензии
Просмотр информации о действующей лицензии
Управление Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center
Управление политиками Kaspersky Endpoint Agent
Создание политики Kaspersky Endpoint Agent
Включение параметров в политике Kaspersky Endpoint Agent

Настройка параметров Kaspersky Endpoint Agent
Открытие окна параметров Kaspersky Endpoint Agent
Настройка параметров безопасности Kaspersky Endpoint Agent
Настройка прав пользователей
Включение защиты паролем
Включение и отключение механизма самозащиты
Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером
Настройка Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent
Настройка использования KSN в Kaspersky Endpoint Agent
Настройка интеграции Kaspersky Endpoint Agent с KATA Central Node
Настройка параметров передачи данных
Настройка параметров регулирования количества запросов
Включение и отключение интеграции с KATA Central Node
Настройка доверенного соединения с KATA Central Node
Настройка параметров синхронизации Kaspersky Endpoint Agent с KATA Central Node
Настройка параметров EDR-телеметрии
Включение и настройка исключений и оптимизации объема отправляемой EDR-телеметрии о процессах программ
Включение и настройка исключений отправляемой EDR-телеметрии о сетевых коммуникациях
Настройка параметров хранилищ в Kaspersky Endpoint Agent
О карантине Kaspersky Endpoint Agent
Об управлении карантином в Kaspersky Endpoint Agent
Настройка параметров карантина и восстановления объектов из карантина
Настройка синхронизации данных с Сервером администрирования
Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response
Настройка диагностики сбоев
Управление задачами Kaspersky Endpoint Agent
Создание локальной задачи
Создание групповой задачи
Просмотр списка задач
Удаление задач из списка
Запуск задач вручную
Запуск задач по расписанию
Просмотр результатов выполнения задач
Изменение срока хранения результатов выполнения задач на Сервере администрирования
Создание задачи активации Kaspersky Endpoint Agent
Управление задачами обновления баз и модулей Kaspersky Endpoint Agent
Создание задачи обновления баз и модулей программы
Настройка параметров задачи обновления баз и модулей программы
Управление задачами поиска IOC в Kaspersky Endpoint Agent
О задачах поиска IOC в Kaspersky Endpoint Agent
Управление задачами поиска IOC в Kaspersky Endpoint Agent
Управление стандартными задачами поиска IOC
Требования к IOC-файлам
Поддерживаемые IOC-термины
Создание и настройка стандартной задачи поиска IOC
Настройка параметров стандартной задачи поиска IOC

Экспорт IOC-коллекции
Просмотр результатов выполнения задачи поиска IOC
Управление Kaspersky Endpoint Agent в Kaspersky Security Center Web Console
Управление политиками Kaspersky Endpoint Agent
Создание политики Kaspersky Endpoint Agent
Включение параметров в политике Kaspersky Endpoint Agent
Настройка параметров Kaspersky Endpoint Agent
Открытие окна параметров Kaspersky Endpoint Agent
Настройка параметров безопасности Kaspersky Endpoint Agent
Настройка прав пользователей
Включение защиты паролем
Включение и отключение механизма самозащиты
Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером
Настройка Kaspersky Security Center в качестве прокси-сервера для активации Kaspersky Endpoint Agent
Настройка типа политики Kaspersky Endpoint Agent
Настройка использования KSN в Kaspersky Endpoint Agent
Настройка интеграции Kaspersky Endpoint Agent с KATA Central Node
Настройка параметров передачи данных
Настройка параметров регулирования количества запросов
Включение и отключение интеграции с KATA Central Node
Настройка доверенного соединения с KATA Central Node
Настройка параметров синхронизации Kaspersky Endpoint Agent с KATA Central Node
Настройка параметров EDR-телеметрии
Включение и настройка исключений и оптимизации объема отправляемой EDR-телеметрии о процессах программ
Включение и настройка исключений отправляемой EDR-телеметрии о сетевых коммуникациях
Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response
Настройка параметров хранилищ в Kaspersky Endpoint Agent
О карантине Kaspersky Endpoint Agent
Об управлении карантином в Kaspersky Endpoint Agent
Настройка параметров карантина и восстановления объектов из карантина
Настройка синхронизации данных с Сервером администрирования
Настройка диагностики сбоев
Управление задачами Kaspersky Endpoint Agent
Создание задач
Просмотр списка задач
Удаление задач из списка
Настройка расписания запуска задач
Запуск задач вручную
Создание задач активации Kaspersky Endpoint Agent
Настройка параметров задачи обновления баз и модулей программы
Управление стандартными задачами поиска IOC
Требования к IOC-файлам
Поддерживаемые IOC-термины
Настройка параметров стандартной задачи поиска IOC
Просмотр результатов выполнения задачи поиска IOC
Настройка параметров задачи Поместить файл на карантин

Настройка параметров задачи Удалить файл
Настройка параметров задачи Запустить процесс
Настройка параметров задачи Завершить процесс
Управление Kaspersky Endpoint Agent через интерфейс командной строки
Управление активацией Kaspersky Endpoint Agent
Управление аутентификацией Kaspersky Endpoint Agent
Настройка трассировки
Настройка создания дампа процессов Kaspersky Endpoint Agent
Просмотр информации о параметрах карантина и объектах на карантине
Действия над объектами на карантине
Управление параметрами интеграции с компонентом KATA Central Node
Запуск обновления баз или модулей Kaspersky Endpoint Agent
Запуск, остановка и просмотр текущего состояния программы
Защита программы паролем
Защита служб программы технологией PPL
Управление параметрами самозащиты
Управление фильтрацией событий
Управление стандартными задачами поиска IOC
Управление сканированием файлов и процессов по YARA-правилам
Управление сканированием объектов точек автозапуска по YARA-правилам
Создание дампа памяти
Создание дампа диска
Управление программой Kaspersky Endpoint Agent для Linux
Установка и удаление Kaspersky Endpoint Agent для Linux
Подготовка к установке Kaspersky Endpoint Agent для Linux
Установка Kaspersky Endpoint Agent для Linux с помощью Консоли администрирования Kaspersky Security Center
Установка плагина управления Kaspersky Endpoint Agent для Linux
Добавление устройств для установки Kaspersky Endpoint Agent для Linux
Создание инсталляционного пакета Kaspersky Endpoint Agent для Linux
Удаленная установка Kaspersky Endpoint Agent для Linux на выбранные устройства
Установка Kaspersky Endpoint Agent для Linux с помощью Kaspersky Security Center Web Console
Установка веб-плагина управления Kaspersky Endpoint Agent
Добавление устройств для установки Kaspersky Endpoint Agent для Linux
Создание инсталляционного пакета Kaspersky Endpoint Agent для Linux
Удаленная установка Kaspersky Endpoint Agent для Linux на выбранные устройства
Локальная установка Kaspersky Endpoint Agent для Linux
Обновление и восстановление Kaspersky Endpoint Agent для Linux
Удаление Kaspersky Endpoint Agent для Linux
Управление Kaspersky Endpoint Agent для Linux с помощью Консоли администрирования Kaspersky Security Center
Управление политиками Kaspersky Endpoint Agent для Linux
Создание политики Kaspersky Endpoint Agent для Linux
Включение параметров в политике Kaspersky Endpoint Agent для Linux
Управление задачами обновления баз и модулей Kaspersky Endpoint Agent

Управление Kaspersky Endpoint Agent для Linux с помощью Kaspersky Security Center Web Console
Управление политиками Kaspersky Endpoint Agent для Linux
Создание политики Kaspersky Endpoint Agent для Linux
Включение параметров в политике Kaspersky Endpoint Agent для Linux
Управление задачами обновления баз и модулей Kaspersky Endpoint Agent
Управление Kaspersky Endpoint Agent для Linux с помощью командной строки
Проверка целостности компонентов программы Kaspersky Endpoint Agent для Linux
Создание резервной копии и восстановление программы
Создание резервной копии параметров сервера Central Node из меню администратора программы
Загрузка файла с резервной копией параметров сервера с сервера Central Node или PCN на жесткий диск компьютера
Загрузка файла с резервной копией параметров сервера с вашего компьютера на сервер Central Node
Восстановление параметров сервера из резервной копии через меню администратора программы
Создание резервной копии программы в режиме Technical Support Mode
Восстановление программы из резервной копии в режиме Technical Support Mode
Обновление Kaspersky Anti Targeted Attack Platform
Обновление компонента Central Node
Состав и объем данных, сохраняемых при обновлении программы Kaspersky Anti Targeted Attack Platform
Взаимодействие с внешними системами по API
Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform
API для проверки объектов внешних систем
Запрос на проверку объектов
Запрос на получение результатов проверки
Запрос на удаление результатов проверки
Запрос на вывод ограничений программы на проверку объектов
API для получения внешними системами информации об обнаружениях программы
Запрос на вывод информации об обнаружениях
Состав передаваемых данных
Данные об обнаруженных объектах
Данные о найденных угрозах
Данные об окружении обнаруженных объектов
API для управления действиями по реагированию на угрозы
Запрос на получение списка хостов Kaspersky Endpoint Agent
Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов Kaspersky Endpoint Agent
Управление сетевой изоляцией хостов
Запрос на включение сетевой изоляции
Запрос на отключение сетевой изоляции
Запрос на добавление исключения в правило сетевой изоляции
Управление правилами запрета
Запрос на создание правила запрета
Запрос на удаление правила запрета
Управление задачей запуска программы
Получение информации о задаче
Запрос на создание задачи
Запрос на удаление задачи
Источники информации о программе

Обращение в Службу технической поддержки
Получение информации о Kaspersky Endpoint Agent для Linux для Службы технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Глоссарий
Advanced persistent threat (APT)
Anti-Malware Engine
Backdoor-программа
Central Node
CSRF-атака
End User License Agreement
ICAP-данные
Intrusion Detection System
IOA
IOC
IOC-файл
Kaspersky Anti Targeted Attack Platform
Kaspersky Endpoint Agent
Kaspersky Private Security Network
Kaspersky Secure Mail Gateway
Kaspersky Security Network (KSN)
Kaspersky Threat Intelligence Portal
KATA
KEDR
Kerberos-аутентификация
Keytab-файл
MIB (Management Information Base)
MITM-атака
NTP-сервер
OpenIOC
Sandbox
Sensor
SIEM-система
SPAN
Syslog
Targeted Attack Analyzer
TLS-шифрование
YARA
Альтернативный поток данных
Атака "нулевого дня"
Вредоносные веб-адреса
Дамп
Зеркалированнный трафик
Имя субъекта-службы (SPN)
Локальная репутационная база KPSN
Мультитенантность
Правила YARA

- Правило TAA (IOA)
- Пропускная способность канала связи
- Распределенное решение
- Сигнатура
- Статус VIP
- Тенант
- Техника MITRE
- Трассировка
- Угрозы нового поколения
- Уязвимость "нулевого дня"
- Фишинговые URL-адреса
- Целевая атака

Информация о стороннем коде

Уведомления о товарных знаках

Справка Kaspersky Anti Targeted Attack Platform

Новые функции

- Что нового в Kaspersky Anti Targeted Attack Platform

Аппаратные и программные требования

- Аппаратные и программные требования к компьютерам для работы с программой через веб-интерфейс
- Совместимость Kaspersky Anti Targeted Attack Platform с Kaspersky Endpoint Agent для Windows и Linux

Лицензирование

- Лицензирование Kaspersky Anti Targeted Attack Platform

Начало работы

- Распределенное решение и мультитенантность
- Масштабирование Kaspersky Anti Targeted Attack Platform
- Установка и первоначальная настройка Kaspersky Anti Targeted Attack Platform
- Настройка интеграции Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent

Работа в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

- Работа в веб-интерфейсе программы – Администратору
- Работа в веб-интерфейсе программы – Сотруднику службы безопасности

Дополнительные возможности

- Работа с компонентом Sandbox через веб-интерфейс
- Управление Kaspersky Endpoint Agent для Windows
- Управление Kaspersky Endpoint Agent для Linux
- Взаимодействие с внешними системами по API

Обновление

- Обновление предыдущей версии Kaspersky Anti Targeted Attack Platform

Обращение в Службу технической поддержки

- Способы получения технической поддержки

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 *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.

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 программой Kaspersky Endpoint Agent и получать данные с отдельных компьютеров, входящих в IT-инфраструктуру организации и работающих под управлением операционных систем Microsoft® Windows® и Linux®. Kaspersky Endpoint Agent осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.
- Интегрироваться с внешними системами с помощью интерфейса REST API и проверять файлы на этих системах.

Программа использует следующие средства анализа угроз (Threat Intelligence):

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

- Интеграцию с информационной системой "Лаборатории Касперского" Kaspersky Threat Intelligence Portal, которая содержит и отображает информацию о репутации файлов и URL-адресов.
- Базу угроз "Лаборатории Касперского" Kaspersky Threats.

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

- Отображать результаты работы в веб-интерфейсе серверов Central Node, Primary Central Node (далее также PCN) или Secondary Central Node (далее также 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, выполнять рекомендации по оценке и расследованию инцидентов.
- Просматривать таблицу событий, происходящих на компьютерах и серверах, входящих в IT-инфраструктуру организации, осуществлять поиск угроз, фильтрацию, просмотр и работу с каждым событием, выполнять рекомендации по оценке и расследованию инцидентов.
- Выполнять задачи на хостах с Kaspersky Endpoint Agent: запускать программы и останавливать процессы, скачивать и удалять файлы, помещать объекты на карантин на компьютерах с программой Kaspersky Endpoint Agent, копии файлов в Хранилище программы, а также восстанавливать файлы из карантина.
- Настраивать политики запрета запуска файлов и процессов, которые они считают небезопасными, на выбранных хостах с программой Kaspersky Endpoint Agent.
- Изолировать отдельные хосты с программой Kaspersky Endpoint Agent от сети.
- Работать с правилами TAA (IOA) для классификации и анализа событий.
- Работать с пользовательскими правилами Targeted Attack Analyzer TAA (IOA), Intrusion Detection System (IDS) и YARA: загружать правила, по которым программа будет проверять события и создавать обнаружения.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах с компонентом Endpoint Agent и в базе обнаружений.
- Добавлять правила TAA (IOA) и правила IDS, предоставленные специалистами "Лаборатории Касперского", в исключения из проверки.
- Работать с объектами на карантине и копиями объектов в Хранилище.

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

Пользователи с ролью **Аудитор** 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, просматривать данные каждого обнаружения.
- Просматривать таблицу событий, происходящих на компьютерах и серверах, входящих в IT-инфраструктуру организации, осуществлять поиск угроз, фильтрацию, просмотр каждого события.
- Просматривать список хостов с компонентом Endpoint Agent и информацию о выбранных хостах.
- Просматривать пользовательские правила Targeted Attack Analyzer TAA (IOA), Intrusion Detection System (IDS) и YARA.
- Просматривать исключенные из проверки правила TAA (IOA) и правила IDS, предоставленные специалистами "Лаборатории Касперского".
- Просматривать отчеты о работе программы и отчеты об обнаружениях.
- Просматривать список обнаружений со статусом VIP, список данных, исключенных из проверки.
- Осуществлять мониторинг работоспособности программы.
- Просматривать все настройки, производимые в веб-интерфейсе программы.

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

- Настраивать параметры работы программы.
- Настраивать серверы для работы в режиме распределенного решения и мультитенантности.
- Производить интеграцию программы с другими программами и системами.
- Работать с TLS-сертификатами и настраивать доверенное соединение сервера Central Node с сервером Sandbox, а также серверов Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent и с внешними системами.
- Управлять учетными записями пользователей программы.
- Осуществлять мониторинг работоспособности программы.

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

- На компьютер локальной сети организации был загружен файл или была предпринята попытка загрузки файла.
- На 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 возможности и доработки:

1. Компонент Central Node может быть развернут в виде отказоустойчивого кластера, который состоит из серверов 2 ролей – серверов хранения и обрабатывающих серверов. Отказоустойчивость достигается за счет дублирования данных между серверами хранения и избыточности вычислительных ресурсов: при выходе из строя одного сервера его функции выполняет другой сервер с аналогичной ролью. Программа при этом продолжает работать.

2. Добавлена возможность настроить параметры масштабирования программы. Вы можете указать планируемый объем SPAN-трафика, почтового трафика, количество хостов с Kaspersky Endpoint Agent, а также планируемый размер Хранилища и базы событий. Программа настроит серверы с компонентом Central Node в соответствии с указанными параметрами.

   Для настройки параметров масштабирования используется отдельный веб-интерфейс – *веб-интерфейс для управления масштабированием*. Если компонент Central Node развернут в виде кластера, в веб-интерфейсе для управления масштабированием вы также можете просмотреть список серверов и выключить кластер.

3. Для компонента Sandbox поддержана установка операционной системы Astra Linux 1.7 и запуск объектов в этой операционной системе.

Использование операционной системы опционально: вы можете выбрать набор операционных систем, на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox – Windows XP, Windows 7, Windows 10; Windows XP, Windows 7, Windows 10, CentOS 7.8 или Windows XP, Windows 7, Windows 10, Astra Linux 1.7.

Программа может запускать в Astra Linux 1.7 следующие объекты:

- Файлы с хостов с Kaspersky Endpoint Agent, отправленные на проверку компоненту Sandbox в соответствии с правилами ТАА (IOA) "Лаборатории Касперского".
- Файлы, загруженные в Хранилище вручную или по задаче **Получить файл** (при условии, что объект был отправлен на проверку).
- Файлы, полученные из почтового или сетевого трафика.

4. Расширен функционал задач для хостов с компонентом Kaspersky Endpoint Agent для Windows:

- Добавлена задача **Получить образ диска**.

  Задача позволяет получить образ диска выбранного хоста.

- Добавлена задача **Получить дамп памяти**.

  Задача позволяет получить дамп оперативной памяти выбранного хоста.

  Файлы, полученные в результате выполнения задач, сохраняются в общий сетевой ресурс.

В связи с добавлением новых типов задач в программе произошли следующие изменения:

- Задачи сбора данных теперь сгруппированы в подменю **Собрать данные**.
- Переименованы следующие типы задач:
  - **Получить файл** → **Файл**.
  - **Собрать данные** → **Форензика**.
  - **Получить ключ реестра** → **Ключ реестра**.
  - **Метафайлы NTFS** → **Метафайлы NTFS**.
  - **Получить дамп памяти процесса** → **Дамп памяти процесса**.

5. Добавлен новый тип события – **Завершен процесс**.

6. В веб-интерфейсе программы произошли следующие изменения:

- В окне параметров сетевого интерфейса добавлена возможность выбрать способ настройки этого интерфейса: вручную или получать параметры от DHCP-сервера.
- В разделе Параметры, подразделе Дата и время упразднена возможность отключить синхронизацию с NTP-сервером.
- Упразднена возможность указать максимальное допустимое значение заполнения жесткого диска серверов Central Node и Sensor.

В Kaspersky Endpoint Agent для Windows 3.14 появились следующие возможности и доработки:

1. Добавлена возможность взаимодействия с отказоустойчивыми кластерами серверов Kaspersky Anti Targeted Attack Platform.
2. Добавлена возможность создавать через интерфейс командной строки полный дамп памяти и полный дамп диска защищаемого устройства для дальнейшего использования Kaspersky Anti Targeted Attack Platform.
3. Добавлен режим работы Kaspersky Endpoint Agent, совместимый с Azure WVD.
4. Исправлена ошибка, связанная с возможной блокировкой обрабатываемых Kaspersky Endpoint Agent файлов.

Для Kaspersky Endpoint Agent 3.12 для Linux актуальны следующие изменения:

Работа с решением Kaspersky Managed Detection and Response больше не поддерживается. Не рекомендуется использовать Kaspersky Endpoint Agent for Linux для работы с этим решением. Для работы с Kaspersky Managed Detection and Response следует использовать программу Kaspersky Endpoint Security для Linux.

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 Kaspersky Anti Targeted Attack Platform входят следующие файлы:

1. Образ диска (файл с расширением iso) с установочными файлами операционной системы Ubuntu Server 20.04.5 и компонентов Sensor, Central Node.

2. Образ диска (файл с расширением iso) с установочными файлами операционной системы CentOS 7.9 и компонента Sandbox.

3. Образы дисков (файлы с расширением iso) операционных систем Windows XP SP3, Windows 7 (64-разрядной), Windows 10 (64-разрядной), CentOS 7.8, в которых компонент Sandbox будет запускать файлы.

   Для российских пользователей также поставляется образ диска с операционной системой Astra Linux 1.7.

4. Скрипт kata-upgrade-preparation для обновления компонента Central Node.

5. Файл с информацией о стороннем коде, используемом в Kaspersky Anti Targeted Attack Platform.

В комплект поставки программы Kaspersky Endpoint Agent входят следующие файлы:

Комплект поставки Kaspersky Endpoint Agent

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

Аппаратные и программные требования

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

- Mozilla™ Firefox™ для Linux.
- Mozilla Firefox для Windows.
- Google™ Chrome™ для Windows.
- Google Chrome для Linux.
- Edge (Windows).
- Safari (Mac).

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

Для развертывания программы на виртуальной платформе должен быть установлен гипервизор VMware ESXi™ версии 6.7.0 или 7.0.

Для корректной работы программы в виртуальной среде необходимо установить для гипервизора актуальный патч.

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

Аппаратные требования к компонентам Central Node, Sensor и Sandbox приведены в Руководстве по масштабированию.

Требования к Kaspersky Endpoint Agent для Windows

В этом разделе описываются аппаратные и программные требования для Kaspersky Endpoint Agent 3.14 для Windows.

Если версия программы Kaspersky Anti Targeted Attack Platform на серверах Central Node несовместима с версией программы Kaspersky Endpoint Agent 3.14 для Windows, установленной на компьютерах локальной сети вашей организации, в работе Kaspersky Anti Targeted Attack Platform возможны ограничения.

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

Программные требования к компьютерам для установки Kaspersky Endpoint Agent 3.14 для Windows

Поддерживаемые операционные системы для рабочих станций:

- Windows 7 SP1 Home / Professional / Enterprise / Ultimate 32-разрядная / 64-разрядная.
- Windows 8.1.1 Professional / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS3 (версия 1703) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS4 (версия 1803) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 RS5 (версия 1809) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 19H1 (версия 1903) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 19H2 (версия 1909) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 20H1 (версия 2004) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 20H2 (версия 2009) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 21H1 (версия 21H1) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 21H2 (версия 21H2) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.
- Windows 11 21H2 (версия 21H2) Home / Professional / Education / Enterprise 32-разрядная / 64-разрядная.

Поддерживаемые серверные операционные системы:

- Windows Server 2008 SP2 Standard / Enterprise 64-разрядная.
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 64-разрядная.
- Windows Server 2012 Foundation / Standard / Enterprise / Datacenter 64-разрядная.
- Windows Server 2012 R2 Foundation / Standard / Enterprise / Datacenter 64-разрядная.
- Windows Server 2016 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 2019 Essentials / Standard / Datacenter 64-разрядная.
- Windows Server 20H2 Standard Core / Datacenter Core 64-разрядная.
- Windows Server 2022 Standard / Datacenter 64-разрядная.

Поддерживаемые встраиваемые операционные системы:

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

Программные требования к компьютерам для установки Kaspersky Endpoint Agent 3.14 для Windows при интеграции с Kaspersky Industrial CyberSecurity for Nodes

Поддерживаемые операционные системы для рабочих станций:

- Windows XP Professional SP2 32-разрядная / 64-разрядная.
- Windows XP Professional SP3 32-разрядная.
- Windows Vista SP2 32-разрядная / 64-разрядная.
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate 32-разрядная / 64-разрядная.
- Windows 8 Pro / Enterprise 32-разрядная / 64-разрядная.
- Windows 8.1 Pro / Enterprise 32-разрядная / 64-разрядная.
- Windows 10 LTSC 2015 (1507) 32-разрядная / 64-разрядная.
- Windows 10 LTSC 2016 (1607) 32-разрядная / 64-разрядная.
- Windows 10 LTSC 2019 (1809) 32-разрядная / 64-разрядная.
- Windows 10 LTSC 2021 (21H2) 32-разрядная / 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 1703 RS2 32-разрядная / 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 1803 RS4 32-разрядная / 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 1809 RS5 32-разрядная / 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 1903 19H1 32-разрядная / 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 1909 19H2 32- или 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 2004 20H1 32-разрядная / 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 2009 20H2 32-разрядная / 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 21H1 32-разрядная / 64-разрядная.
- Windows 10 Home / Pro / Education / Enterprise 21H2 32-разрядная / 64-разрядная.

Поддерживаемые серверные операционные системы:

- Windows Server 2003 SP1 Standard / Enterprise / Datacenter 32-разрядная / 64-разрядная.
- Windows Server 2003 SP2 Standard / Enterprise / Datacenter 32-разрядная / 64-разрядная.
- Windows Server 2008 SP2 Standard / Enterprise / Datacenter 32-разрядная / 64-разрядная.
- Windows Server 2003 R2 Standard / Enterprise / Datacenter 32-разрядная / 64-разрядная.

- Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter 32-разрядная / 64-разрядная.
- Windows Server 2012 Foundation / Standard / Essentials / Datacenter 64-разрядная.
- Windows Server 2012 R2 Foundation / Standard / Enterprise / Datacenter 64-разрядная.
- Windows Server 2016 Essentials / Standard / Datacenter 64-разрядная следующих версий: 1709 и 1803.
- Windows Server 2019 Standard Core / Datacenter Core 64-разрядная следующих версий: 1903, 1909, 2004, 20H2, 21H2.

Поддерживаемые встраиваемые операционные системы:

- Windows XP Embedded SP2 (WEPOS) 32-разрядная / 64-разрядная.
- Windows XP Embedded SP3 (POSReady 2009) 32-разрядная.
- Windows 7 SP1 Embedded (POSReady 7) 32-разрядная / 64-разрядная.
- Windows Embedded 8.1 Industry Pro 32-разрядная / 64-разрядная.
- Windows 10 IoT Enterprise 32-разрядная / 64-разрядная следующих версий: 1703, 1803, 1809, 1903, 1909, 2004, 2009, 21H1, 21H2.

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

Аппаратные требования к компьютерам для установки Kaspersky Endpoint Agent 3.14 для Windows

Минимальная конфигурация:

- Процессор: 1.4 ГГц (одноядерный) или выше.
- Оперативная память: 256 МБ (512 МБ при 64-разрядной операционной системе).
- Объем свободного места на диске: 500 МБ.
- Один сетевой адаптер со скоростью передачи данных 1 Гбит/с.

При интеграции с Kaspersky Endpoint Security программа Kaspersky Anti Targeted Attack Platform имеет ограниченную функциональность, если на сервере с Kaspersky Endpoint Security установлена операционная система Windows Server® 2008 SP2 x64

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

Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform

Программа Kaspersky Endpoint Agent использует предустановленные параметры, которые определяют его влияние на производительность локального компьютера в сценариях получения информации и взаимодействия с компонентом Central Node.

Если версия программы Kaspersky Anti Targeted Attack Platform, установленной на серверах Central Node, несовместима с версией программы Kaspersky Endpoint Agent, установленной на компьютерах локальной сети вашей организации, возможны ограничения в работе Kaspersky Anti Targeted Attack Platform.

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

Совместимость версий Kaspersky Endpoint Agent для Windows с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Agent	Тип Kaspersky Endpoint Agent	Совместимость с KATA 3.7	Совместимость с KATA 3.7.1	Совместимость с KATA 3.7.2	Совместимость с KATA 4.0	Совместимость с KATA 4.1	Совместимост с KATA 5.0
Endpoint Agent 3.7	Устанавливается отдельно или в составе KES версий 11.2 и 11.3	Нет	Нет	Нет	Нет	Нет	Нет
Endpoint Agent 3.8	Устанавливается отдельно	Да	Да	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения
Endpoint Agent 3.9	Устанавливается отдельно или в составе программ EPP	Да	Да	Есть ограничения	Есть ограничения	Есть ограничения	Есть ограничения
Endpoint Agent 3.10	Устанавливается отдельно или в составе программ EPP	Нет	Есть ограничения	Да	Есть ограничения	Есть ограничения	Есть ограничения
Endpoint Agent 3.11	Устанавливается отдельно или в составе KES 11.7	Нет	Есть ограничения	Да	Есть ограничения	Есть ограничения	Есть ограничения
Endpoint Agent 3.12	Устанавливается отдельно	Нет	Нет	Нет	Да	Есть ограничения	Есть ограничения
Endpoint Agent 3.13	Устанавливается отдельно	Нет	Нет	Нет	Есть ограничения	Да	Есть ограничения
Endpoint Agent 3.14	Устанавливается отдельно	Нет	Нет	Нет	Есть ограничения	Есть ограничения	Да

Совместимость версий Kaspersky Endpoint Agent для Windows с программами EPP

Вы можете использовать только программу Kaspersky Endpoint Agent или настроить интеграцию Kaspersky Endpoint Agent с программами защиты рабочих станций (Endpoint Protection Platform, далее также "EPP") Kaspersky Endpoint Security для Windows, Kaspersky Security для Windows Server и Kaspersky Security для виртуальных сред Легкий агент. Если интеграция между программами настроена, Kaspersky Endpoint Agent будет также передавать на сервер Central Node данные об угрозах, обнаруженных программами EPP, и о результатах их обработки.

Описанные сценарии интеграции не работают при установке программы Kaspersky Endpoint Agent на виртуальный рабочий стол в инфраструктуре Virtual Desktop Infrastructure.

Для интеграции Kaspersky Endpoint Agent с Kaspersky Endpoint Security для Windows и Kaspersky Security для Windows Server требуется установить Kaspersky Endpoint Agent в составе этих программ.

Совместимость Kaspersky Endpoint Agent для Windows с версиями Kaspersky Security для Windows Server

Вы можете установить в составе Kaspersky Security для Windows Server следующие версии Kaspersky Endpoint Agent:

- Kaspersky Endpoint Agent 3.9 в составе Kaspersky Security 11 для Windows Server.
- Kaspersky Endpoint Agent 3.10 в составе Kaspersky Security 11.0.1 для Windows Server.

При установке Kaspersky Endpoint Agent в составе Kaspersky Security для Windows Server отдельно установленная ранее программа Kaspersky Endpoint Agent той же или более ранних версий удаляется. Если версия Kaspersky Endpoint Agent в составе Kaspersky Security для Windows Server более ранняя, программа не будет установлена. В этом случае вам требуется предварительно удалить отдельно установленную программу Kaspersky Endpoint Agent.

При необходимости вы можете обновить программу Kaspersky Endpoint Agent, уже установленную в составе Kaspersky Security для Windows Server. Интеграция между совместимыми версиями программ сохранится как при обновлении Kaspersky Endpoint Agent, так и при обновлении Kaspersky Security для Windows Server.

Информация о совместимости версий программ Kaspersky Endpoint Agent и Kaspersky Security для Windows Server приведена в таблице ниже.

Совместимость версий Kaspersky Endpoint Agent и Kaspersky Security для Windows Server

Версия Kaspersky Security для Windows Server	Совместимость с Endpoint Agent 3.8, 3.9, 3.10	Совместимость с Endpoint Agent 3.11, 3.12	Совместимость с Endpoint Agent 3.13, 3.14
• KSWS 10.1.2	Да	Нет	Нет
• KSWS 11	Да	Да	Нет
• KSWS 11.0.1	Нет	Да	Да

Подробнее об установке Kaspersky Security для Windows Server см. в *справке Kaspersky Security для Windows Server*.

Совместимость Kaspersky Endpoint Agent для Windows с версиями Kaspersky Endpoint Security для Windows

Вы можете установить в составе Kaspersky Endpoint Security для Windows следующие версии Kaspersky Endpoint Agent (Endpoint Sensors):

- Kaspersky Endpoint Agent 3.7 или Kaspersky Endpoint Agent (Endpoint Sensors) 3.6.1 в составе Kaspersky Endpoint Security 11.2, 11.3 для Windows.

  Программа Kaspersky Endpoint Agent (Endpoint Sensors) 3.6.1 несовместима с Kaspersky Anti Targeted Attack Platform 4.1 и выше.

  Программа Kaspersky Endpoint Agent 3.7 несовместима со всеми версиями Kaspersky Anti Targeted Attack Platform.

- Kaspersky Endpoint Agent 3.9 в составе Kaspersky Endpoint Security 11.4, 11.5.
- Kaspersky Endpoint Agent 3.10 в составе Kaspersky Endpoint Security 11.6.
- Kaspersky Endpoint Agent 3.11 в составе Kaspersky Endpoint Security 11.7, 11.8.

При установке Kaspersky Endpoint Agent версии 3.10 и выше в составе Kaspersky Endpoint Security для Windows отдельно установленная ранее программа Kaspersky Endpoint Agent той же или более ранних версий удаляется. Если отдельно установленная программа Kaspersky Endpoint Agent более поздних версий, программа в составе Kaspersky Endpoint Security для Windows не будет установлена. В этом случае вам требуется предварительно удалить отдельно установленную программу Kaspersky Endpoint Agent.

При необходимости вы можете обновить программу Kaspersky Endpoint Agent, уже установленную в составе Kaspersky Endpoint Security для Windows. Интеграция между совместимыми версиями программ сохранится как при обновлении программы Kaspersky Endpoint Agent, так и при обновлении программы Kaspersky Endpoint Security для Windows. Обновление с предыдущей версии Kaspersky Endpoint Agent до версии 3.14 доступно для Kaspersky Endpoint Agent версии 3.7 и выше.

Информация о совместимости версий Kaspersky Endpoint Agent и Kaspersky Endpoint Security для Windows приведена в таблице ниже.

Совместимость версий Kaspersky Endpoint Agent и Kaspersky Endpoint Security для Windows

Версия Kaspersky Endpoint Security	Совместимость с Endpoint Agent 3.8, 3.9	Совместимость с Endpoint Agent 3.10, 3.12	Совместимость с Endpoint Agent 3.11	Совместимость с Endpoint Agent 3.13, 3.14
• KES 10 SP2 MR2	Нет	Нет	Нет	Нет
• KES 10 SP2 MR3/MR4	Да	Нет	Нет	Нет
• KES 11.0.0	Нет	Нет	Нет	Нет
• KES 11.0.1	Да	Нет	Нет	Нет
• KES 11.1 • KES 11.1.1	Да	Да	Нет	Нет
• KES 11.2 • KES 11.3	Да	Да	Да	Нет
• KES 11.4 • KES 11.5	Да	Да	Да	Нет
• KES 11.6–11.12 • KES 11.14–11.18	Да	Да	Да	Да
• KES 11.13	Нет	Нет	Нет	Да

Подробнее об установке Kaspersky Endpoint Security см. в *справке Kaspersky Endpoint Security для Windows*.

Совместимость Kaspersky Endpoint Agent с версиями Kaspersky Security для виртуальных сред Легкий агент

Вы можете настроить интеграцию для отдельно установленных программ Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент.

Информация о совместимости версий программ Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент приведена в таблице ниже.

Совместимость версий Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент

Версия Kaspersky Security для виртуальных сред Легкий агент	Совместимость с Endpoint Agent 3.8, 3.9, 3.10	Совместимость с Endpoint Agent 3.12	Совместимость с Endpoint Agent 3.11, 3.13, 3.14
• KSV 5.1 LA	Да	Да	Нет
• KSV 5.1.1 LA	Да	Нет	Нет
• KSV 5.2 LA	Нет	Да	Да

Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент, установленные на виртуальную машину, дают такую же нагрузку на сервер Central Node, как Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент, установленные на хост.

Подробнее о включении интеграции между Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент см. в *справке Kaspersky Security для виртуальных сред Легкий агент*.

Совместимость Kaspersky Endpoint Agent с версиями Kaspersky Industrial CyberSecurity for Nodes

Вы можете установить программу Kaspersky Endpoint Agent на устройство с установленной программой Kaspersky Industrial CyberSecurity for Nodes. Программы интегрируются автоматически.

Интеграция поддерживается только для Kaspersky Endpoint Agent версии 3.14 и Kaspersky Industrial CyberSecurity for Nodes версии 3.1. Интеграция между другими версиями программ не поддерживается.

Для интеграции с Kaspersky Industrial CyberSecurity for Nodes в Kaspersky Endpoint Agent должен быть установлен соответствующий лицензионный ключ.

Для получения детальной информации вы можете обратиться к вашему аккаунт-менеджеру.

Совместимость версий Kaspersky Endpoint Agent для Windows с другими программами

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

Совместимость Kaspersky Endpoint Agent 3.8 и 3.9 для Windows с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent версий 3.8 и 3.9 совместимо со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center версий 11, 12 и выше.
- Kaspersky Sandbox 1.0.

Совместимость Kaspersky Endpoint Agent 3.8 и 3.9 для Windows с антивирусными программами других производителей

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

- Symantec™ Endpoint Protection.
- Sophos Endpoint Protection.

- ESET NOD32 Business Edition Smart Security.
- Bitdefender® GravityZone® Advanced Business Security.
- McAfee® Endpoint Security 10.6.1.
- McAfee Endpoint Security 10.7.

Если на компьютере одновременно установлены несколько антивирусных программ других производителей, корректная работа программы Kaspersky Endpoint Agent не гарантируется.

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

Совместимость Kaspersky Endpoint Agent 3.10 для Windows с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.10 поддерживает интеграцию со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center версий 11 и 12.1.
- Kaspersky Sandbox 1.0.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Совместимость Kaspersky Endpoint Agent 3.10 для Windows с антивирусными программами других производителей

На компьютерах, на которые вы хотите установить программу Kaspersky Endpoint Agent 3.10, может быть установлена антивирусная программа Bitdefender GravityZone Advanced Business Security.

Совместимость Kaspersky Endpoint Agent 3.11 для Windows с другими программами "Лаборатории Касперского"

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

- Kaspersky Security Center версий 10.5, 11, 12.1, 13 и выше.
- Kaspersky Sandbox 1.0.

- Kaspersky Endpoint Detection and Response Optimum 1.0.
- Kaspersky Industrial CyberSecurity for Networks 3.0.

Совместимость Kaspersky Endpoint Agent 3.11 для Windows с антивирусными программами других производителей

На компьютерах, на которые вы хотите установить программу Kaspersky Endpoint Agent 3.11, может быть установлена антивирусная программа Bitdefender GravityZone Advanced Business Security.

Совместимость Kaspersky Endpoint Agent 3.12 для Windows с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.12 поддерживает интеграцию со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center версий 13, 13.1 и 13.2.
- Kaspersky Security Center Cloud Console.
- Kaspersky Sandbox 1.0.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Совместимость Kaspersky Endpoint Agent 3.13, 3.14 для Windows с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent версий 3.13, 3.14 поддерживает интеграцию со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center версий 13, 13.1, 13.2 и 14.
- Kaspersky Sandbox 2.0.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Требования к Kaspersky Endpoint Agent для Linux

В этом разделе описываются аппаратные и программные требования для Kaspersky Endpoint Agent 3.12 для Linux.

Программные требования к компьютерам для установки программы Kaspersky Endpoint Agent 3.12 для Linux

Для работы программы Kaspersky Endpoint Agent 3.12 на компьютерах должны быть установлена одна из следующих операционных систем:

- Ubuntu® 16.04 LTS и выше.
- Ubuntu 18.04 LTS и выше.
- Ubuntu 20.04 LTS.
- Red Hat® Enterprise Linux® 7.2 и выше.
- Red Hat Enterprise Linux 8.0 и выше.
- CentOS 7.2 и выше.
- CentOS 8.0 и выше.
- Debian GNU / Linux 9.4 и выше.
- Debian GNU / Linux 10.1 и выше.
- Debian GNU / Linux 11 и выше.
- Oracle® Linux 7.3 и выше.
- Oracle Linux 8 и выше.
- SUSE Linux Enterprise Server 12 и выше.
- SUSE Linux Enterprise Server 15.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
- Astra Linux Common Edition (очередное обновление 2.12).
- Альт 8 СП Сервер.
- Альт Сервер 9.
- Альт Рабочая станция 9.
- Гослинукс 7.17.
- РЕД ОС 7.3.

Аппаратные требования к компьютерам для установки программы Kaspersky Endpoint Agent 3.12 для Linux

Минимальные аппаратные требования:

- Процессор: 2 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Необходимое программное обеспечение

Для работы Kaspersky Endpoint Agent для Linux необходима программа Linux Audit Daemon 2.8 или выше. Устанавливается на хосты с Kaspersky Endpoint Agent.

Совместимость программы Kaspersky Endpoint Agent 3.12 для Linux с программами EPP "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.12 поддерживает интеграцию с Kaspersky Endpoint Security для Linux: 11.1, 11.2.

Совместимость программы Kaspersky Endpoint Agent 3.12 для Linux с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.12 поддерживает интеграцию со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center версий 13, 13.2.
- Плагин управления Kaspersky Endpoint Agent версии 3.10, 3.11, 3.12.
- Веб-плагин Kaspersky Endpoint Agent версии 3.10, 3.11, 3.12.

Совместимость версий Kaspersky Endpoint Agent для Linux с версиями Kaspersky Anti Targeted Attack Platform

Информация о совместимости версий программы Kaspersky Endpoint Agent с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Совместимость версий Kaspersky Endpoint Agent для Linux с версиями Kaspersky Anti Targeted Attack Platform

Версия Endpoint Agent	Тип Endpoint Agent	Совместимость с KATA 3.6.1	Совместимость с KATA 3.7, 3.7.1	Совместимость с KATA 3.7.2	Совместимость с KATA 4.0	Совместимость с KATA 4.1, 5.0
Endpoint Agent 3.9	Устанавливается отдельно или в составе KES версии 11.1	Нет	Нет	Да	Да	Нет
Endpoint Agent 3.12	Устанавливается отдельно	Нет	Нет	Да	Да	Да

Совместимость версий Kaspersky Endpoint Agent для Linux с программами EPP

Вы можете использовать только программу Kaspersky Endpoint Agent или настроить интеграцию Kaspersky Endpoint Agent с программой защиты рабочих станций (Endpoint Protection Platform, далее также "EPP") Kaspersky Endpoint Security для Linux. Если интеграция настроена, Kaspersky Endpoint Agent будет также передавать на сервер Central Node данные об угрозах, обнаруженных этой программой, и о результатах их обработки.

Версии Kaspersky Endpoint Agent 3.9 и 3.12 совместимы со следующими версиями Kaspersky Endpoint Security для Linux: 11.1, 11.2.

Подробнее об установке Kaspersky Endpoint Security см. в *справке Kaspersky Endpoint Security для Linux*.

Совместимость версий Kaspersky Endpoint Agent для Linux с другими программами

Совместимость программы Kaspersky Endpoint Agent 3.9 для Linux с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.9 поддерживает интеграцию со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center версий 12.1 и 12.2.
- Плагин управления Kaspersky Endpoint Agent версии 3.10.
- Веб-плагин Kaspersky Endpoint Agent версии 3.10.

Совместимость программы Kaspersky Endpoint Agent 3.12 для Linux с другими программами "Лаборатории Касперского"

Программа Kaspersky Endpoint Agent 3.12 поддерживает интеграцию со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center версий 13, 13.2.
- Плагин управления Kaspersky Endpoint Agent версии 3.10, 3.11, 3.12.
- Веб-плагин Kaspersky Endpoint Agent версии 3.10, 3.11, 3.12.

Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform

Вы можете использовать Kaspersky Endpoint Security в качестве компонента Endpoint Agent.

Информация о совместимости версий Kaspersky Endpoint Security с версиями Kaspersky Anti Targeted Attack Platform приведена в таблице ниже.

Совместимость версий Kaspersky Endpoint Security для Windows с версиями Kaspersky Anti Targeted Attack Platform

Версия Kaspersky Endpoint Security	Совместимость с KATA 3.7	Совместимость с KATA 3.7.1	Совместимость с KATA 3.7.2	Совместимость с KATA 4.0	Совместимость с KATA 4.1	Совместимость с KATA 5.0
Kaspersky Endpoint Security 12.1	Нет	Нет	Нет	Нет	Да	Да
Kaspersky Endpoint Security 12.2	Нет	Нет	Нет	Нет	Да	Да

Для интеграции Kaspersky Endpoint Security 12.1 и выше с Kaspersky Anti Targeted Attack Platform не требуется устанавливать Kaspersky Endpoint Agent.

Ограничения текущей версии программы

В Kaspersky Anti Targeted Attack Platform версии 5.0 известны следующие ограничения:

1. При обновлении программы до версии 5.0 устанавливается неотказоустойчивая версия программы. Данные программы в процессе обновления сохраняются.

2. Для обновления компонента Central Node на сервере с этим компонентом требуется предварительно запустить скрипт. Скрипт входит в комплект поставки программы.

3. Если компонент Central Node установлен на виртуальном сервере, перед обновлением программы вам нужно убедиться, что для виртуальной машины выбран режим загрузки BIOS. Если для виртуальной машины выбран режим загрузки EFI, при установке обновления произойдет ошибка.

Ограничения, действующие при развертывании компонента Central Node:

Пароль для учетной записи локального администратора предустановлен. Вы можете изменить пароль в веб-интерфейсе программы.

Ограничения, действующие при развертывании компонента Central Node в виде кластера:

1. Кластер Central Node должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. Вы можете масштабировать кластер для увеличения количества обрабатываемого трафика или количества подключенных хостов в соответствии с Руководством по масштабированию.

2. Рекомендуется добавлять в кластер серверы с одинаковой аппаратной конфигурацией. В противном случае пропорциональное увеличение производительности не гарантируется.

3. Добавление в кластер дополнительного сервера не ускоряет обработку объектов, которые уже находятся в очереди на проверку.

4. Веб-интерфейс программы может быть недоступен некоторое время при отказе сервера, на котором он расположен.

5. При отказе обрабатывающего сервера возможна потеря полученных по протоколам ICAP, POP3 и SMTP данных трафика и копий сообщений электронной почты, которые ждут обработки, и обнаружений, связанных с ними.

6. Если для обрабатывающего сервера настроено получение зеркалированного трафика со SPAN-портов, то при выходе из строя этого сервера SPAN-трафик не обрабатывается.

7. Возможна временная рассинхронизация данных в базе событий при отказе одного из серверов кластера или временной потере связи между сервером и программой Kaspersky Endpoint Agent.

8. При изменении конфигурации серверов кластера возможно временное замедление обработки трафика и событий с хостов с Kaspersky Endpoint Agent.

Ограничения, действующие для компонента Sandbox:

Если набор операционных систем, установленных на сервере Sandbox, не совпадает с набором, выбранным на сервере Central Node, Kaspersky Anti Targeted Attack Platform не отправляет объекты на проверку серверу Sandbox. При подключении к серверу Central Node нескольких серверов Sandbox программа отправляет объекты на проверку тем серверам Sandbox, на которых установлены операционные системы, соответствующие выбранному на Central Node набору.

Ограничения программы, действующие при интеграции с Kaspersky Endpoint Agent для Windows:

1. Задачи получения дампа оперативной памяти и образа диска могут быть назначены только на хосты с программой Kaspersky Endpoint Agent для Windows версии 3.14.

2. Задачи получения дампа памяти процесса, метафайлов NTFS и ключа реестра могут быть назначены только на хосты с программой Kaspersky Endpoint Agent для Windows версии 3.13 и выше.

3. Задача проверки хостов с помощью правил YARA может быть назначена только на хосты с программой Kaspersky Endpoint Agent для Windows версии 3.12 и выше. При одновременном назначении задачи на хосты с Kaspersky Endpoint Agent 3.12 и выше, а также на хосты с более ранними версиями программы задача выполняется только на хостах с Kaspersky Endpoint Agent 3.12 и выше.

   Если в качестве области проверки выбраны точки автозапуска, задача выполняется только на хостах с Kaspersky Endpoint Agent 3.13 и выше.

Ограничения программы, действующие при интеграции с Kaspersky Endpoint Agent 3.12 для Linux:

1. Для хостов с установленной программой Kaspersky Endpoint Agent для Linux недоступны следующие функции:

   - Сетевая изоляция хоста.
   - Создание правил запрета.

     Программа не создает уведомления о неуспешном применении правила запрета на хостах с программой Kaspersky Endpoint Agent для Linux.

   - Поиск индикаторов компрометации на хостах с помощью IOC-файлов.

     Программа не создает уведомления о неуспешном поиске индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent для Linux.

2. В результате поиска угроз по базе событий по критерию **OSVersion** отображаются только хосты с программой Kaspersky Endpoint Agent для Linux. Хосты с программой Kaspersky Endpoint Agent для Windows в результате поиска не отображаются.

3. Поле **Версия ОС** в информации о событии заполняется только для событий, записанных в базу событий Kaspersky Endpoint Agent для Linux. В информации о событиях, записанных в базу событий Kaspersky Endpoint Agent для Windows, поле не заполняется.

4. Список событий, которые Kaspersky Endpoint Agent для Linux записывает в базу событий, ограничен следующими типами:

   - **Изменен файл**;
   - **Запущен процесс**;
   - **Журнал событий ОС**;
   - **Обнаружение**;
   - **Результат обработки обнаружения**.

5. Список задач, которые вы можете создать на хостах с программой Kaspersky Endpoint Agent для Linux, ограничен следующими типами:

   - **Получить файл**.
   - **Выполнить программу**.

     Программа не проверяет на корректность указанный при создании задачи путь к исполняемому файлу или файлу, который вы хотите получить.

6. В информации о событиях, записанных в базу событий программой Kaspersky Endpoint Agent для Linux, в поле **Время создания** отображается время изменения файла.

В Kaspersky Endpoint Agent 3.14 для Windows известны следующие ограничения:

1. Для корректной работы Kaspersky Endpoint Agent необходима поддержка SHA-2 в Windows.

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

3. В Kaspersky Security Center версии 13.2 и выше для установки Kaspersky Endpoint Agent на устройства под управлением Windows XP необходимо использовать стандартный дистрибутив Kaspersky Endpoint Agent версии 3.14, а не инсталляционный пакет, созданный в Kaspersky Security Center.

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

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

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

7. После установки, восстановления, изменения набора компонентов или удаления Kaspersky Endpoint Agent, рекомендуется выполнить перезагрузку операционной системы в ближайшее доступное время, поскольку настройка некоторых параметров программы может быть завершена только в момент запуска операционной системы.

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

9. Компонент запрета открытия документов имеет следующее ограничение: правила блокирования открытия документов не применяются к объектам, которые открываются с использованием OLE-автоматизации.

10. Перед отправкой событий телеметрии на сервер KATA Central Node программа Kaspersky Endpoint Agent сохраняет данные в очередь событий. Если очередь событий превышает 10000 необработанных событий, Kaspersky Endpoint Agent не размещает события в очереди, пока в очереди не появятся места.

11. При работе программы Kaspersky Endpoint Agent на устройствах с операционной системой Windows 7 программа исключает из телеметрии данные о сетевых соединениях, относящихся к процессам с идентификаторами PID=4 и PID=0.

12. Если программа Kaspersky Endpoint Agent используется на одном устройстве с программой Kaspersky Endpoint Security, и в программе Kaspersky Endpoint Security установлен компонент, обеспечивающий файловое шифрование (FLE), программа Kaspersky Endpoint Agent не регистрирует события телеметрии о загрузке модулей (LoadImage) и не отправляет их компоненту KATA Central Node.

13. Если при настройке параметров исключения из сетевой изоляции для критерия *Приложение* указано больше одной программы, Kaspersky Endpoint Agent разрешит подключение только для первой программы из списка. Сетевые подключения для остальных указанных программ будут проигнорированы. Ограничение воспроизводится при изоляции устройств, работающих под управлением операционных систем Windows 7 и Windows Server 2008 R2.

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

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

16. В секциях параметров для управления доступом на основе ролей (RBAC) в Консоли администрирования, в разделе с правами управления плагином Kaspersky Endpoint Agent отображаются флажки, соответствующие правам "Чтение" и "Выполнение операций с выборками устройств", которые не применяются к блокам параметров в Kaspersky Security Center. Если вы установите эти флажки, права "Чтение" и "Выполнение операций с выборками устройств" не будут ограничены для указанных пользователей.

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

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

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

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

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

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

19. После установки, восстановления, изменения набора компонентов или удаления Kaspersky Endpoint Agent, рекомендуется выполнить перезагрузку операционной системы в ближайшее доступное время, поскольку настройка некоторых параметров программы может быть завершена только в момент запуска операционной системы.

20. Если при запуске групповых задач выставлено расписание запуска **При запуске программы**, в истории выполнения задачи статус выполнения задачи обновляется с отсрочкой. По этой причине в некоторых случаях в истории выполнения задачи не будут отображаться статусы выполнения задачи.

21. Если операционная система активирована по корпоративной лицензии (Volume License), то после установки Kaspersky Endpoint Agent из-за установки сетевых драйверов программы может потребоваться повторная активация операционной системы.

22. В операционных системах Windows XP и Windows Vista в событиях телеметрии, отправляемых на сервер сбора телеметрии, может отсутствовать некоторая информация о файлах. Это связано с тем, что возможность получения некоторой информации о файлах появилась в более поздних версиях операционных систем MS Windows.

В Kaspersky Endpoint Agent 3.12 для Linux известны следующие ограничения:

1. Kaspersky Endpoint Agent для Linux не поддерживает работу с системами принудительного контроля доступа AppArmor и SELinux в блокирующем режиме работы этих систем. Для корректной работы программы данные системы должны быть переведены в разрешающий режим работы.

2. Для работы Kaspersky Endpoint Agent для Linux на устройствах должен быть установлен компонент Linux Audit Daemon версии 2.8 или выше.

3. Для связи Kaspersky Endpoint Agent для Linux с программой Kaspersky Endpoint Security для Linux используется сервис rsyslog с загруженным модулем imuxsock. Чтобы проверить, загружен ли модуль imuxsock в конфигурации сервиса rsyslog, запустите следующую команду: grep -r imuxsock /etc/rsyslog*. Если строка загрузки модуля закомментирована, удалите знак комментирования # в начале строки и перезапустите сервис rsyslog для сохранения изменений.

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". Данные передаются по зашифрованным каналам связи.

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.

Служебные данные программы

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.

К служебным данным Kaspersky Anti Targeted Attack Platform относятся:

- Данные об учетных записях пользователей.
- Данные о подключенных к компоненту Central Node компьютерах, на которых установлена программа Kaspersky Endpoint Agent.
- Данные о предустановках и правилах запрета.
- Данные о задачах, назначенных на компьютеры с программой Kaspersky Endpoint Agent.
- Данные о пользовательских правилах TAA (IOA).
- Данные о пользовательских правилах IDS.
- Данные о пользовательских правилах IOC.
- Данные о правилах сетевой изоляции.
- Данные об исключениях из проверки.
- Данные о шаблонах отчетов.
- Данные о сертификатах Kaspersky Endpoint Agent.

  Указанные выше данные хранятся бессрочно на сервере с компонентом Central Node в директории `/data`, если компонент Central Node установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.
- Журнал событий ОС.

  Файлы журнала ОС хранятся бессрочно в директории `/var/log` на сервере с компонентом Central Node.
- Журнал с информацией о работе программы.

  Файл журнала хранится бессрочно в директории `data/` на сервере с компонентом Central Node, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.
- Очередь файлов на проверку.

  Файлы хранятся на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные хранятся до выполнения проверки.
- Файлы, полученные с компьютеров с Kaspersky Endpoint Agent.

  Файлы хранятся на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.
- Файлы с правилами YARA и IDS (пользовательские и от "Лаборатории Касперского").

  Файлы хранятся бессрочно в директории `data/` на сервере с компонентом Central Node, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.

- Файлы с данными о переданных во внешние системы обнаружениях.

  Файлы хранятся бессрочно на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных бессрочно.

- Артефакты компонента Sandbox.

  Файлы хранятся на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.

- Файлы, для которых были созданы обнаружения компонентом Sandbox.

  Файлы хранятся на сервере с компонентом Central Node в директории `/data`, если компонент установлен на сервере. При установке компонента Central Node на кластер данные хранятся на серверах хранения данных. Данные ротируются при заполнении места на диске.

- Файлы сертификатов, которые используются для аутентификации компонентов программы.

  Файлы хранятся бессрочно в директории /var/log на сервере с компонентом Central Node, PCN, SCN, Sensor или на компьютере с Kaspersky Endpoint Agent.

- Ключи шифрования, которые передаются между компонентами программы.

  Файлы хранятся бессрочно в директории /var/log на сервере с компонентом Central Node, PCN, SCN, Sensor или на компьютере с Kaspersky Endpoint Agent.

Программа хранит об учетных записях пользователей следующую информацию:

- Идентификатор учетной записи.
- Имя учетной записи.
- Хеш и соль пароля учетной записи.
- Доменное имя пользователя.
- Роль учетной записи.
- Статус учетной записи.
- Права доступа к тенантам в режиме распределенного решения и мультитенантности.
- Идентификатор тенанта в режиме распределенного решения и мультитенантности.

Программа хранит о подключенных к компоненту Central Node компьютерах, на которых установлена программа Kaspersky Endpoint Agent, следующую информацию:

- Идентификатор компьютера, присвоенный Kaspersky Security Center.
- Имя компьютера.
- IP-адрес компьютера.
- Операционная система, используемая на компьютере.
- Версия Kaspersky Endpoint Agent.

- Статус механизма самозащиты.
- Дата и время отправки первого и последнего пакета телеметрии, отправленного компоненту Central Node.
- Дата и время последней запущенной IOC-проверки.
- Результат последней запущенной IOC-проверки.

Программа хранит о правилах запрета следующую информацию:

- MD5- или SHA256-хеш файла, запрещенного для запуска.
- Имя учетной записи пользователя, создавшего правило запрета.
- Имя учетной записи пользователя, изменившего правило запрета.
- Список компьютеров, на которых запрещен запуск файла.
- Журнал изменений правил запрета.

Программа хранит о задачах, назначенных на компьютеры с программой Kaspersky Endpoint Agent, следующую информацию:

- Тип задачи.
- Имя компьютера.
- IP-адрес компьютера.
- Дата и время создания задачи.
- Срок действия задачи.
- Имя учетной записи пользователя, создавшего задачу.
- Данные параметров задачи.
- Данные отчета о выполнении задачи.
- Комментарий к задаче.

Программа хранит о пользовательских правилах TAA (IOA) следующую информацию:

- Имя правила.
- Исходный код запроса, по которому осуществляется проверка.
- Идентификатор правила.
- Статус правила.
- Дата и время создания правила.

- Важность, указанная при добавлении правила.
- Уровень надежности в зависимости от вероятности ложных срабатываний, заданный при добавлении правила.

Программа хранит о пользовательских правилах IDS следующую информацию:

- Имя учетной записи пользователя, загрузившего файл с правилами.

Программа хранит о пользовательских правилах IOC следующую информацию:

- Имя учетной записи пользователя, загрузившего файл с правилами.
- Имя IOC-файла.
- Содержимое IOC-файла.

Программа хранит о правилах сетевой изоляции следующую информацию:

- Имя учетной записи пользователя, включившего сетевую изоляцию.
- Идентификатор изолированного компьютера.
- Имя правила.
- Статус правила.
- Список ресурсов, исключенных из сетевой изоляции.

Программа хранит об исключениях из проверки следующую информацию:

- Имя учетной записи пользователя, добавившего исключение.
- Список объектов, исключенных из проверки.
- Идентификатор правила исключения.

Программа хранит о шаблонах отчетов следующую информацию:

- Идентификатор учетной записи пользователя, создавшего или изменившего шаблон.
- Дата создания шаблона.
- Дата последнего изменения шаблона.
- Текст шаблона в виде HTML-кода.

Программа хранит о сертификатах Kaspersky Endpoint Agent следующую информацию:

- Имя учетной записи пользователя, загрузившего файл сертификата.
- Дайджест сертификата.
- Серийный номер сертификата.
- Публичный ключ.

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 трафика компонента Sensor

Данные трафика компонента Sensor хранятся на сервере с компонентом Sensor или на сервере с компонентами Sensor и Central Node, если Sensor и Central Node установлены на одном сервере.

Данные трафика записываются и хранятся в последовательно создаваемых файлах. Программа перестает записывать данные в один файл и начинает записывать в следующий файл в следующих случаях:

- при достижении максимального размера файла (вы можете настроить этот параметр);
- по окончании заданного в настройках промежутка времени (вы можете настроить этот параметр);
- при перезагрузке службы сохранения трафика или всей программы Kaspersky Anti Targeted Attack Platform.

По мере накопления данных трафика, Kaspersky Anti Targeted Attack Platform фильтрует данные и оставляет только следующую информацию:

- информацию, связанную с обнаружениями, выполненными технологией Targeted Attack Analyzer;
- PCAP-файлы, в которых:
  - IP-адрес источника или назначения совпадают каким-либо IP-адресом из обнаружения;
  - данные трафика относятся ко времени, отстоящему от времени обнаружения не более, чем на 15 минут.

Отфильтрованные данные трафика переносятся в отдельный раздел. Все остальные данные трафика (не отвечающие условиям фильтрации), удаляются.

Данные отфильтрованного трафика сохраняются в последовательно создаваемых файлах. Программа перестает записывать данные в один файл и начинает записывать в следующий файл в следующих случаях:

- при достижении максимального размера файла;
- по окончании заданного в настройках промежутка времени.

Данные отфильтрованного трафика хранятся за последние сутки. Более старые данные удаляются.

Данные в обнаружениях

Данные пользователя могут содержаться в обнаружениях. Если компонент Central Node установлен на сервере, информация об обнаружениях и файлы, по результатам проверки которых возникло обнаружение, хранятся на сервере с компонентом Central Node в директории `/data`. При установке компонента Central Node на кластер информация об обнаружениях и файлы, по результатам проверки которых возникло обнаружение, хранятся на серверах хранения данных.

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.
- Категория обнаруженного объекта.
- Имя обнаруженного файла.
- Обнаруженный URL-адрес.
- MD5- , SHA256-хеш обнаруженного файла.
- Комментарии пользователя, добавленные в информацию об обнаружении.
- Идентификатор правила TAA, по которому было выполнено обнаружение.
- IP-адрес и имя компьютера, на котором выполнено обнаружение.
- Идентификатор компьютера, на котором выполнено обнаружение.

При изменении обнаружения на сервере хранится следующая информация:

- Учетная запись пользователя, который изменил обнаружение.
- Учетная запись пользователя, которому было назначено обнаружение.
- Дата и время изменения обнаружения.

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

- Адреса электронной почты отправителя и получателей сообщения, копии и скрытой копии сообщения.
- Тема сообщения электронной почты.

- Дата и время поступления сообщения в Kaspersky Anti Targeted Attack Platform, с точностью до секунд.
- Все служебные заголовки сообщения (так, как они выглядят в сообщении).

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

- Имя компьютера, с которого были отправлены данные.
- Имя компьютера, получившего данные.
- IP-адрес компьютера, с которого были отправлены данные.
- IP-адрес компьютера, получившего данные.
- URI переданного ресурса.
- 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:

- Имя компьютера, с которого были отправлены данные.
- Имя компьютера, получившего данные.
- IP-адрес компьютера, с которого были отправлены данные.
- IP-адрес компьютера, получившего данные.
- Переданные данные.
- Время передачи данных.
- URL-адрес, извлеченный из файла с трафиком, User Agent, метод.
- Файл с трафиком, в котором произошло обнаружение.

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

- Версия правил YARA, с помощью которых было выполнено обнаружение.
- Категория обнаруженного объекта.
- Имя обнаруженного объекта.
- MD5-хеш обнаруженного объекта.

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

- Версия баз программы, с помощью которых было выполнено обнаружение.
- Категория обнаруженного объекта.
- Имена обнаруженных объектов.
- MD5-хеши обнаруженных объектов.
- Информация об обнаруженных объектах.

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

- Дата и время выполнения проверки.
- Идентификаторы компьютеров, на которых выполнено обнаружение.
- Имя правила TAA (IOA).
- Имя IOC-файла.
- Информация об обнаруженных объектах.

Если обнаружение выполнено выполнено технологией Anti-Malware Engine, на сервере может храниться следующая информация:

- Версии баз компонентов Kaspersky Anti Targeted Attack Platform, с помощью которых было выполнено обнаружение.
- Категория обнаруженного объекта.
- Список обнаруженных объектов.
- MD5-хеш обнаруженных объектов.
- Дополнительная информация об обнаружении.

Данные в событиях

Данные пользователя могут содержаться в событиях. Если компонент Central Node установлен на сервере, информация о произошедших событиях хранится на сервере с компонентом в директории `/data`. При установке компонента Central Node на кластер информация хранится на серверах хранения данных.

Данные ротируются по мере заполнения диска.

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.
- Уникальный идентификатор компьютера с Kaspersky Endpoint Agent.
- Имя пользователя, под учетной записью которого произошло событие.
- Имя группы, в которую входит пользователь.
- Тип события.
- Время события.
- Информация о файле, для которого записано событие: имя, путь, полное имя.
- MD5- и SHA256-хеш файла.
- Время создания файла.
- Время изменения файла.
- Флаги прав доступа к файлу.
- Переменные окружения процесса.
- Параметры командной строки.
- Текст команды, введенный в командную строку.
- 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.
- Протокол сетевого соединения.
- Метод HTTP-запроса.
- Заголовок HTTP-запроса.
- Информация о переменных реестра Windows: путь к переменной, имя переменной, значение переменной.
- Содержание скрипта или двоичного файла, переданного на AMSI-проверку.
- 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.

Данные в отчетах

Данные пользователя могут содержаться в отчетах. Если компонент Central Node установлен на сервере, информация о произошедших событиях хранится на сервере с компонентом в директории `/data` бессрочно. При установке компонента Central Node на кластер информация хранится на серверах хранения данных.

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.
- Идентификатор учетной записи пользователя, сформировавшего отчет.
- Статус отчета.
- Текст отчета в виде HTML-кода.

Данные об объектах в Хранилище и на карантине

Объекты в Хранилище и на карантине могут содержать данные пользователя. Информация об объектах в Хранилище и о копиях объектов, помещенных на карантин на компьютерах с Kaspersky Endpoint Agent, сохраненных на сервере с помощью задачи **Получить файл**, хранится на сервере с компонентом Central Node в директории /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 и на карантине могут содержать следующую информацию:

- Имя объекта.
- Путь к объекту на компьютере с Kaspersky Endpoint Agent.
- MD5-, SHA256-хеш файла.
- Идентификатор пользователя, поместившего объект на карантин на компьютере с Kaspersky Endpoint Agent.
- Идентификатор пользователя, поместившего объект в Хранилище.
- IP-адрес компьютера, на котором хранится объект, помещенный на карантин.
- Имя компьютера, на котором хранится объект, помещенный на карантин.
- Уникальный идентификатор компьютера, на котором хранится объект, помещенный на карантин.
- Идентификатор правила TAA (IOA), по которому было выполнено обнаружение.
- Категория обнаруженного объекта.
- Результаты проверки объекта с помощью отдельных модулей и технологий программы.

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.

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 Kaspersky Endpoint Agent для Windows

Программа Kaspersky Endpoint Agent для Windows отправляет на компонент Central Node отчеты о выполнении задач, информацию о событиях и обнаружениях, произошедших на компьютерах с Kaspersky Endpoint Agent для Windows, 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 программа Kaspersky Endpoint Agent для Windows не будет удалена с компьютера, но не более 21 дня.

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

1. Общие сведения для всех событий:
   - Тип события.
   - Время события.
   - Учетная запись пользователя, от имени которой было совершено событие.
   - Имя хоста, на котором произошло событие.
   - IP-адрес хоста.
   - Тип операционной системы, установленной на хосте.
2. 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.
3. Событие мониторинга реестра.
   - Сведения о процессе, изменившем реестр: ID процесса, имя файла процесса, MD5-, SHA256-хеш файла процесса.
   - Путь к ключу реестра.
   - Имя параметра реестра.
   - Значение параметра реестра.
   - Тип параметра реестра.
   - Предыдущий путь к ключу реестра.
   - Предыдущее значение параметра реестра.
   - Предыдущий тип параметра реестра.

4. Событие загрузки драйвера.

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

5. 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.

6. Событие в журнале ОС.

- 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.

- 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.

7. Событие запуска процесса.

- Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, дата создания и изменения файла, имя организации, выпустившей цифровой сертификат файла, результат проверки цифровой подписи файла.

- UniquePID.

- Параметры запуска процесса.

- Время запуска процесса.

- Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, параметры запуска процесса.

8. Событие остановки процесса

- Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла, время завершения процесса.

- UniquePID.

- Параметры запуска процесса.

- Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, параметры запуска процесса.

9. Событие загрузки модуля.

- Сведения о файле, загрузившем модуль: UniquePID, имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла.

- Имя DLL.

- Путь к DLL.

- Полное имя DLL.
- MD5-, SHA256-хеш DLL.
- Размер DLL.
- Дата создания и изменения DLL.
- Имя организации, выпустившей цифровой сертификат DLL.
- Результат проверки цифровой подписи DLL.

10. 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.

11. 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.

12. Событие программы Kaspersky Endpoint Security для Windows.

    - 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.
- Содержание скрипта, проверенного с помощью AMSI.

13. Событие AMSI-проверки.
    - Содержание скрипта, проверенного с помощью AMSI.

Central Node и Kaspersky Endpoint Agent для Linux

Программа Kaspersky Endpoint Agent для Linux отправляет на компонент Central Node отчеты о выполнении задач, информацию о событиях и обнаружениях, произошедших на компьютерах с Kaspersky Endpoint Agent для Linux, 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 программа Kaspersky Endpoint Agent для Linux не будет удалена с компьютера, но не более 21 дня.

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

1. Общие сведения для всех событий:
    - Тип события.
    - Время события.
    - Учетная запись пользователя, от имени которой было совершено событие.
    - Имя хоста, на котором произошло событие.
    - IP-адрес хоста.
    - Тип и версия операционной системы, установленной на хосте.
    - Имя хоста, с которого был совершен удаленный вход в систему.
    - Имя пользователя, назначенное при регистрации в системе.
    - Группа, к которой принадлежит пользователь.
    - Имя пользователя, которое использовалось для входа в систему.
    - Группа, к которой принадлежит пользователь, чье имя использовалось для входа в систему.
    - Имя пользователя, создавшего файл.
    - Название группы, пользователи которой могут изменить или удалить файл.

- Разрешения, которые могут использоваться для доступа к файлу.
- Наследуемые привилегии файла.

2. Событие запуска процесса.

- Сведения о файле процесса: имя файла, путь к файлу, полное имя файла, MD5-, SHA256-хеш файла, размер файла.
- UniquePID.
- Команда, с помощью которой был запущен процесс.
- Тип процесса.
- Переменные окружения процесса.
- Время запуска процесса.
- Время завершения процесса.
- Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, команда, с помощью которой был запущен процесс.

3. Событие создания файла.

- Сведения о процессе, создавшем файл: имя файла процесса, MD5-, SHA256-хеш файла процесса.
- Имя файла.
- Путь к файлу.
- Полное имя файла.
- Тип файла.
- MD5-, SHA256-хеш файла.
- Дата создания и изменения файла.
- Размер файла.

4. Событие в журнале ОС.

- Время события.
- Тип события.
- Результат операции.
- Сведения о родительском процессе: путь к файлу, UniquePID, MD5-, SHA256-хеш файла процесса, команда, с помощью которой был запущен процесс.

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.
- Список данных, исключенных из проверки.
- Данные программы Endpoint Sensors, если настроена интеграция с прокси-сервером.
- Базы программы, если настроено получение обновления баз от компонента Central Node.

Серверы с ролями PCN и SCN

Если программа работает в режиме распределенного решения, то между PCN и подключенными SCN передаются следующие данные:

- Об обнаружениях.
- О событиях.
- О задачах.
- О политиках.
- О проверке по пользовательским правилам IOC, TAA (IOA), IDS, YARA.
- О файлах в Хранилище.
- Об учетных записях пользователей.
- О лицензии.
- Список компьютеров с Kaspersky Endpoint Agent.
- Объекты, помещенные в Хранилище.

- Объекты, помещенные на карантин на компьютерах с Kaspersky Endpoint Agent.
- Файлы, прикрепленные к обнаружениям.
- IOC- и YARA-файлы.

Данные в файлах трассировки программы

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 файлы трассировки могут попасть любые персональные данные пользователя или конфиденциальные данные вашей организации. Файлы хранятся в директории `/data/var/log/kaspersky` бессрочно.

Данные Kaspersky Endpoint Agent для Windows

Программа Kaspersky Endpoint Agent для Windows хранит и обрабатывает данные локально для обеспечения основной функциональности, аудита и повышения скорости решения возникших проблем специалистами Службы технической поддержки "Лаборатории Касперского".

На компьютерах с Kaspersky Endpoint Agent для Windows хранятся данные, подготовленные для отправки на серверы Kaspersky Anti Targeted Attack Platform и в Kaspersky Security Center в автоматическом режиме.

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

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

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

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

Не используйте программу Kaspersky Endpoint Agent для Windows на тех компьютерах, передача данных с которых запрещена политикой вашей организации.

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

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

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

Файлы, зашифрованные на компьютерах с Kaspersky Endpoint Agent для Windows 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 Kaspersky Endpoint Agent для Windows, 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 Kaspersky Endpoint Agent для Windows 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 Kaspersky Endpoint Agent для Windows:

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

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

Данные, получаемые от компонента Central Node

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

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

Данные удаляются при удалении программы Kaspersky Endpoint Agent.

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

- О сетевых соединениях.
- Об операционной системе, установленной на сервере с компонентом Central Node.
- Об учетных записях пользователей операционной системы.
- О пользовательских сессиях в операционной системе.
- О журнале событий Windows.
- О ресурсе типа RT_VERSION.
- О содержимом PE-файла.
- О службах операционной системы.
- Сертификат сервера с компонентом Central Node.
- URL- и IP-адреса посещенных веб-сайтов.
- Заголовки протокола HTTP.
- Имя компьютера.
- MD5-хеши файлов.
- Уникальный идентификатор компьютера с Kaspersky Endpoint Agent.
- Имена и значения ключей реестра Windows.
- Пути к ключам реестра Windows.
- Имена переменных реестра Windows.
- Имя записи локального DNS-кеша.
- Адрес из записи локального DNS-кеша в формате IPv4.
- IP-адрес или имя запрашиваемого хоста из локального DNS-кеша.
- Хост элемента локального DNS-кеша.
- Доменное имя элемента локального DNS-кеша.
- Адрес элемента ARP-кеша в формате IPv4.
- Физический адрес элемента APR-кеша.
- Серийный номер логического диска.
- Домашняя директория локального пользователя.

- Имя учетной записи пользователя, запустившего процесс.
- Путь к скрипту, запускаемому при входе пользователя в систему.
- Имя пользователя, под учетной записью которого произошло событие.
- Имя компьютера, на котором произошло событие.
- Полные пути к файлам компьютеров с Kaspersky Endpoint Agent.
- Имена файлов компьютеров с Kaspersky Endpoint Agent.
- Маски файлов компьютеров с Kaspersky Endpoint Agent.
- Полные имена папок компьютеров с Kaspersky Endpoint Agent.
- Комментарии поставщика файла.
- Маска файла-образа процесса.
- Путь к файлу-образу процесса, открывшего порт.
- Имя процесса, открывшего порт.
- Локальный IP-адрес порта.
- Доверенный публичный ключ цифровой подписи исполняемых модулей.
- Имя процесса.
- Имя сегмента процесса.
- Параметры командной строки.

Данные в полях событий Windows Event Log программы Kaspersky Endpoint Agent

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

Эти данные могут автоматически передаваться в Kaspersky Security Center.

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

Данные о событиях могут содержать следующую информацию:

- О пользовательских сессиях в операционной системе.
- Об учетных записях пользователей операционной системы (userID).

- Об ошибках выполнения задач проверки объектов.
- О задачах на проверку объектов.
- Об обнаружениях Kaspersky Sandbox.
- О событиях Kaspersky Sandbox.
- Об IOC-файлах Kaspersky Endpoint Agent, сформированных при автоматическом реагировании.
- О результатах проверки объектов.
- О сертификатах серверов Kaspersky Sandbox.
- Об очереди объектов на проверку.
- Об изменении параметров Kaspersky Endpoint Agent.
- Об изменении политик Kaspersky Security Center.
- Об изменении статуса задачи на проверку объектов.
- О политиках Kaspersky Security Center.
- Об объектах на карантине.
- О действиях по автоматическому реагированию на обнаруженные угрозы.
- Об ошибках взаимодействия с серверами программы.
- Об объектах, заблокированных по правилам запрета.
- О результатах выполнения задач **Удалить файл**.
- О результатах выполнения задач **Завершить процесс**.
- О результатах выполнения задач **Выполнить программу**.
- О результатах выполнения задач **Получить файл**.
- О действующей лицензии Kaspersky Endpoint Detection and Response Optimum.
- О статусе активации программы.

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

Данные в запросах Kaspersky Endpoint Agent для Windows к Kaspersky Anti Targeted Attack Platform

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

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

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

1. В запросах на синхронизацию:
   - уникальный идентификатор Kaspersky Endpoint Agent;
   - базовая часть веб-адреса сервера;
   - имя устройства;
   - IP-адрес устройства;
   - MAC-адрес устройства;
   - локальное время на устройстве;
   - статус самозащиты Kaspersky Endpoint Agent;
   - имя и версия операционной системы, установленной на устройстве;
   - версия Kaspersky Endpoint Agent;
   - версии параметров программы и параметров задач;
   - состояние задач в Kaspersky Endpoint Agent: идентификаторы выполняющихся задач, статусы выполнения, коды ошибок выполнения;
   - состояние параметров Kaspersky Endpoint Agent: тип применяющихся параметров, версия параметров, статус применения параметров, коды ошибок применения.
2. В запросах на получение файлов с сервера:
   - уникальные идентификаторы файлов;
   - уникальный идентификатор Kaspersky Endpoint Agent;
   - уникальные идентификаторы задач;
   - базовая часть веб-адреса сервера с компонентом Central Node;
   - IP-адрес узла.

3. В отчетах о результатах выполнения задач:

- IP-адрес узла;
- информация об объектах, обнаруженных при поиске IOC или сканировании YARA;
- флаги дополнительных действий, выполняемых Kaspersky Endpoint Agent по завершении задач (например, `"deleteFileAfterReboot": false`);
- ошибки выполнения задач и коды возврата;
- статусы, с которыми завершались задачи;
- время завершения выполнения задач;
- версии параметров, с которыми выполнялись задачи;
- информация об объектах, переданных на сервер, помещенных на карантин, восстановленных из карантина: пути к объектам, MD5 и SHA256-хеши объектов, идентификаторы объектов на карантине;
- информация о процессах, запущенных или остановленных на устройстве с Kaspersky Endpoint Agent по запросу сервера: PID и UniquePID, error code, MD5 и SHA256-хеши объектов;
- информация о службах, запущенных или остановленных на устройстве по запросу сервера (имя службы, тип запуска, error code, MD5 и SHA256-хеши файловых образов служб);
- информация об объектах, для которых был снят дамп памяти для сканирования YARA (пути, идентификатор файла дампа);
- файлы, запрошенные сервером;
- пакеты телеметрии.
- Данные о запущенных процессах:
  - имя исполняемого файла, включая полный путь и расширение;
  - параметры автозапуска процесса;
  - идентификатор процесса;
  - код сеанса входа в систему;
  - имя сеанса входа в систему;
  - дата и время запуска процесса;
  - MD5-хеш объекта;
  - SHA256-хеш объекта

- Данные о файлах:
  - путь к файлу;
  - имя файла;
  - размер файла;
  - атрибуты файла;
  - дата и время создания файла;
  - дата и время последнего изменения файла;
  - описание файла;
  - название компании;
  - MD5-хеш объекта;
  - SHA256-хеш объекта;
  - раздел реестра (для точек автозапуска).
- Данные в ошибках получения информации об объектах:
  - полное имя объекта, при обаботке которого возникла ошибка.
  - код ошибки.

1. Данные телеметрии:
   - IP-адрес узла;
   - тип данных в реестре до зафиксированной операции изменения;
   - данные в ключе реестра до зафиксированной операции изменения;
   - текст обрабатываемого скрипта или его части;
   - тип обрабатываемого объекта;
   - способ передачи команды в командный интерпретатор.

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

1. Параметры задач:
   - типы задач;
   - параметры расписания запуска задач;
   - имена и пароли учетных записей, под которыми необходимо запускать задачи;
   - версии параметров;

- идентификаторы объектов на карантине;
- пути к объектам;
- MD5 и SHA256-хеши объектов;
- командная строка запуска процесса с аргументами;
- флаги дополнительных действий, выполняемых Kaspersky Endpoint Agent по завершении задачи;
- идентификаторы IOC-файлов, которые нужно получить с сервера;
- IOC-файлы;
- наименование служб;
- тип запуска служб;
- папки, для которых необходимо получить результаты задачи **Собрать форензику**;
- маски имен объектов и расширений для задачи **Собрать форензику**.

2. Параметры сетевой изоляции:

- типы параметров;
- версии параметров;
- списки исключений из сетевой изоляции и параметры исключений: направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам;
- флаги дополнительных действий, выполняемых Kaspersky Endpoint Agent;
- время автоматического отключения изоляции.

3. Параметры запрета запуска и открытия документов:

- типы параметров;
- версии параметров;
- списки правил запрета запуска и параметры правил: пути к объектам, типы объектов, MD5 и SHA256-хеши объектов;
- флаги дополнительных действий, выполняемых Kaspersky Endpoint Agent.

4. Параметры фильтрации событий:

- имена модулей;
- полные пути к объектам;
- MD5 и SHA256-хеши объектов;
- идентификаторы записей в журнале событий Windows;

- параметры цифровых сертификатов;
- направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам;
- имена пользователей;
- типы входа пользователей;
- типы событий телеметрии, для которых применяются фильтры.

Служебные данные Kaspersky Endpoint Agent для Windows

К служебным данным Kaspersky Endpoint Agent относятся:

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

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

Эти данные могут автоматически передаваться в Kaspersky Security Center.

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

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

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

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent:
   - Пароль доступа к Kaspersky Endpoint Agent.
   - Файлы на карантине.
   - Параметры Kaspersky Endpoint Agent.
   - Учетные данные пользователей операционной системы для запуска задач с правами определенного пользователя.

- Учетные данные для авторизации на Сервере администрирования Kaspersky Security Center.
- Учетные данные для авторизации на прокси-сервере.
- Адреса пользовательских источников обновлений.
- Открытый ключ сертификата для интеграции с Kaspersky Sandbox.

2. Кеш Kaspersky Endpoint Agent:
   - Время записи результата проверки в кеш.
   - MD5-хеш задачи проверки.
   - Идентификатор задачи проверки.
   - Результат проверки объекта.
3. Очередь запросов на проверку объекта:
   - Идентификатор объекта в очереди.
   - Время помещения объекта в очередь.
   - Статус обработки объекта в очереди.
   - Идентификатор пользовательской сессии в операционной системе, в которой создана задача на проверку объекта.
   - Системный идентификатор (SID) пользователя операционной системы, с правами учетной записью которого создана задача на проверку объекта.
   - MD5-хеш задачи на проверку объекта.
4. Информация о задачах, для которых Kaspersky Endpoint Agent ожидает результат проверки от Kaspersky Sandbox:
   - Время получения задачи на проверку объекта.
   - Статус обработки объекта.
   - Идентификатор пользовательской сессии в операционной системе, в которой создана задача на проверку объекта.
   - Идентификатор задачи на проверку объекта.
   - MD5-хеш задачи на проверку объекта.
   - Системный идентификатор (SID) пользователя операционной системы, под учетной записью которого создана задача.
   - XML-схема автоматически созданного IOC.
   - MD5 и SHA256-хеши проверяемого объекта.

- Ошибки обработки.
- Имена объектов, на проверку которых создана задача.
- Результат проверки объекта.

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

1. Обрабатываемые файлы и данные, передаваемые пользователем в ходе настройки параметров Kaspersky Endpoint Agent:
   - Файлы на карантине.
   - Параметры Kaspersky Endpoint Agent:
     - Пароль доступа к Kaspersky Endpoint Agent.
     - Учетные данные пользователей операционной системы для запуска задач с правами определенного пользователя.
     - Учетные данные для авторизации на Сервере администрирования Kaspersky Security Center.
     - Учетные данные для авторизации на прокси-сервере.
     - Адреса пользовательских источников обновлений.
     - Открытый ключ сертификата для интеграции с KATA Central Node.
     - Открытый ключ сертификата для интеграции с Kaspersky Sandbox.
     - Данные о лицензии.
2. Данные, необходимые для интеграции с компонентом KATA Central Node:
   - Обновляемые схемы фильтрации телеметрии.
   - Очередь пакетов событий телеметрии.
   - Кеш идентификаторов IOC-файлов, полученных от компонента KATA Central Node.
   - Объекты для передачи на сервер в рамках задачи **Получить файл**.
   - Отчеты о результатах задачи **Собрать форензику**.

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

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

Данные в файлах трассировки и дампов Kaspersky Endpoint Agent для Windows

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

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

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

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

По умолчанию Kaspersky Endpoint Agent не записывает отладочную информацию.

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

Отладочная информация может понадобиться при обращении в Службу технической поддержки.

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

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

Данные в файлах трассировки и дампов могут содержать следующую информацию:

- Действия, выполненные Kaspersky Endpoint Agent для Windows на хосте.
- Информация об объектах, обрабатываемых Kaspersky Endpoint Agent для Windows.
- Ошибки, возникшие в процессе работы Kaspersky Endpoint Agent для Windows.
- 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 Kaspersky Endpoint Agent для Windows.
- 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 Kaspersky Endpoint Agent для Windows.
- Полное доменное имя компьютера.
- Серийный номер логического диска.
- Заголовки протокола HTTP.
- Полные пути к файлам компьютеров с Kaspersky Endpoint Agent для Windows.
- Имена файлов компьютеров с Kaspersky Endpoint Agent для Windows.
- Полные имена папок компьютеров с Kaspersky Endpoint Agent для Windows.

- 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 службу операционной системы.
- Параметры, с которыми запущена служба операционной системы.
- Исходное имя файла (OriginalFileName) для ресурса RT_VERSION.

Данные, отправляемые в "Лабораторию Касперского" при принятии условий Положения о KSN

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

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

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

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

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

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

Данные в обнаружениях и событиях

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

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

Данные о событиях могут содержать следующую информацию:

- Об исполняемых модулях.
- О сетевых соединениях.
- Об операционной системе, установленной на компьютере с Kaspersky Endpoint Agent.
- О пользовательских сессиях в операционной системе.
- Об учетных записях пользователей операционной системы.

- О журнале событий Windows.
- Об обнаружениях Kaspersky Endpoint Security для Windows.
- Об организационных подразделениях (OU) Active Directory.
- Заголовки протокола HTTP.
- Полное доменное имя компьютера.
- MD5-, SHA256-хеш файлов и их фрагментов.
- Уникальный идентификатор компьютера с Kaspersky Endpoint Agent.
- Уникальные идентификаторы сертификатов.
- Издатель сертификата.
- Субъект сертификата.
- Название алгоритма, при помощи которого выполнен отпечаток сертификата.
- Адрес и порт локального сетевого интерфейса.
- Адрес и порт удаленного сетевого интерфейса.
- Поставщик программы.
- Название программы.
- Имя переменной реестра Windows.
- Путь к ключу реестра Windows.
- Данные переменной реестра Windows.
- Имя обнаруженного объекта.
- Идентификатор Агента администрирования Kaspersky Security Center.
- Содержимое файла hosts.
- Командная строка запуска процесса.

Данные в отчетах о выполнении задач

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

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

Отчеты о выполнении задач содержат следующую информацию:

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

Данные о файлах, запрещенных к запуску

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

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

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

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

Данные, связанные с выполнением задач

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

- для программы Kaspersky Endpoint Agent, входящей в состав программы Kaspersky Endpoint Security, в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp;
- для программы Kaspersky Endpoint Agent, установленной из пакета Kaspersky Anti Targeted Attack Platform, в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data\kata\temp.

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

- для программы Kaspersky Endpoint Agent, входящей в состав программы Kaspersky Endpoint Security, в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp;
- для программы Kaspersky Endpoint Agent, установленной из пакета Kaspersky Anti Targeted Attack Platform, в папке C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data\kata\temp.

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

Данные Kaspersky Endpoint Agent для Linux

Программа Kaspersky Endpoint Agent для Linux хранит и обрабатывает данные локально для обеспечения основной функциональности, аудита и повышения скорости решения возникших проблем специалистами Службы технической поддержки "Лаборатории Касперского".

На компьютерах с Kaspersky Endpoint Agent для Linux хранятся данные, подготовленные для отправки на серверы Kaspersky Anti Targeted Attack Platform и в Kaspersky Security Center автоматически .

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

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

Не используйте программу Kaspersky Endpoint Agent для Linux на тех компьютерах, передача данных с которых запрещена политикой вашей организации.

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

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

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

Администратору Kaspersky Anti Targeted Attack Platform необходимо обеспечить безопасность компьютеров с программой Kaspersky Endpoint Agent для Linux 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 Kaspersky Endpoint Agent для Linux:

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

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

Данные в запросах Kaspersky Endpoint Agent для Linux к Kaspersky Anti Targeted Attack Platform

При интеграции с компонентом Central Node следующие данные хранятся локально на устройстве с Kaspersky Endpoint Agent для Linux:

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

1. Данные в запросах на синхронизацию:
   - Уникальный идентификатор Kaspersky Endpoint Agent для Linux.
   - Имя устройства.
   - Локальное время на устройстве.
   - Имя и версия операционной системы, установленной на устройстве.
   - Версия Kaspersky Endpoint Agent для Linux.

- Версии параметров программы и параметров задач.
- Состояние задач в Kaspersky Endpoint Agent для Linux (идентификаторы выполняющихся задач, статусы выполнения, коды ошибок выполнения).

2. Данные о запущенных процессах:

- Информация об исполняемом файле процесса. Состав данных о файле см. ниже.
- Параметры автозапуска процесса.
- Значения переменных окружения.
- Идентификатор процесса.
- Идентификатор родительского процесса.
- Код сеанса входа в систему.
- Имя сеанса входа в систему.
- Идентификаторы пользователей и групп, запустивших процесс.
- Дата и время запуска процесса.
- Данные об остановленных процессах:
  - Идентификатор процесса.
  - Дата и время остановки процесса.
- Данные о файлах:
  - Путь к файлу.
  - Имя файла.
  - Размер файла.
  - Атрибуты файла.
  - Дата и время создания файла.
  - Дата и время последнего изменения файла.
  - Имена и уникальные идентификаторы пользователя-владельца и группы-владельца файла.
  - Права доступа к файлу.
  - Уникальный идентификатор файла.

- Данные об изменениях файлов:
  - Уникальный идентификатор файла.
  - Тип произведенной операции с файлом (запись, чтение, изменение атрибутов, переименование, удаление).
- Данные о сеансе входа в систему:
  - Дата и время начала сеанса входа в систему.
  - Тип сеанса.
  - Имя пользователя, запустившего сеанс.
  - Тип пользователя, запустившего сеанс.
  - IP-адрес удаленного компьютера.
- Данные об обнаружениях на компьютере с Kaspersky Endpoint Agent для Linux и Kaspersky Endpoint Security для Linux.
  - Тип обнаруженного объекта.
  - Имя объекта и полный путь до объекта.
  - Название обнаружения.
  - MD5-хеш объекта.
  - URL, с которого был загружен объект.
  - IP-адрес удаленного компьютера.
  - IP-адрес локального компьютера.
  - Результат обработки обнаружения.

До отправки данные хранятся в директории /var/opt/kaspersky/epagent/data/cache/queue в открытом незашифрованном виде. По умолчанию доступ к файлам имеют только пользователи с правами root.

3. В параметрах задач, полученных Kaspersky Endpoint Agent для Linux от Central Node:
   - Типы задач.
   - Параметры расписания запуска задач.
   - Имена и пароли учетных записей, под которыми необходимо запускать задачи.
   - Версии параметров.
   - Пути к объектам.
   - MD5 и SHA256-хеши объектов.

- Командная строка запуска процесса с аргументами.
- Информация о конкретной задаче хранится на устройстве до получения Kaspersky Endpoint Agent запроса на удаление со стороны Central Node или до удаления самого Kaspersky Endpoint Agent с устройства.

Данные о задачах хранятся в директории /var/opt/kaspersky/epagent/tasks в открытом незашифрованном виде. По умолчанию доступ к файлам имеют только пользователи с правами root.

4. В отчетах о результатах выполнения задач, передаваемых Kaspersky Endpoint Agent для Linux на Central Node:
   - Ошибки выполнения задач и коды возврата.
   - Статусы, с которыми завершались задачи.
   - Время завершения выполнения задач.
   - Версии параметров, с которыми выполнялись задачи.
   - Информация об объектах, переданных на сервер (пути к объектам, MD5 и SHA256-хеши объектов).
   - Файлы, запрошенные сервером.
   - Содержимое стандартного потока вывода процесса.
   - Содержимое стандартного потока ошибок процесса.
   - Kaspersky Endpoint Agent для Linux передает на Central Node отчеты о результатах выполнения задач.

Данные о результатах выполнения задач хранятся в директории /var/opt/kaspersky/epagent/tasks в открытом незашифрованном виде. По умолчанию доступ к файлам имеют только пользователи с правами root.

Информация с отчетом о выполнении задачи удаляется после передачи этой информации на Central Node.

Служебные данные Kaspersky Endpoint Agent для Linux

К служебным данным Kaspersky Endpoint Agent для Linux относятся данные, попадающие в конфигурационные файлы в результате настройки параметров администратором локально или с помощью плагина Kaspersky Security Center.

Служебные данные хранятся в директориях /var/opt/kaspersky/epagent/settings и /var/opt/kaspersky/epagent/policy. Данные хранятся до удаления Kaspersky Endpoint Agent для Linux.

Эти данные могут автоматически передаваться в Kaspersky Security Center.

По умолчанию доступ к файлам имеют только пользователи с правами root.

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

Kaspersky Endpoint Agent для Linux хранит следующие данные:

- Адрес сервера Central Node.
- Открытый ключ серверного сертификата для интеграции с Central Node.
- Контейнер с клиентским сертификатом для интеграции с Central Node.
- Учетные данные для авторизации на прокси-сервере.
- Адреса пользовательских источников обновлений.
- Настройки частоты синхронизации и передачи телеметрии на сервер Central Node.

Данные в файлах трассировки и дампов Kaspersky Endpoint Agent для Linux

Данные в файлах трассировки

Пользователи лично отвечают за безопасность данных, хранящихся на их компьютерах, в частности, за мониторинг и ограничение доступа к данным до момента их передачи в "Лабораторию Касперского".

Файлы трассировки хранятся на компьютере в течение всего времени использования программы и удаляются без возможности восстановления при удалении программы.

По умолчанию файлы трассировки хранятся в директории /var/log/kaspersky/epagent/. Вы можете просмотреть данные, хранящиеся в файлах трассировки. Для доступа к заданной по умолчанию директории хранения файлов трассировки требуются root-права.

Во всех файлах трассировки хранятся общие данные:

- время возникновения события;
- номер потока исполнения;
- компонент программы, инициировавший событие;
- уровень важности события (информационное событие, предупреждение, критическое событие, ошибка);
- описание события, связанного с выполнением команды компонентом программы, и результат выполнения этой команды.

В дополнение к общим данным в файлах трассировки могут храниться следующие данные:

- статусы компонентов Kaspersky Endpoint Agent и их рабочие данные;
- данные обо всех объектах и событиях операционной системы, включая данные о действиях пользователей;
- данные, содержащиеся в объектах операционной системы (например, содержимое файлов, в которых могут находиться персональные данные пользователей);
- данные о сетевом трафике (например, содержимое полей ввода на веб-сайте, которые могут включать данные банковской карты или любые другие конфиденциальные данные);
- данные, полученные с серверов "Лаборатории Касперского" (например, версия баз программы).

Запись данных трассировки производится в файл lena2021-01-18T052236.log. После того, как размер файла достигнет 10 МБ, файл будет сохранен в директории /var/log/kaspersky/epagent/. Для записи текущих данных будет создан новый файл с временной меткой. Всего в директории может храниться 10 файлов с данными трассировки. После того, как размер последнего созданного файла достигнет 10 МБ, самый старый файл будет удален.

Файлы трассировки других программ хранятся на компьютере до момента удаления программы.

Данные в файлах дампов

Сохраненные файлы дампов могут содержать персональные данные. Чтобы обеспечить контроль и ограничение доступа к данным, необходимо самостоятельно позаботься о безопасности файлов дампов.

Файлы дампов формируются автоматически при сбое программы и хранятся на компьютере в течение всего времени использования программы. Файлы дампов удаляются без возможности восстановления при удалении программы.

Файлы дампов хранятся в директории /var/opt/kaspersky/epagent/dumps/.

Файл дампов содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Agent для Linux на момент создания файла дампов. Файл дампов может также содержать персональные данные.

Для доступа к файлам дампов требуются root-права.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы Kaspersky Anti Targeted Attack Platform.

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 Kaspersky Anti Targeted Attack Platform, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

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

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN может быть недоступна в программе на территории США.

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 добавленного лицензионного 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**, **Пользовательские правила**, **Хранилище**, **Endpoint Agents**.

О файле ключа

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

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

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

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

Для восстановления файла ключа обратитесь к продавцу лицензии.

Просмотр информации о лицензии и добавленных ключах

В режиме распределенного решения и мультитенантности 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 мультитенантности – 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 и мультитенантности 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 мультитенантности 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 мультитенантности 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, выполните следующие действия:

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

Просмотр текста Лицензионного соглашения на компьютере с Kaspersky Endpoint Agent

На каждом компьютере, на котором установлена отдельная программа Kaspersky Endpoint Agent, файл с Лицензионным соглашением Kaspersky Anti Targeted Attack Platform находится в папке EULA в той директории, в которой установлена программа Kaspersky Endpoint Agent.

Добавление ключа

В режиме распределенного решения 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 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 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**, **Пользовательские правила**, **Хранилище**, **Endpoint Agents**.

Коммерческая лицензия

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

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

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

В текущей версии Kaspersky Anti Targeted Attack Platform функциональность программы также зависит от типа добавленного лицензионного 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**, **Пользовательские правила**, **Хранилище**, **Endpoint Agents**.

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.
- *Kaspersky Endpoint Agent.* Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации. 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 – 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.

Компонент Sensor также может использоваться в качестве прокси-сервера для соединений, исходящих от программы Kaspersky Endpoint Agent.

Если в качестве компонента Sensor используется программа KSMG или KLMS, то правила исключений из проверки, 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

Компонент может быть развернут на одном сервере или в виде отказоустойчивого кластера, который состоит из серверов 2 ролей – серверов хранения и обрабатывающих серверов.

Отказоустойчивость достигается за счет дублирования данных между серверами хранения и избыточности вычислительных ресурсов: при выходе из строя одного сервера его функции выполняет другой сервер с аналогичной ролью. Kaspersky Anti Targeted Attack Platform при этом продолжает работать.

На каждом сервере или кластере с компонентом Central Node работают следующие модули, ядра и технологии программы:

- *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 анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации, на основе правил TAA (IOA). 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.
- CentOS 7.8.

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 Kaspersky Endpoint Agent

Компонент представлен программами Kaspersky Endpoint Agent для Windows, Kaspersky Endpoint Agent для Linux и Kaspersky Endpoint Security для Windows. Программы устанавливаются на рабочие станции и серверы в IT-инфраструктуре организации (далее также "компьютеры локальной сети организации" или "компьютеры"). На этих компьютерах программы постоянно наблюдают за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляют данные наблюдения на сервер с компонентом Central Node.

Компьютеры, предназначенные для установки программ, должны удовлетворять аппаратным и программным требованиям Kaspersky Endpoint Agent для Windows, Kaspersky Endpoint Agent для Linux и Kaspersky Endpoint Security для Windows.

Принцип работы программы

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

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

Вы можете использовать как полную функциональность программы (ключ KATA и ключ KEDR), так и неполную (только ключ KATA или только ключ KEDR).

Принцип работы Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack включает в себя следующие компоненты:

- Sensor.
- Central Node.
- Sandbox.

Компоненты Sensor, Central Node и Sandbox взаимодействуют между собой по следующему принципу:

- Компонент Sensor получает зеркалированный SPAN-, ERSPAN-, RSPAN-трафик, объекты и метаинформацию HTTP-, FTP-, SMTP- и DNS-протоколов, данные HTTP- и FTP-трафика, а также HTTPS-трафика (если администратор настроил подмену SSL-сертификата на прокси-сервере), копии сообщений электронной почты и производит с полученными данными следующие действия:
  - Проверяет интернет-трафик на наличие признаков вторжения в IT-инфраструктуру организации с помощью технологии Intrusion Detection System (далее также "IDS").

    Технология IDS позволяет распознать и обнаружить сетевую активность по 80 протоколам, в частности по 53 протоколам прикладного уровня модели TCP/IP, фиксируя подозрительный трафик и сетевые атаки. В числе поддерживаемых протоколов TCP, UDP, FTP, TFTP, SSH, SMTP, SMB, CIF, SSL, HTTP, HTTP/2, HTTPS, TLS, ICMPv4, ICMPv6, IPv4, IPv6, IRC, LDAP, NFS, DNS, RDP, DCERPC, MS-RPC, WebSocket, Citrix и другие.
  - Проверяет репутацию файлов и URL-адресов по базе знаний Kaspersky Security Network (далее также "KSN") или Kaspersky Private Security Network (далее также "KPSN").
  - Отправляет объекты и файлы на проверку компоненту Central Node.

В качестве компонента Sensor также может использоваться *почтовый сенсор* – 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").

- Компонент Central Node проверяет файлы и объекты с помощью антивирусных баз, баз YARA-правил, создаваемых пользователями Kaspersky Anti Targeted Attack, при необходимости отправляет файлы и объекты на проверку компоненту Sandbox.

- Компонент Sandbox анализирует поведение объектов в виртуальных операционных системах для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации и отправляет данные о результатах проверки на сервер Central Node.

При обнаружении угроз сервер Central Node записывает информацию о них в базу обнаружений. Вы можете просмотреть таблицу обнаружений в разделе **Обнаружения** веб-интерфейса программы или сформировав отчет об обнаружениях.

Информация об обнаружениях также может публиковаться в SIEM-систему, которая используется в вашей организации, и во внешние системы. Информация об обнаружениях компонента Sandbox может публиковаться в локальную репутационную базу Kaspersky Private Security Network.

Принцип работы Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection and Response включает в себя следующие компоненты:

- Central Node.

- Kaspersky Endpoint Agent.

  Компонент представлен программами Kaspersky Endpoint Agent для Windows, Kaspersky Endpoint Agent для Linux и Kaspersky Endpoint Security для Windows.

- Sandbox.

  Опциональный компонент.

  > В качестве прокси-сервера для соединений, исходящих от компонента Kaspersky Endpoint Agent, может использоваться компонент Sensor.

Компоненты Kaspersky Endpoint Agent и Central Node взаимодействуют между собой по следующему принципу:

- Программы Kaspersky Endpoint Agent для Windows и Kaspersky Endpoint Agent для Linux устанавливаются на отдельных компьютерах, входящих в IT-инфраструктуру организации, и осуществляют постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные наблюдения отправляются на сервер с компонентом Central Node. На основе этих данных формируются события.

  Kaspersky Endpoint Agent для Windows передает на сервер Central Node данные о следующих событиях:

  - **Запущен процесс**;
  - **Загружен модуль**;
  - **Удаленное соединение**;
  - **Правило запрета**;
  - **Заблокирован документ**;

- **Изменен файл**;
- **Журнал событий ОС**;
- **Изменение в реестре**;
- **Прослушан порт**;
- **Загружен драйвер**;
- **Интерпретированный запуск файла**;
- **Интерактивный ввод команд в консоли**.

Kaspersky Endpoint Agent для Linux передает на сервер Central Node данные о следующих событиях:

- **Запущен процесс**;
- **Изменен файл**;
- **Журнал событий ОС**.

Программы могут интегрироваться с программами защиты рабочих станций (Endpoint Protection Platform (далее также "EPP")).

Kaspersky Endpoint Agent для Windows может интегрироваться со следующими программами EPP:

- Kaspersky Endpoint Security для Windows.
- Kaspersky Security для Windows Server.
- Kaspersky Security для виртуальных сред Легкий Агент для Windows.

Kaspersky Endpoint Agent для Linux может интегрироваться с программой Kaspersky Endpoint Security для Linux.

В этом случае программа Kaspersky Endpoint Agent также передает на сервер Central Node данные об угрозах, обнаруженных программами EPP, и о результатах обработки угроз этими программами.

Программы EPP, Kaspersky Endpoint Agent и сервер Central Node взаимодействуют между собой по следующему принципу:

- Программы EPP передают Kaspersky Endpoint Agent данные об обнаруженных угрозах и о результате обработки угроз.

  Программа Kaspersky Endpoint Security для Windows также может передавать Kaspersky Endpoint Agent для Windows данные об отправке сторонним приложением с поддержкой Antimalware Scan Interface (далее также "AMSI") объектов (например, скриптов PowerShell) в Kaspersky Endpoint Security для Windows для дополнительной проверки.

- Программа Kaspersky Endpoint Agent передает данные наблюдения за процессами, открытыми сетевыми соединениями и изменяемыми файлами, а также данные, полученные от программ EPP, на сервер Central Node.

  Сервер Central Node обрабатывает полученные данные и отображает в веб-интерфейсе программы соответствующие события.

  В результате обработки данных программ EPP формируются события **Обнаружение**, **Результат обработки обнаружения**, **AMSI-проверка** (при интеграции Kaspersky Endpoint Agent для Windows с Kaspersky Endpoint Security для Windows).

События, поступающие на сервер Central Node, отмечаются правилами TAA (IOA). В результате разметки для событий, требующих внимания пользователя, формируются обнаружения. При наличии компонента Sandbox вы можете также включить автоматическую отправку файлов с хостов Kaspersky Endpoint Agent на проверку компоненту Sandbox в соответствии с правилами TAA (IOA) "Лаборатории Касперского".

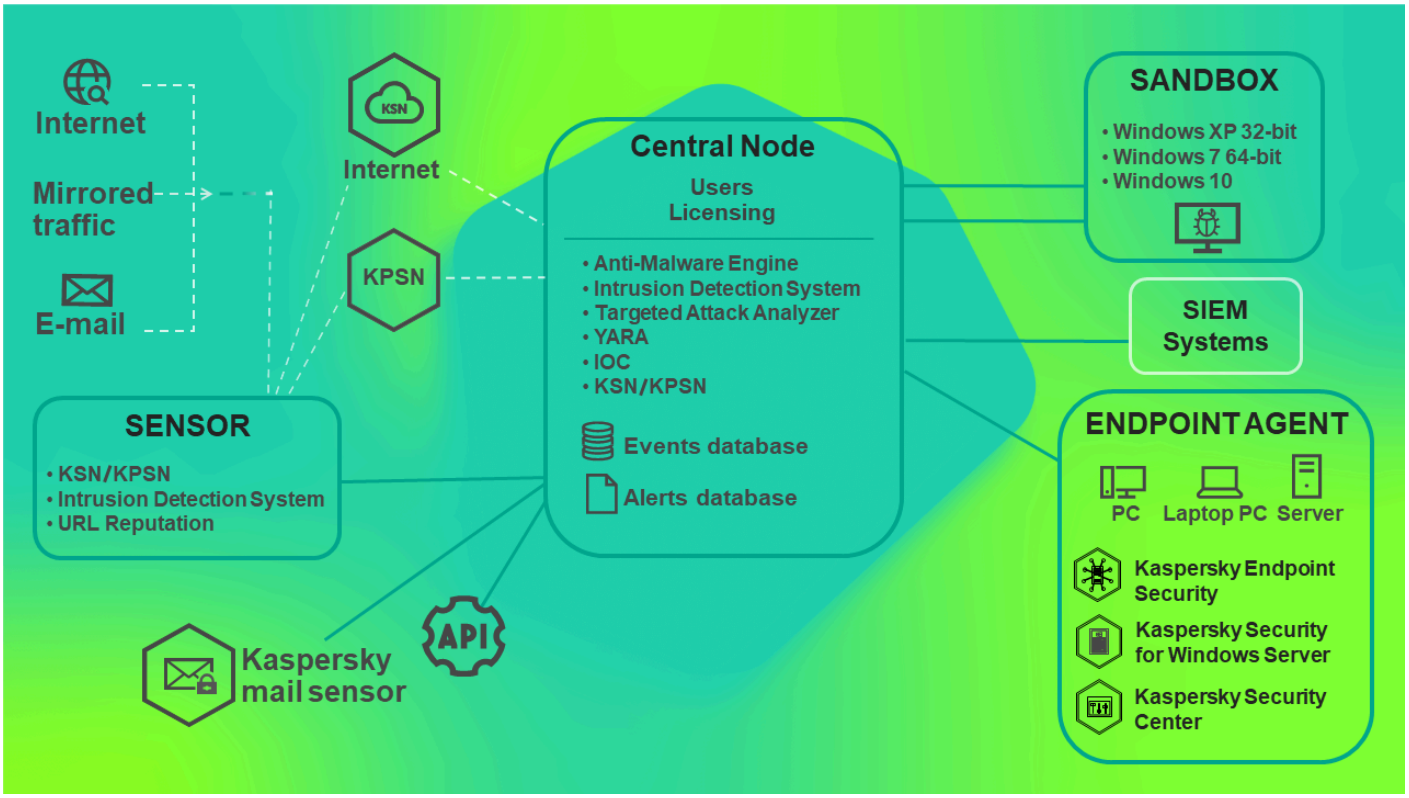
При интеграции сервера Central Node с Kaspersky Endpoint Agent для Windows вы можете осуществлять следующие меры по реагированию на обнаруженные угрозы:

- Работать с файлами и программами путем выполнения задач **Завершить процесс**, **Собрать форензику**, **Запустить YARA-проверку**, **Выполнить программу**, **Получить файл**, **Удалить файл**, **Поместить файл на карантин**, **Восстановить файл из карантина**, **Управление службами**, **Получить образ диска**, **Получить дамп памяти** на хостах с Kaspersky Endpoint Agent.
- Настраивать политики запрета запуска файлов и процессов на выбранных хостах с Kaspersky Endpoint Agent.
- Изолировать отдельные хосты с Kaspersky Endpoint Agent от сети.
- Работать с правилами TAA (IOA) для классификации и анализа событий.
- Работать с файлами открытого стандарта описания индикаторов компрометации OpenIOC (IOC-файлы) для поиска признаков целевых атак, зараженных и возможно зараженных объектов на хостах с Kaspersky Endpoint Agent и в базе обнаружений.

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

- Работать с файлами и программами путем выполнения задач **Получить файл**, **Выполнить программу**.
- Работать с правилами TAA (IOA) для классификации и анализа событий.

Принцип работы Kaspersky Anti Targeted Attack Platform показан на рисунке ниже.

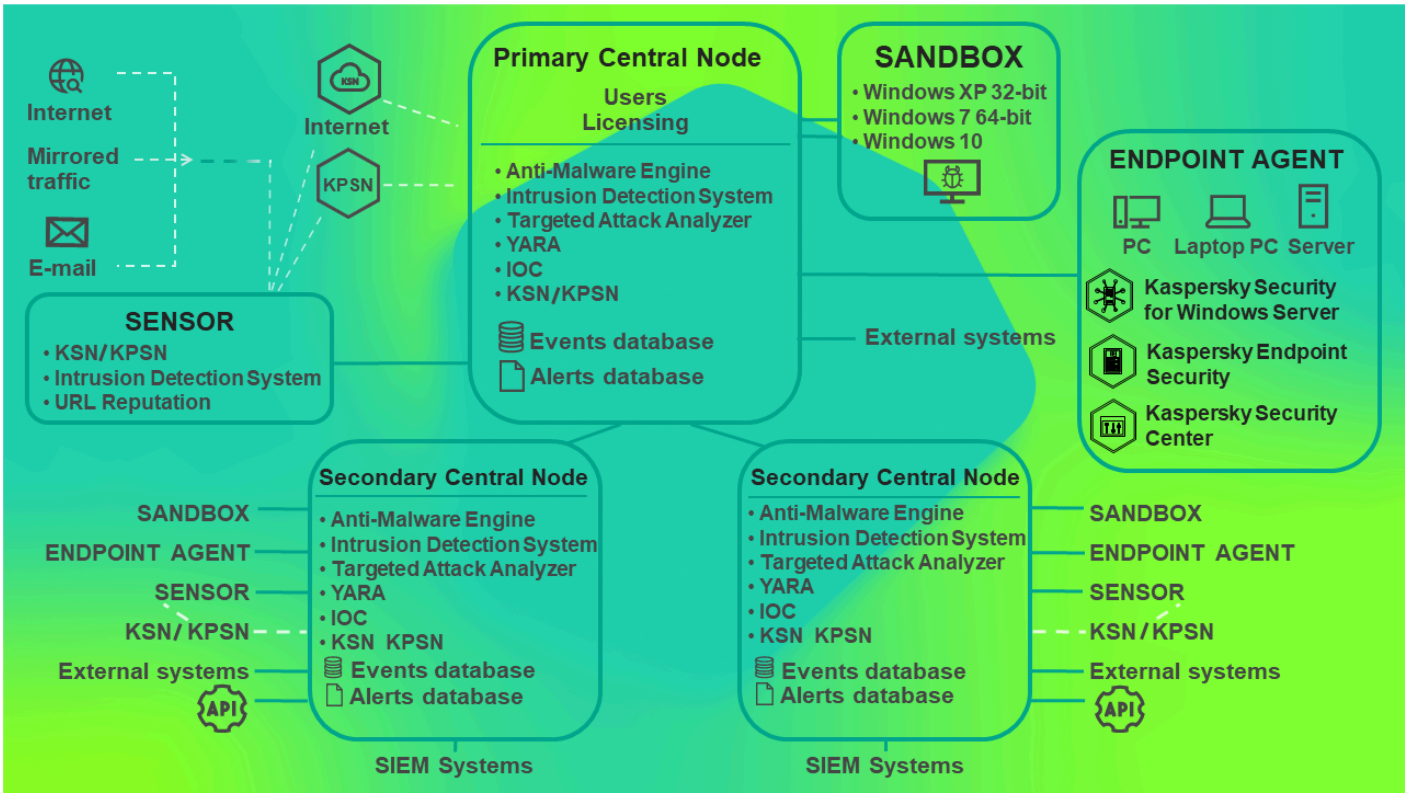


Принцип работы Kaspersky Anti Targeted Attack Platform

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 Central Node. В этой структуре выделяется главный сервер управления – Primary Central Node (PCN) и подчиненные серверы – Secondary Central Node (SCN).

Принцип работы Kaspersky Anti Targeted Attack Platform в режиме распределенного решения показан на рисунке ниже.



Принцип работы Kaspersky Anti Targeted Attack Platform в режиме распределенного решения

Распределенное решение и мультитенантность

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 требуется подключить SCN к PCN.

Если вы развернули компонент Central Node в виде кластера, весь кластер выполняет роль PCN или SCN.

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:

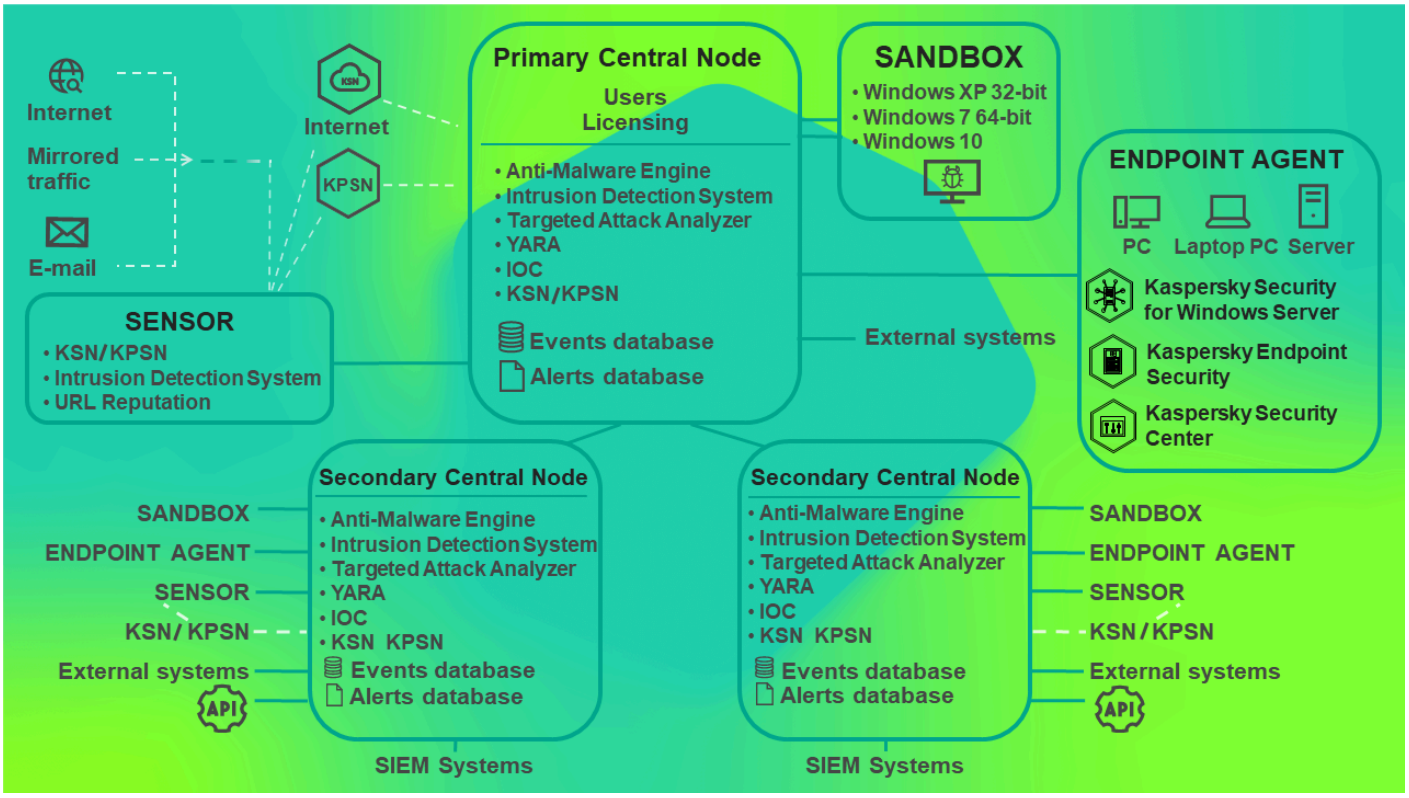
- Пользователи.
- Обнаружения.
- Поиск угроз.
- Задачи.
- Политики.
- Пользовательские правила.
- Хранилище.
- Endpoint Agents, в том числе сетевая изоляция хостов.
- Отчеты.

Если вы поддерживаете несколько организаций или филиалов одной организации, вы можете использовать программу в режиме мультитенантности.

Мультитенантность - это режим работы, при котором решение используется для защиты инфраструктуры нескольких организаций или филиалов одной организации (далее также "тенантов") одновременно. Вы можете установить Kaspersky Anti Targeted Attack Platform на один или несколько серверов Central Node для каждого тенанта. Каждый тенант может работать с программой независимо от других тенантов. Поставщик услуг может работать с данными нескольких тенантов.

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

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



Принцип работы программы в режиме распределенного решения

Вы можете использовать режим распределенного решения и мультитенантности в следующих случаях:

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

При переключении программы в режим распределенного решения и мультитенантности на серверах с ролью SCN все ранее добавленные лицензионные ключи удаляются. Каждый подключенный SCN получает ключ от PCN. Если для PCN используется полная функциональность программы (ключ KATA и KEDR), а для SCN неполная (только ключ KATA или только ключ KEDR), в связи с увеличением объема данных возможно превышение допустимого уровня нагрузки на сервер SCN. Если для PCN используется неполная функциональность программы (только ключ KATA или только ключ KEDR), а для SCN полная (ключ KATA и KEDR), часть функционала программы будет недоступна.

Управление лицензионными ключами будет доступно только на PCN.

Вы можете развернуть программу в режиме распределенного решения и мультитенантности 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 5.0.

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

Сценарий перехода в режим распределенного решения и мультитенантности

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

1. **Установка компонентов Central Node**
2. Назначение одному из серверов роли PCN
3. Назначение остальным серверам роли SCN и отправка запросов на подключение к PCN
4. Обработка запроса на подключение SCN к PCN

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

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

Изменения в параметрах программы при переключении в режим распределенного решения и мультитенантности

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

Функциональная область	PCN	SCN
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 столбец **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.
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 столбце **Central Node** для них отображается имя PCN. На PCN также сохраняется содержимое Хранилища всех подключенных SCN.	Все файлы и метаданные, которые хранились на SCN до перехода в режим распределенного решения, сохраняются.
Исключения ТАА	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Правила уведомлений	Изменений нет.	Изменений нет.
Интеграция с почтовыми сенсорами	Изменений нет.	Изменений нет.
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 выбранного тенанта.	Изменений нет.
Пользовательские правила - ТАА	IOC-файлы, добавленные на сервере Central Node до назначения ему роли PCN, распространяются на PCN. Правила ТАА (IOA), добавленные на сервере Central Node до назначения ему роли PCN, распространяются на PCN.	Отображаются IOC-файлы и правила ТАА (IOA), добавляемые на PCN, а также IOC-файлы и правила ТАА (IOA), добавляемые на этом SCN до и после перехода в режим распределенного решения.
Резервное копирование программы	Резервное копирование программы доступно только на PCN, к которому не подключены SCN. Чтобы сделать резервное копирование программы на PCN, необходимо отключить все SCN от этого PCN.	Резервное копирование программы на SCN недоступно. Чтобы сделать резервное копирование программы на SCN, необходимо отключить этот сервер от PCN, переведя его в режим отдельного сервера.

Назначение серверу роли PCN

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

Чтобы назначить серверу роль PCN:

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 тенанта** введите название тенанта, к которому 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 тенанта.

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.
- **Тенанты** – информация о тенантах, к которым относится этот сервер, и все подключенные серверы 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, подключенных к тенантам.
- Таблица **Серверы, ожидающие авторизации** с информацией о подключенных SCN.

Назначение серверу роли SCN

Чтобы назначить серверу роль SCN:

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 тому тенанту, который укажет администратор PCN.

Обработка запросов на подключение SCN к PCN

Чтобы обработать запрос на подключение SCN к PCN:

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

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

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

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

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

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

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

     1. Нажмите на кнопу **Принять**.

        Откроется окно **Принять запрос на подключение**.

     2. В списке **Тенант** выберите тенант, которому вы хотите назначить этот сервер SCN. Список формируется из тенантов, добавленных ранее.

     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 о тенантах, 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 о серверах PCN и SCN в режиме мультитенантности:

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 о серверах:

- **Текущий режим** – Распределенное решение.
- **Роль сервера** – Primary Central Node.
- **Отпечаток сертификата** – отпечаток сертификата сервера PCN.
- **Тенанты** – информация о тенантах, к которым относятся 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 серверов SCN, а также количество серверов, подключенных к тенанту.

- 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 тенанта на сервере PCN

Чтобы добавить тенант в веб-интерфейсе сервера PCN:

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

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

Тенант будет добавлен и отобразится в списке.

Удаление тенанта на сервере PCN

Чтобы удалить тенант в веб-интерфейсе сервера PCN:

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

   Вам нужно войти в веб-интерфейс сервера PCN, для которого вы хотите удалить тенант.
2. В окне веб-интерфейса программы выберите раздел **Режим работы**.
3. В рабочей области **Тенанты** выберите тенант, который 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 этим тенантом, будут потеряны.

5. Нажмите на кнопку **Да**.

Тенант будет удален.

Изменение названия тенанта на сервере PCN

Чтобы изменить название тенанта в веб-интерфейсе сервера PCN:

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

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

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

3. В списке **Тенанты** нажмите на значок справа от названия тенанта, которое вы хотите изменить.

   Откроется окно изменения названия тенанта.

4. В поле **Имя** измените название тенанта.

5. Нажмите на кнопку **Сохранить**.

Название тенанта 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 одного тенанта другому, необходимо удалить все данные, оставшиеся на сервере после использования Kaspersky Anti Targeted Attack Platform и переустановить Kaspersky Anti Targeted Attack Platform перед передачей сервера другому тенанту.

Чтобы отключить SCN от PCN через веб-интерфейс PCN:

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:

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.

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.

Функциональная область	PCN	SCN
Отчеты	Все созданные ранее отчеты об отключенном SCN, а также возможность фильтровать список отчетов по этому серверу, сохраняются.	Шаблоны и отчеты не изменяются.
Политики	Политики, созданные на отключенном SCN, удаляются.	Политики, созданные на PCN, удаляются. Информация о пользователях, создавших политики на SCN, сохраняется.
Хранилище	Из Хранилища удаляются все объекты, относящиеся к отключенному SCN.	Все объекты в Хранилище сохраняются. В информации об объектах, полученных в рамках задач, созданных на PCN, перестает работать ссылка на задачу.
Исключения TAA	Изменений нет.	Изменений нет.
Статус VIP	Изменений нет.	Изменений нет.
Правила уведомлений	Изменений нет.	Изменений нет.
Интеграция с почтовыми сенсорами	Изменений нет.	Изменений нет.
Поиск угроз	В результате обработки поискового запроса события, связанные с отключенным SCN, не отображаются.	Изменений нет.
Пользовательские правила - TAA и IOC	IOC- и правила TAA (IOA) отключенного SCN удаляются.	IOC- и правила TAA (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 одного тенанта другому, необходимо удалить все данные, оставшиеся на сервере после использования Kaspersky Anti Targeted Attack Platform и переустановить Kaspersky Anti Targeted Attack Platform перед передачей сервера другому тенанту.

Вывод сервера SCN из эксплуатации программой состоит из следующих этапов:

1. **Удаление всех данных на SCN**
2. **Отключение SCN от PCN через веб-интерфейс PCN**
3. **Отключение SCN от PCN через веб-интерфейс SCN**
4. **Удаление SCN через веб-интерфейс PCN**

Чтобы удалить SCN через веб-интерфейс PCN:

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.

Руководство по масштабированию

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

Выбор оптимальной конфигурации программы состоит из следующих этапов:

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

Типовые схемы развертывания и установки компонентов программы

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

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

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

Выбор схемы развертывания зависит от используемой функциональности программы. 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 программ Kaspersky Endpoint Agent, не рекомендуется использовать компонент Central Node для обработки трафика.

Вы можете использовать компонент Sensor в качестве прокси-сервера для соединения хостов с программой Kaspersky Endpoint Agent и Central Node. Один компонент Sensor поддерживает подключение до 1000 хостов с программой Kaspersky Endpoint Agent.

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.

Выбор схемы развертывания при использовании функциональности KATA и KEDR

Критерий	Схема на два сервера	Схема на три сервера	Схема на четыре и более серверов	Распределенное решение
Сетевой и почтовый трафик не может быть принят на одном устройстве	Нет	Да	Да	Да
Количество хостов с программой Kaspersky Endpoint Agent	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.

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.

Выбор схемы развертывания при использовании функциональности KATA

Критерий	Схема на два сервера	Схема на три сервера	Схема на четыре и более серверов
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

Критерий	Схема на два сервера	Схема на три сервера	Схема на четыре и более серверов
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;
- схема с компонентом Sandbox.

Схема развертывания на два сервера

При использовании функциональности KATA и KEDR вы можете установить программу Kaspersky Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA программа Kaspersky Endpoint Agent не устанавливается.

При использовании этой схемы развертывания компоненты Central Node и Sensor устанавливаются на одном сервере или кластере. Этот сервер или кластер 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 рисунке ниже.

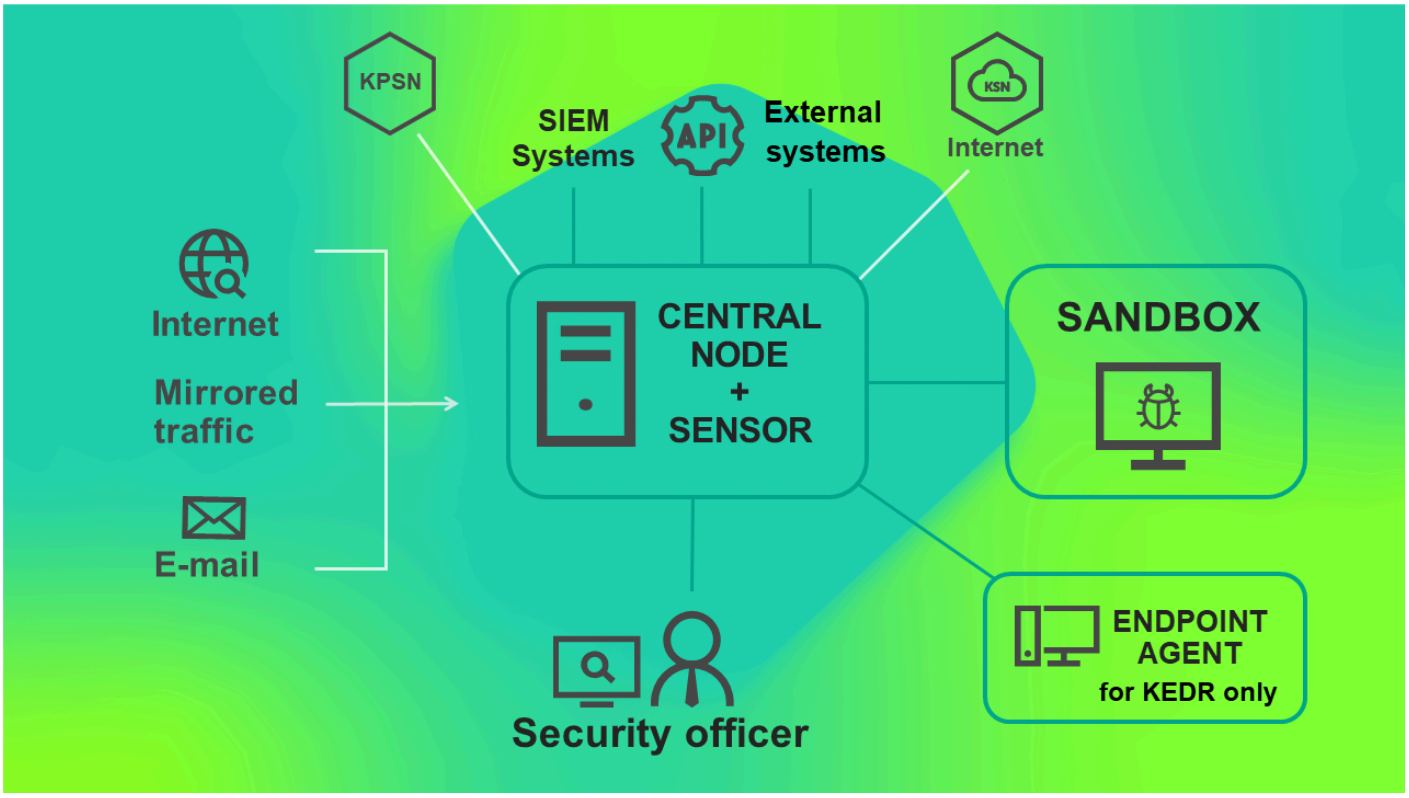


Схема работы программы при развертывании на два сервера

Схема развертывания на три сервера

При использовании функциональности KATA и KEDR вы можете установить программу Kaspersky Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA программа Kaspersky Endpoint Agent не устанавливается.

При использовании этой схемы развертывания компоненты Sensor, Central Node и Sandbox устанавливаются на отдельных серверах. Компонент Central Node также может быть развернут в виде кластера. Сервер с компонентом Sensor принимает трафик, выполняет первичный анализ, извлекает файлы и пересылает их компоненту 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, передаваемый 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.

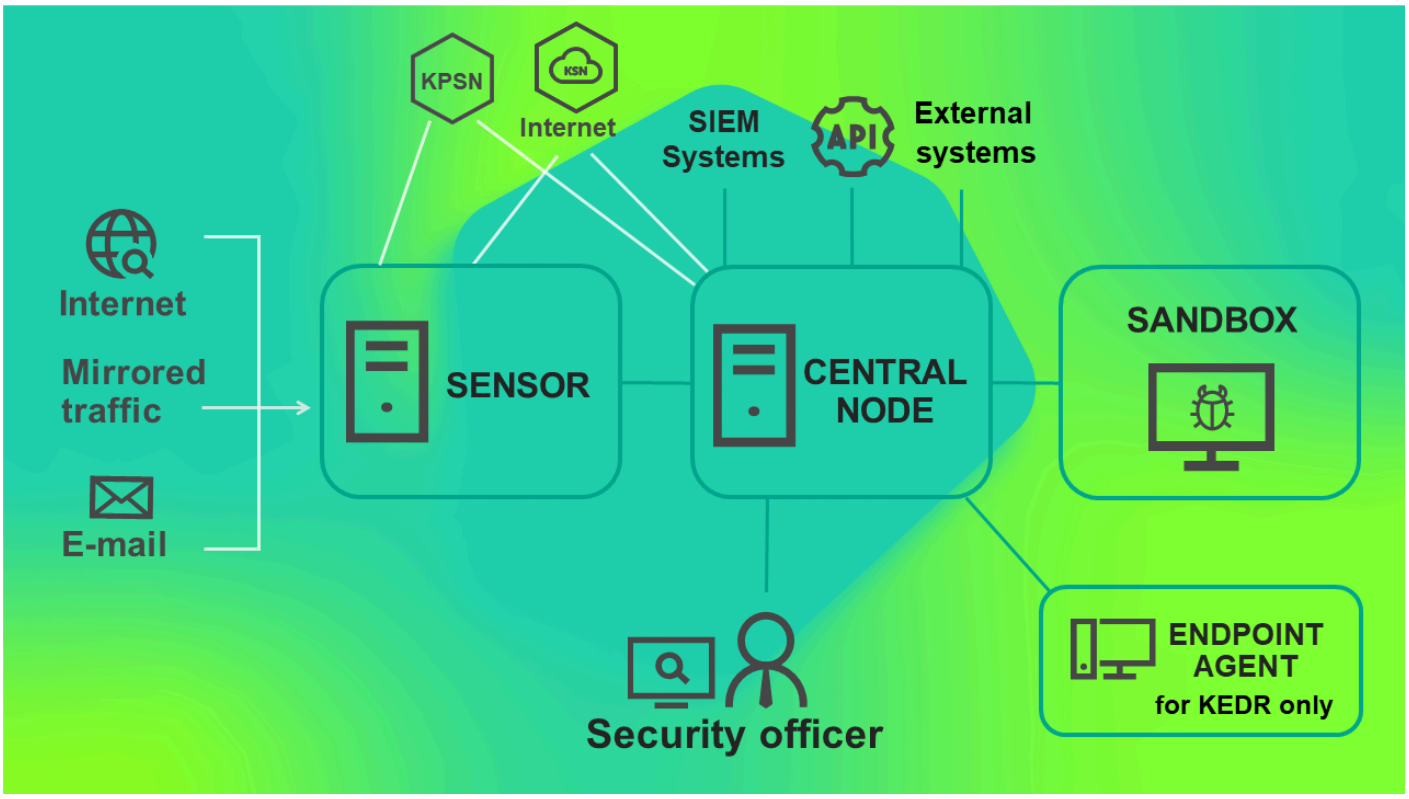


Схема работы программы при развертывании на три сервера

Схема развертывания на четыре и более сервера

При использовании функциональности KATA и KEDR вы можете установить программу Kaspersky Endpoint Agent на компьютерах локальной сети организации. При использовании функциональности KATA программа Kaspersky Endpoint Agent не устанавливается.

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.

Схема работы программы при развертывании на четыре и более сервера представлена на рисунке ниже.

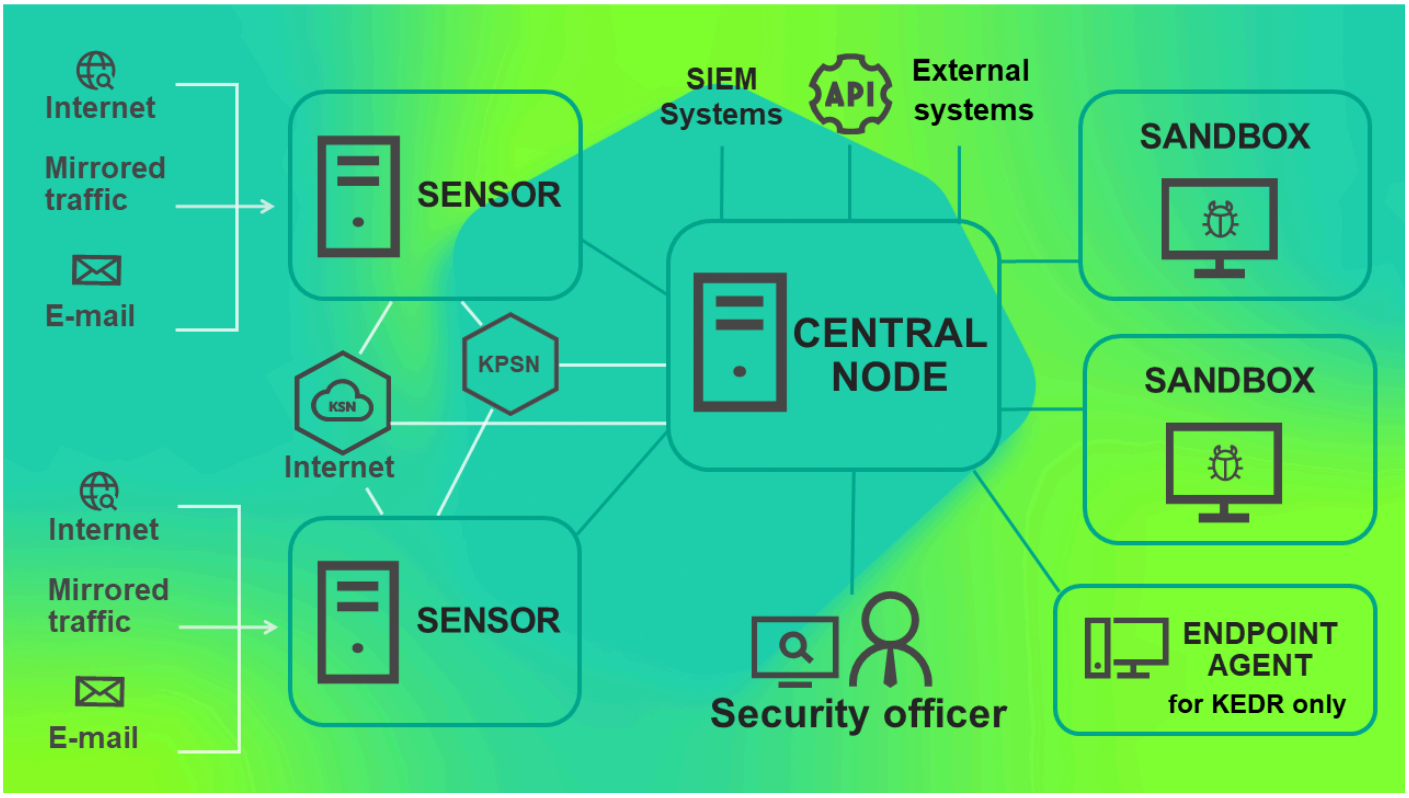


Схема работы программы при развертывании на четыре и более сервера

Схема развертывания функциональности KEDR с компонентом Sandbox

При такой схеме развертывания вам требуется установить компонент Central Node отдельно от компонента Sensor.

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

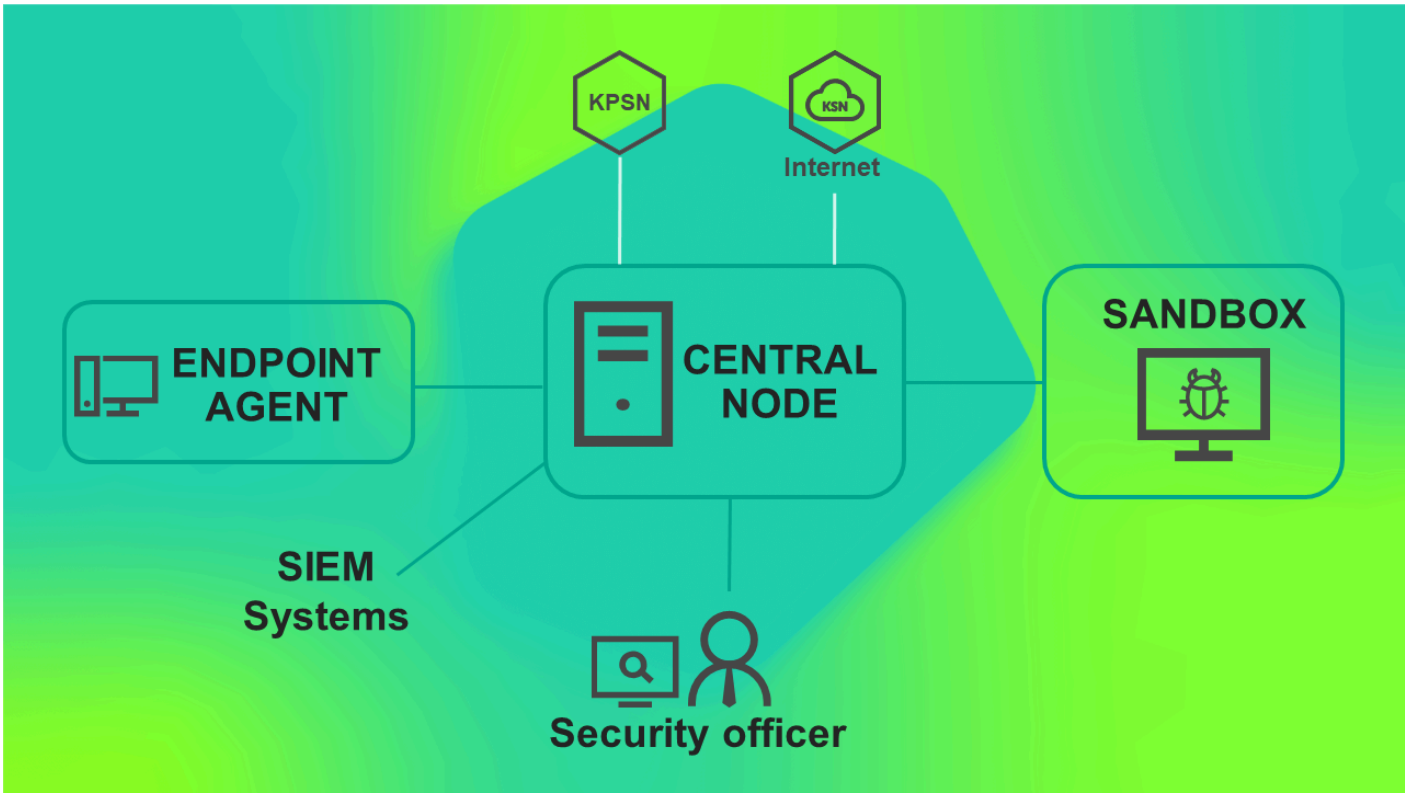


Схема работы программы при развертывании функциональности KEDR с компонентом Sandbox

Схема развертывания функциональности KEDR без компонента Sandbox

Вы можете не устанавливать компонент Sandbox и использовать компонент Central Node только для управления программой Kaspersky Endpoint Agent и анализа данных.

При такой схеме развертывания вам требуется установить компонент Central Node отдельно от компонента Sensor.

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

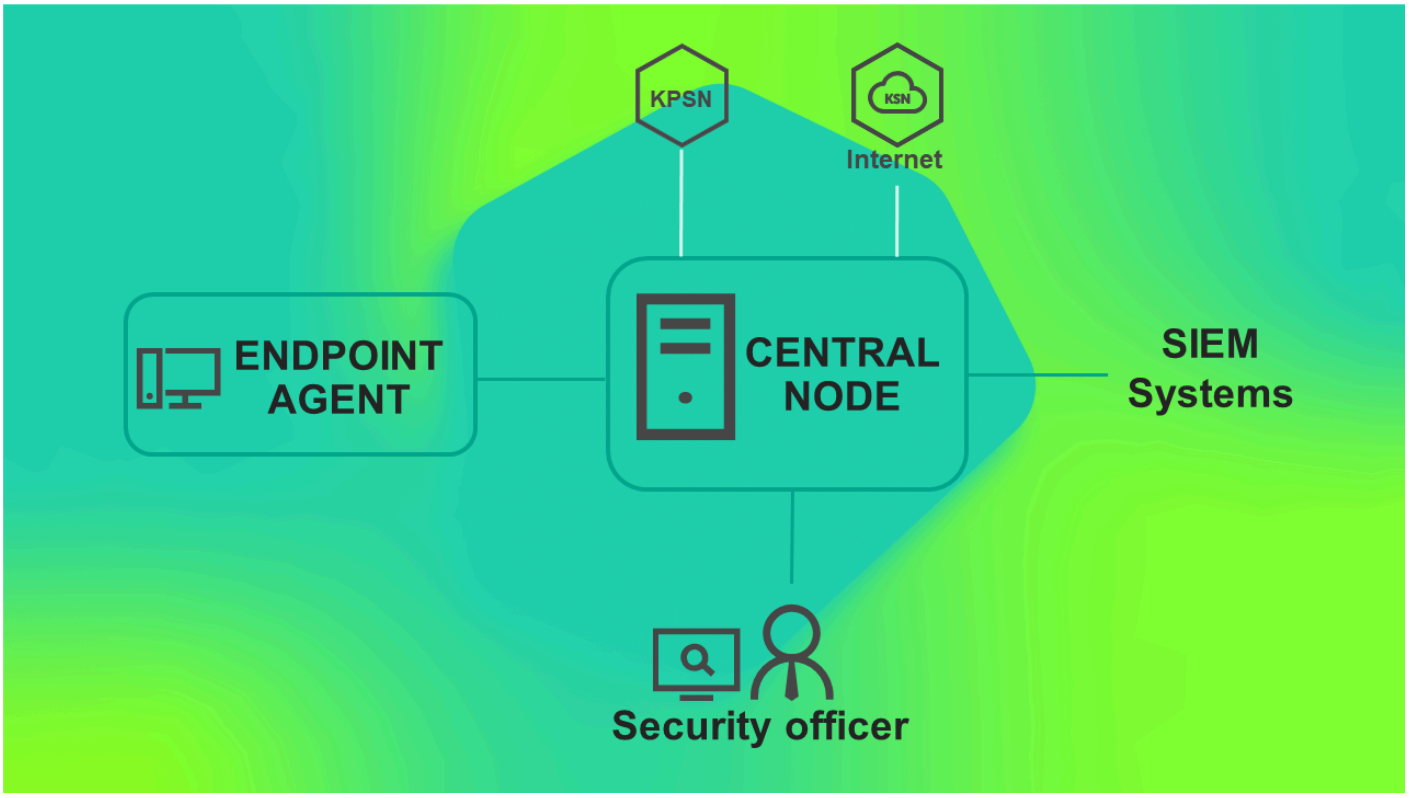


Схема работы программы при развертывании функциональности KEDR без компонента Sandbox

Калькулятор масштабирования

После того, как вы выбрали схему развертывания, наиболее подходящую для вашей IT-инфраструктуры, вам требуется рассчитать аппаратные требования к серверам для установки компонентов программы.

Расчеты для компонента Sensor

Данные расчеты применимы также при развертывании программы на виртуальной платформе.

При расчете аппаратных требований к компоненту Sensor требуется учитывать, что максимальный объем обрабатываемого трафика для одного компонента Sensor составляет 4 Гбит/с. Наиболее ресурсоемкой технологией является Intrusion Detection System.

Вы можете использовать сервер с компонентом Sensor в качестве прокси-сервера при обмене данными между программой Kaspersky Endpoint Agent и компонентом Central Node, чтобы упростить настройку сетевых правил. Например, если компьютеры с Kaspersky Endpoint Agent находятся в отдельном сегменте сети, то будет достаточно настроить соединение между серверами с компонентами Central Node и Sensor.

При настройке перенаправления трафика Kaspersky Endpoint Agent на компонент Central Node учитывайте следующие ограничения:

- Максимальное количество компьютеров с Kaspersky Endpoint Agent, подключенных к одному компоненту Central Node, составляет 15 000 шт.
- Максимально допустимые потери пакетов, пересылаемых между серверами с компонентами Sensor и Central Node, составляют 10% при задержке отправки пакетов до 100 мс.

Аппаратные требования к серверу с компонентом Sensor зависят от объема обрабатываемого трафика. Требуемая пропускная способность канала связи между серверами с компонентами Central Node и Sensor является суммой трафика компонента Sensor (10% от трафика на SPAN-порте + почтовый трафик + трафик по протоколу ICAP) и требованиям к каналу связи между компонентом Central Node и программой Kaspersky Endpoint Agent (в зависимости от количества компьютеров с Kaspersky Endpoint Agent, трафик которых перенаправляется компонентом Sensor на компонент Central Node).

При расчете аппаратных требований к серверу с компонентом Sensor требуется учитывать, что одна программа Kaspersky Endpoint Agent для Linux дает такую же нагрузку, как три программы Kaspersky Endpoint Agent для Windows.

Если пропускная способность канала связи составляет более 2 Гбит/с, требуется **настроить использование одного ядра для обработки сетевых прерываний**.

1. На сервере с компонентом Sensor в файле /var/opt/kaspersky/apt-preprocessor/preprocessor.conf добавьте строку `pcap_cores=$CORES-1`, где `$CORES` является числом логических ядер сервера.
2. Перезапустите службу, чтобы применить измененные параметры. Для этого выполните следующую команду:

   ```
   systemctl restart apt-preprocessor.service
   ```

3. В файле /etc/sysconfig/irqbalance добавьте одну из следующих строк:
   - Если на первом шаге вы указали `pcap_cores=31`, добавьте `IRQBALANCE_BANNED_CPUS=80000000`
   - Если на первом шаге вы указали `pcap_cores=47`, добавьте `IRQBALANCE_BANNED_CPUS=8000,00000000`
4. Перезапустите службу, чтобы применить измененные параметры. Для этого выполните следующую команду:

   ```
   service irqbalance restart
   ```

Аппаратные требования к компоненту Sensor в зависимости от обрабатываемого трафика

Компонент Sensor может быть интегрирован с IT-инфраструктурой организации следующими способами:

- получение зеркалированного трафика от сетевых устройств со SPAN-портов;
- подключение к почтовому серверу по протоколу POP3;

- подключение к почтовому серверу по протоколу SMTP;
- получение трафика от прокси-сервера по протоколу ICAP.

Аппаратные требования к компоненту Sensor приведены в таблице ниже. Расчеты приведены для случая, когда компонент Sensor не обрабатывает сообщения электронной почты и трафик по протоколу ICAP. Если компонент Sensor осуществляет перенаправление трафика с компьютеров с Kaspersky Endpoint Agent, следует также учитывать требования к каналам связи.

Аппаратные требования к компоненту Sensor в зависимости от объема обрабатываемого трафика со SPAN-портов

Максимальное количество компьютеров с Kaspersky Endpoint Agent для Windows	Максимальный объем обрабатываемого трафика (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер
10000	100	16	4
15000	500	16	8
15000	1000	24	16
15000	2000	32	32
15000	4000	32	48

Аппаратные требования к компоненту Sensor, интегрированному с почтовым сервером, приведены в таблице ниже. Расчеты приведены для случая, когда компонент Sensor не обрабатывает зеркалированный трафик и трафик по протоколу ICAP.

Аппаратные требования к компоненту Sensor, интегрированному с почтовым сервером

Максимальное количество сообщений электронной почты в секунду	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер
1–4	16	4
5–20	16	8

Для обработки трафика по протоколу ICAP требуется меньше ресурсов, чем для обработки сообщений электронной почты.

Если один компонент Sensor обрабатывает трафик по нескольким протоколам, следует учитывать следующие рекомендации:

- Одновременная обработка трафика по протоколу ICAP и со SPAN-портов рекомендуется для анализа объектов, передаваемых через прокси-сервер по протоколу HTTPS.

  Для обработки трафика по протоколу HTTPS прокси-сервер должен поддерживать смену сертификата сервера.

- При настроенной интеграции с почтовыми сенсорами нецелесообразно извлекать SMTP-трафик из SPAN-трафика.

Требования к дисковому пространству на сервере с компонентом Sensor

Рекомендуется использовать дисковый массив RAID 1. Общий объем дискового пространства должен составлять не менее 500 ГБ. Минимальные требования к свободному дисковому пространству для разных типов данных приведены в таблице ниже.

Минимальные требования к дисковому пространству на сервере с компонентом Sensor

Тип данных	Дисковое пространство (ГБ)
Дамп базы данных Redis	16
Операционная система	25
Временные файлы	32
Файлы трассировок и пакеты обновлений	151
Всего	**224**

При объеме обрабатываемого трафика более 1 Гбит/с рекомендуется выделить не менее 600 ГБ дискового пространства.

Расчеты для компонента Central Node

При развертывании программы на виртуальной платформе требуется на 10 процентов больше ресурсов процессора. В параметрах виртуального диска должен быть выбран тип диска Thick Provision.

Чтобы избежать возможного снижения производительности при развертывании приложения на виртуальной платформе, рекомендуется выполнить следующие действия:

- Установить параметры High Latency Sensitivity.
- Зарезервировать всю оперативную память.
- Зарезервировать всю частоту процессора.

Аппаратные требования к серверу с компонентами Central Node и Sensor

Аппаратные требования к серверу, на котором установлены компоненты Central Node и Sensor, зависят от следующих условий:

- объем обрабатываемого трафика;
- количество обрабатываемых сообщений электронной почты в секунду;
- количество хостов с Kaspersky Endpoint Agent.

  Программа Kaspersky Endpoint Agent может быть установлена на терминальный сервер, файловый сервер или в сетевое хранилище (NAS).

  Если программа Kaspersky Endpoint Agent установлена на терминальный сервер, расчет создаваемой программой нагрузки выполняется следующим образом: одна программа Kaspersky Endpoint Agent на терминальном сервере, обслуживающем X пользователей, дает такую же нагрузку, как X программ Kaspersky Endpoint Agent на хосте (X пользователей = X программ Kaspersky Endpoint Agent).

  Если программа Kaspersky Endpoint Agent установлена на файловый сервер или в сетевое хранилище, расчет создаваемой программой нагрузки выполняется следующим образом: одна программа Kaspersky Endpoint Agent на файловом сервере или в сетевом хранилище дает такую же нагрузку, как 20 программ Kaspersky Endpoint Agent на хосте.

При расчете количества хостов с Kaspersky Endpoint Agent требуется учитывать, что одна программа Kaspersky Endpoint Agent для Linux дает такую же нагрузку, как три программы Kaspersky Endpoint Agent для Windows.

Программа Kaspersky Endpoint Agent для Windows также может быть установлена на сервер SCADA.

Если программа Kaspersky Endpoint Agent для Windows установлена на сервер SCADA, расчет создаваемой программой нагрузки выполняется следующим образом: одна программа Kaspersky Endpoint Agent для Windows на сервере SCADA дает такую же нагрузку, как 20 программ Kaspersky Endpoint Agent для Windows на хосте.

Вы можете использовать одновременно программы Kaspersky Endpoint Agent для Linux и Kaspersky Endpoint Agent для Windows.

При объеме обрабатываемого трафика более 1 Гбит/с рекомендуется устанавливать компоненты Central Node и Sensor на отдельных серверах.

На сервере с компонентом Central Node рекомендуется использовать две дисковые подсистемы RAID:

- Первая дисковая подсистема RAID 1 или RAID 10 используется для всех данных, указанных в таблице ниже, кроме базы данных Targeted Attack Analyzer.
- Вторая дисковая подсистема RAID 10 используется для базы данных Targeted Attack Analyzer и хранения части журналов.

Kaspersky Anti Targeted Attack Platform не поддерживает работу с программным RAID-массивом.

Аппаратные требования к серверу с компонентом Central Node в зависимости от используемой функциональности представлены в таблице ниже.

Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KEDR

Максимальное количество хостов с Kaspersky Endpoint Agent для Windows	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подсистема				Вторая дисковая подсист		
			ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 1 или RAID 10 (ТБ)	Количество дисков в массиве RAID 1 или RAID 10	ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 10 (ТБ)
1000	64	8	100	1000	1	4	300	200	Не более 6 дисков по 2,4 ТБ
3000	80	12	100	1000	1	4	700	500	
5000	96	12	100	1000	1	4	1000	600	
10 000	160	20	100	1000	1	4	2000	800	
15 000	192	32	100	1000	1	4	2000	800	

Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KATA и KEDR

Максимальное количество хостов с Kaspersky Endpoint Agent для Windows	Максимальное количество сообщений электронной почты в секунду	Макисмальный объем трафика со SPAN-портов на сервере с компонентом Central Node	Максимальный объем трафика со SPAN-портов на серверах с компонентом Sensor (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер с частотой 3 ГГц	Первая дисковая подс		
						ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объ диско масс RAID 1 RAID (ТБ
1000	1	200	Не обрабатывается	96	12	100	1000	1,9
2000	2	500	Не обрабатывается	128	20	100	1000	2
5000	1	1000	Не обрабатывается	160	36	100	1000	2
10 000	2	1000	Не обрабатывается	192	40	100	1000	2
5000	5	Не обрабатывается	2000	144	20	100	1000	1,9
10 000	20	Не обрабатывается	4000	192	36	100	1000	1,9
15 000	20	Не обрабатывается	4000	256	48	100	1000	1,9

Примеры расчета требуемой конфигурации серверов с компонентами Kaspersky Anti Targeted Attack Platform

Если вы хотите:

- обрабатывать трафик с сетевого устройства с пропускной способностью до 4 Гбит/с;
- обрабатывать 20 сообщений электронной почты в секунду;
- использовать 15 000 хостов с Kaspersky Endpoint Agent для Windows **или** 5000 хостов с Kaspersky Endpoint Agent для Linux,

то вам требуется два сервера со следующими аппаратными характеристиками:

- сервер с компонентом Central Node: не менее 256 ГБ оперативной памяти и 48 логических ядер процессора;
- сервер с компонентом Sensor: не менее 32 ГБ оперативной памяти и 48 логических ядер процессора.

Указанные расчеты справедливы также для инфраструктуры с 5000 хостов с Kaspersky Endpoint Agent для Linux или при совместном использовании программ (например, 9000 хостов с Kaspersky Endpoint Agent для Windows и 2000 хостов с Kaspersky Endpoint Agent для Linux).

Требования к дисковому пространству на сервере с компонентом Central Node

При отсутствии компонента Sensor на сервере с компонентом Central Node должно быть не менее 2000 ГБ свободного пространства на первой дисковой подсистеме и не менее 2400 ГБ на второй дисковой подсистеме. Объем требуемого пространства на второй дисковой подсистеме зависит от желаемой политики хранения данных и может быть вычислен по следующей формуле:

```
150 ГБ + <количество хостов с Kaspersky Endpoint Agent для Windows>/15000 * (400 ГБ + 240 ГБ * <срок, за который требуется хранить данные, в днях>), но не более 12 ТБ
```

Эта формула может быть использована для примерной оценки требуемого дискового пространства. Реальный объем хранимых данных зависит от профиля трафика организации и может отличаться от полученного результата вычислений.

Минимальные требования к свободному дисковому пространству для каждого типа данных приведены в таблице ниже.

Минимальные требования к дисковому пространству на сервере с компонентом Central Node при отсутствии компонента Sensor

Тип данных	Первая дисковая подсистема (ГБ)	Вторая дисковая подсистема (ГБ)
База данных Targeted Attack Analyzer	0	1500
База данных обнаруженных объектов	50	0
Очереди технологий обнаружения	390	0
Очередь задач	1	0
Данные, полученные после анализа компонентом Sandbox	300	0
Карантин	300	0
Файлы, ожидающие повторной проверки	300	0
Файл дампа базы данных Redis	16	0
Операционная система	25	0
Временные файлы	64	0
Файлы трассировки	50	100
Пакеты обновлений	1	0
Всего	**1497**	**1600**

При использовании компонента Sensor на сервере с компонентом Central Node должно быть не менее 1900 ГБ свободного пространства на первой дисковой подсистеме и не менее 3900 ГБ на второй дисковой подсистеме. Минимальные требования к свободному дисковому пространству для каждого типа данных приведены в таблице ниже.

Минимальные требования к дисковому пространству на сервере с компонентом Central Node при использовании компонента Sensor

Тип данных	Первая дисковая подсистема на сервере с компонентом Central Node (ГБ)	Вторая дисковая подсистема на сервере с компонентом Central Node (ГБ)	Дисковое пространство на сервере с компонентом Sensor (ГБ)
База данных Targeted Attack Analyzer	0	1500	0
База данных обнаруженных объектов	50	0	0
Очереди технологий обнаружения	390	0	0
Очередь задач	1	0	0
Данные, полученные после анализа компонентом Sandbox	300	0	0
Карантин	300	0	0
Файлы,ожидающие повторной проверки	300	0	0
Файл дампа базы данных Redis	16	0	16
Операционная система	25	0	25
Временные файлы	32	0	32
Файлы трассировки	50	100	150
Пакеты обновлений	1	0	1
Всего	**1465**	**1600**	**224**

Если вы настроили интеграцию с внешней системой с помощью REST API, вам необходимо выделить дополнительные ресурсы для обработки объектов этой системы. Дополнительные аппаратные требования приведены в таблице ниже.

Дополнительные аппаратные требования к серверу с компонентом Central Node при наличии интегрированных внешних систем

Максимальное количество обрабатываемых объектов в секунду	Количество дополнительных логических ядер	Количество дополнительных серверов с компонентом Sandbox
8	2	1
16	4	2
24	7	3

Требования к серверу PCN в режиме распределенного решения

При небольшой нагрузке на серверы SCN аппаратные требования к серверу PCN не отличаются от требований к серверу с компонентом Central Node в автономном режиме.

Аппаратные требования к серверу PCN при наличии 10 серверов SCN с большой нагрузкой приведены в таблице ниже.

Аппаратные требования к серверу PCN

Максимальное количество хостов с Kaspersky Endpoint Agent для Windows	Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Первая дисковая подсистема			
					ROPS (чтение, операций в секунду)	WOPS (запись, операций в секунду)	Объем дискового массива RAID 1 или RAID 10 (ТБ)	Количество дисков в массиве RAID 1 или RAID 10
10 000	0	0	160	24	100	1000	1	4
1000	1	200	112	40	100	1000	1,9	4
5000	5	2000	160	28	100	1000	1,9	4
10 000	20	4000	208	40	100	1000	1,9	4

Требования к каналам связи

Минимальные требования к каналу связи между компьютерами с компонентом Endpoint Agent и сервером с компонентом Central Node приведены в таблице ниже.

Минимальные требования к каналу связи между компьютерами с компонентом Endpoint Agent и сервером с компонентом Central Node

Максимальное количество хостов с Kaspersky Endpoint Agent для Windows	Требуемая пропускная способность канала связи, зарезервированная для компонентов Endpoint Agent для Windows (Мбит/с)
10	1
50	2
100	3
1000	20
10 000	200

Минимальные требования к каналу связи между серверами PCN и SCN в режиме распределенного решения приведены в таблице ниже.

Минимальные требования к каналу связи между серверами PCN и SCN

Максимальное количество хостов с Kaspersky Endpoint Agent для Windows	Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Требуемая пропускная способность канала связи (Мбит/с)
5000	5	2000	20
10 000	20	4000	30

Аппаратные требования к серверам кластера Central Node

Кластер должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. Если вы хотите обрабатывать трафик от 15 000 хостов с программой Kaspersky Endpoint Agent, вам нужно минимум 2 сервера хранения и 2 обрабатывающих сервера. Для обработки трафика от 30 000 хостов с программой Kaspersky Endpoint Agent вам требуется не менее 2 серверов хранения и 3 обрабатывающих серверов.

Каждый сервер кластера должен иметь два сетевых адаптера для настройки кластерной и внешней подсети. Кластерная подсеть должна функционировать со скоростью 10 Гбит/с. Внешняя подсеть должна функционировать со скоростью 1 Гбит/с.

Для кластерной подсети также должны выполняться следующие требования:

- В кластерную подсеть должны входить только серверы кластера и сетевые коммутаторы.
- Серверы кластера должны находиться в одном L1- или L2-сегменте. Для этого вы можете подключить все серверы кластера к одному коммутатору или использовать программное туннелирование. Например, L2TPv3 или Overlay Transport Virtualization (OTV).
- Значение сетевой задержки ("network latency") должно удовлетворять требованию "single digit latency", то есть в миллисекундах значение должно быть менее 10.

Аппаратные требования к серверам кластера при использовании функциональности KEDR приведены в таблице ниже.

Аппаратные требования к обрабатывающим серверам при использовании функциональности KEDR

Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Тип массива RAID	Количество дисков в массиве RAID	Объем одного жесткого диска (ГБ)
256	48	RAID 1	2	1200

Аппаратные требования к серверам хранения при использовании функциональности KEDR

Минимальный объем оперативной памяти (ГБ)	Минимальное количество логических ядер	Первая дисковая подсистема			Вторая дисковая подсистема	
		Тип массива RAID	Количество дисков в массиве RAID	Объем одного жесткого диска (ГБ)	Количество дисков	Объем одного жесткого диска (ГБ)
128	16	RAID 1	2	1200	6	1200

Требования к скорости дисковых подсистем аналогичны требованиям, указанным в таблице *Аппаратные требования к серверу с компонентом Central Node при использовании функциональности KEDR* (см. выше).

Расчеты для компонента Sandbox

Аппаратные требования к серверу с компонентом Sandbox зависят от типа и объема обрабатываемого трафика и от допустимого времени проверки объекта.

По умолчанию допустимое время проверки объекта составляет 1 час. Для уменьшения этого времени требуется более мощный сервер или большее количество серверов с компонентом Sandbox.

Рекомендуется рассчитывать конфигурацию компонента Sandbox следующим образом:

1. Установите компоненты Central Node и Sensor на одном сервере и компонент Sandbox на другом сервере для пилотирования программы.

   Для получения достаточных статистических данных необходимо, чтобы программа обрабатывала трафик организации в течение недели.

2. Запустите скрипт для записи данных, выполнив команды:

   ```
   kata-collect --output-dir path-to-folder
   ```

   ```
   --output-dir <путь к директории>
   ```

   Когда скрипт завершит работу, в указанную директорию будет помещен архив *collect.tar.gz*.

3. Передайте этот архив для анализа сотрудникам "Лаборатории Касперского".

   При одновременном запуске нескольких виртуальных машин скорость обработки объектов из очереди увеличивается.

Аппаратные требования к серверу с компонентом Sandbox

Расчет количества серверов с компонентом Sandbox в зависимости от нагрузки приведен в таблице ниже.

Аппаратные требования к компоненту Sandbox в зависимости от объема обрабатываемого трафика

Максимальное количество сообщений электронной почты в секунду	Максимальный объем трафика со SPAN-портов (Мбит/с)	Максимальное количество компьютеров с Kaspersky Endpoint Agent для Windows	Количество физических серверов с компонентом Sandbox	
			При использовании трех образов с ОС Windows	При использовании трех образов с ОС Windows и одного образа с ОС Linux
1	200	1000	1	1
2	500	3000	1	1
1	1000	5000	1	1
5	2000	5000	1	1
20	4000	10000	2	3

Оценка количества компонентов Sandbox приведена для серверов следующей конфигурации:

- При установке компонента Sandbox на физический сервер:
  - 2 процессора Intel® Xeon® 8 Core™ (HT) с частотой 2,6 ГГц или выше.
  - 80 ГБ оперативной памяти.
  - 2 HDD объемом 300 ГБ каждый, объединенные в массив RAID 1.
- При установке компонента Sandbox на виртуальную машину VMware ESXi:
  - Процессор Intel Xeon 15 Core (HT) с частотой 2,1 ГГц или выше;
  - 32 ГБ оперативной памяти;
  - HDD объемом 300 ГБ.

    На виртуальной машине:

    1. Разрешена вложенная виртуализация.
    2. Установлены параметры High Latency Sensitivity.
    3. Зарезервирована вся оперативная память.
    4. Зарезервирована вся частота процессора.

При установке компонента Sandbox на виртуальную машину VMware ESXi нужно установить ограничение для количества одновременно запускаемых виртуальных машин – 12.

3-4 виртуальные машины компонента Sandbox обеспечивают такую же производительность, как один компонент Sandbox на физическом сервере.

Установка и первоначальная настройка программы

В этом разделе содержатся инструкции по установке и первоначальной настройке Kaspersky Anti Targeted Attack Platform.

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 программа Kaspersky Endpoint Agent, удовлетворяют аппаратным и программным требованиям.

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 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 входящие соединения к серверу с компонентом Central Node на следующие порты:

   - TCP 22 для подключения к серверу по SSH.
   - TCP 443 для получения данных от компьютеров с программой Kaspersky Endpoint Agent.
   - TCP 8443 для просмотра результатов проверки в веб-интерфейсе программы.
   - UDP 53 для связи с сервером с компонентом Sensor.

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

   - TCP 80, 443 и 1443 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.
   - UDP 53 для связи с сервером с компонентом Sensor.

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 компьютеров с Kaspersky Endpoint Agent на сервер с компонентом Central Node.
   - UDP 53 для связи с сервером с компонентом Central Node.

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

   - TCP 80 и 443 для связи с серверами службы KSN и серверами обновлений "Лаборатории Касперского".
   - TCP 995 (или TCP 110 для незащищенных соединений) для интеграции с почтовым сервером.
   - UDP 53 для связи с сервером с компонентом Central Node.

   При установке дополнительного 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 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 протоколов ESP, AH, IKEv1 и IKEv2.

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

   a. Разрешите входящее соединение сервера с ролью PCN на порты 8443.

   b. Разрешите на сетевом оборудовании установку шифрованного канала связи между серверами PCN и SCN.

      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:

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:

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:

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:

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:

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

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

Виртуальная машина будет готова к установке компонента Sandbox.

Порядок установки и настройки компонентов программы

Установка и настройка программы состоит из следующих этапов:

1. Установка образа диска с компонентом Sandbox
2. Настройка компонента Sandbox через веб-интерфейс Sandbox
3. Установка образов дисков операционных систем Microsoft Windows и программ для работы компонента Sandbox
4. **Установка компонентов Central Node и Sensor**

   Вы можете установить компоненты Central Node и Sensor в одной из следующих конфигураций:

   - Кластер.
   - Сервер.

   При наличии нескольких компонентов Central Node вы можете использовать программу в режиме распределенного решения.
5. Установка компонента Sensor

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

6. Настройка компонентов Central Node и Sensor

7. **Установка программы Kaspersky Endpoint Agent для Windows или Kaspersky Endpoint Agent для Linux на компьютеры, входящие в IT-инфраструктуру организации**

   Вы можете использовать программу Kaspersky Endpoint Agent в следующих конфигурациях:

   - Без интеграции с программой EPP.

     В этом случае вам требуется установить только программу Kaspersky Endpoint Agent для Windows или программу Kaspersky Endpoint Agent для Linux.

   - Настроив интеграцию с программой EPP.

     В этом случае Kaspersky Endpoint Agent также передает на сервер Central Node данные об угрозах, обнаруженных программой EPP, и о результатах обработки угроз этой программой.

   Kaspersky Endpoint Agent для Windows может интегрироваться со следующими программами EPP:

   - Kaspersky Endpoint Security для Windows.

     Интеграция Kaspersky Endpoint Agent для Windows с Kaspersky Endpoint Security для Windows

     Для интеграции программ вам требуется установить Kaspersky Endpoint Agent в составе Kaspersky Endpoint Security. Возможность настроить интеграцию для отдельно установленных программ не предусмотрена.

     Чтобы установить Kaspersky Endpoint Agent в составе Kaspersky Endpoint Security:

     1. Запустите установку программы Kaspersky Endpoint Security, в комплект поставки которой входит Kaspersky Endpoint Agent.

        Подробнее об установке Kaspersky Endpoint Security см. в *справке Kaspersky Endpoint Security для Windows*.

     2. При установке выберите компонент Endpoint Agent.

     После установки программы с компонентом Endpoint Agent в список установленных программ будут добавлены Kaspersky Endpoint Security и Kaspersky Endpoint Agent.

     При необходимости вы можете обновить программу Kaspersky Endpoint Agent, уже установленную в составе Kaspersky Endpoint Security. Интеграция между совместимыми версиями программ сохранится как при обновлении программы Kaspersky Endpoint Agent, так и при обновлении программы Kaspersky Endpoint Security. Обновление с предыдущей версии Kaspersky Endpoint Agent до версии 3.12 доступно для Kaspersky Endpoint Agent версии 3.7 и выше.

   - Kaspersky Security для Windows Server.

     Интеграция Kaspersky Endpoint Agent для Windows с Kaspersky Security для Windows Server

     Для интеграции программ вам требуется установить Kaspersky Endpoint Agent в составе Kaspersky Security для Windows Server. Возможность настроить интеграцию для отдельно установленных программ не предусмотрена.

Чтобы установить Kaspersky Endpoint Agent в составе Kaspersky Security для Windows Server:

1. Запустите установку программы Kaspersky Security для Windows Server, в комплект поставки которой входит Kaspersky Endpoint Agent.

   Подробнее об установке Kaspersky Security для Windows Server см. в *справке Kaspersky Security для Windows Server*.

2. При установке выберите компонент Kaspersky Endpoint Agent.

После установки программы с компонентом Kaspersky Endpoint Agent в список установленных программ будут добавлены Kaspersky Security для Windows Server и Kaspersky Endpoint Agent.

При необходимости вы можете обновить программу Kaspersky Endpoint Agent, уже установленную в составе Kaspersky Security для Windows Server. Интеграция между совместимыми версиями программ сохранится как при обновлении программы Kaspersky Endpoint Agent, так и при обновлении программы Kaspersky Security для Windows Server.

- Kaspersky Security для виртуальных сред Легкий агент.

  Интеграция Kaspersky Endpoint Agent для Windows с Kaspersky Security для виртуальных сред Легкий агент

  Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент устанавливаются отдельно. Установка Kaspersky Endpoint Agent в составе Kaspersky Security для виртуальных сред Легкий агент не предусмотрена.

  Чтобы включить интеграцию Kaspersky Endpoint Agent с Kaspersky Security для виртуальных сред Легкий агент:

  1. Установите программу Kaspersky Security для виртуальных сред Легкий агент, если программа не была установлена ранее.

  2. Включите интеграцию Легкого агента с Kaspersky Endpoint Agent.

     Вы можете включить интеграцию с Kaspersky Endpoint Agent во время установки или обновления Легкого агента. Вы также можете включить интеграцию с Kaspersky Endpoint Agent с помощью процедуры изменения состава установленных компонентов Легкого агента.

     Подробнее об установке, включении интеграции и обновлении программы, а также о процедуре изменения состава установленных компонентов программы см. в *Справке Kaspersky Security для виртуальных сред Легкий агент*.

  3. На виртуальную машину с установленным Легким агентом установите программу Kaspersky Endpoint Agent, если она не была установлена ранее.

  Для интеграции с Kaspersky Security для виртуальных сред 5.2 Легкий агент рекомендуется использовать Kaspersky Endpoint Agent 3.12. При необходимости вы можете обновить программу Kaspersky Endpoint Agent и Kaspersky Security для виртуальных сред Легкий агент. При обновлении интеграция между совместимыми версиями программ сохранится.

- Kaspersky Industrial CyberSecurity for Nodes.

  Интеграция Kaspersky Endpoint Agent для Windows с Kaspersky Industrial CyberSecurity for Nodes

Чтобы включить интеграцию Kaspersky Endpoint Agent с Kaspersky Industrial CyberSecurity for Nodes:

1. Установите программу Kaspersky Industrial CyberSecurity for Nodes, если программа не была установлена ранее.

   Подробнее об установке см. в *справке Kaspersky Industrial CyberSecurity for Nodes*.

2. Установите на том же устройстве программу Kaspersky Endpoint Agent, если она не была установлена ранее.

Программы интегрируются автоматически.

Для интеграции с Kaspersky Industrial CyberSecurity for Nodes в Kaspersky Endpoint Agent должен быть установлен соответствующий лицензионный ключ.

Для получения детальной информации вы можете обратиться к вашему аккаунт-менеджеру.

Kaspersky Endpoint Agent для Linux может интегрироваться с EPP-системой Kaspersky Endpoint Security для Linux.

Интеграция Kaspersky Endpoint Agent для Linux с Kaspersky Endpoint Security для Linux

Для интеграции Kaspersky Endpoint Agent для Linux и Kaspersky Endpoint Security для Linux вы можете использовать программы, установленные отдельно.

Чтобы включить интеграцию Kaspersky Endpoint Agent с Kaspersky Endpoint Security:

1. Установите Kaspersky Endpoint Security.

   Подробнее об установке программы см. в *справке Kaspersky Endpoint Security для Linux*.

2. Выполните следующие действия:

   a. Если программа Kaspersky Endpoint Agent не была установлена ранее, установите Kaspersky Endpoint Agent.

      Интеграция между программами будет включена автоматически.

   b. Если программа Kaspersky Endpoint Agent была установлена ранее, включите интеграцию между программами.

      Для этого вам требуется включить запись информации о событиях в syslog для Kaspersky Endpoint Security для Linux.

      Подробнее об изменении параметров программы см. в *Справке Kaspersky Endpoint Security для Linux*.

При необходимости вы можете обновить программу Kaspersky Endpoint Agent и Kaspersky Endpoint Security для Linux. При обновлении интеграция между совместимыми версиями программ сохранится.

Установка компонента Sandbox

Этот раздел представляет собой пошаговую инструкцию по установке компонента Sandbox.

Чтобы приступить к установке компонента Sandbox, выполните следующие действия:

1. Запустите образ диска с компонентом Sandbox.

   Запустится мастер установки.

2. Нажмите на кнопку **Ok**.

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:

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

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

   Откроется окно с текстом Лицензионного соглашения.

2. Ознакомьтесь с Лицензионным соглашением.

3. Если вы принимаете условия Лицензионного соглашения, нажмите на кнопку **I accept**.

   Откроется окно с текстом Политики конфиденциальности.

4. Ознакомьтесь с Политикой конфиденциальности.

5. Если вы принимаете условия Политики конфиденциальности, нажмите на кнопку **I accept**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор диска для установки компонента Sandbox

Выберите физический диск для установки компонента Sandbox.

Чтобы выбрать диск для установки компонента Sandbox:

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

   Если диск не пустой, отобразится окно подтверждения форматирования этого диска и установки программы на него.

2. Нажмите на кнопку **Install**.

   Архив с установочными файлами распакуется на диск. Сервер перезагрузится.

Мастер установки перейдет к следующему шагу.

Шаг 3. Назначение имени хоста

Назначьте имя хоста сервера для использования DNS-серверами.

Чтобы назначить имя хоста сервера:

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

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

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор управляющего сетевого интерфейса в списке

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

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

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

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

Выберите сетевой интерфейс, который вы хотите использовать в качестве управляющего.

Чтобы выбрать управляющий сетевой интерфейс:

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:

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

Мастер установки перейдет к следующему шагу.

Шаг 6. Добавление адресов DNS-серверов

Чтобы добавить адреса DNS-серверов:

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

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

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

Мастер установки перейдет к следующему шагу.

Шаг 7. Настройка статического сетевого маршрута

Чтобы настроить статический сетевой маршрут:

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

   Откроется окно **IPv4 Static Route**.
2. В поле **Address/Mask** введите IP-адрес и маску подсети, для которой вы хотите настроить сетевой маршрут.
3. Если вы хотите использовать сетевой маршрут по умолчанию, введите 0.0.0.0/0.
4. В поле **Gateway** введите IP-адрес шлюза.

5. Нажмите на кнопку **Ok**.

6. Если вы хотите добавить другие сетевые маршруты, повторите действия в окне **IPv4 Static Route**.

7. Когда вы закончите добавлять сетевые маршруты, нажмите на кнопку **Continue**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Настройка минимальной длины пароля администратора Sandbox

Чтобы задать минимальную длину пароля администратора компонента Sandbox:

1. В поле **Minimal length** введите количество символов. Рекомендуется использовать пароли длиной 12 и более символов.

2. Нажмите на кнопку **Ok**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Создание учетной записи администратора Sandbox

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:

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

2. В поле **Password** введите пароль учетной записи администратора.

   Пароль должен удовлетворять следующим требованиям:

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

3. В поле **Confirm password** введите пароль повторно.

4. Нажмите на кнопку **Ok**.

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

Сервер Sandbox перезагрузится.

Перейдите к настройке компонента Sandbox через веб-интерфейс.

Развертывание компонентов Central Node и Sensor в виде кластера

Развертывание компонентов Central Node и Sensor в виде кластера включает следующие этапы:

1. **Развертывание первого сервера хранения**

   Первым требуется развернуть сервер хранения. После того, как он будет развернут, вы можете добавить в кластер дополнительные серверы хранения и обрабатывающие серверы.

   > Кластер должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. Чтобы определить подходящее для вашей организации количество серверов, вы можете воспользоваться руководством по масштабированию.

2. **Развертывание обрабатывающих серверов** и **дополнительных серверов хранения**

   Вы можете разворачивать серверы в произвольном порядке.

3. **Настройка параметров масштабирования программы**

   На завершающем этапе развертывания кластера вам нужно настроить параметры масштабирования программы: указать планируемый объем SPAN-трафика, почтового трафика, количество хостов с Kaspersky Endpoint Agent, а также размер Хранилища и базы событий.

> Компонент Central Node всегда устанавливается вместе с компонентом Sensor. Если вам требуется использовать компонент Central Node отдельно, при развертывании обрабатывающего сервера откажитесь от получения зеркалированного трафика со SPAN-портов на шаге 10.

Развертывание сервера хранения данных

Для развертывания сервера хранения данных вам нужно запустить образ диска с компонентами Central Node и Sensor.

> Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки.

Шаг 1. Выбор роли сервера

Чтобы выбрать роль сервера:

1. Введите одно из следующих чисел:

   - 1 – сервер хранения для развертывания компонента Central Node в виде кластера.
   - 2 – обрабатывающий сервер для развертывания компонента Central Node в виде кластера.

     Роль включает также установку и настройку компонента Sensor.

   - 3 – компоненты Central Node и Sensor для установки на одном сервере.
   - 4 – компонент Sensor для установки на отдельном сервере.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор режима развертывания

Чтобы выбрать режим развертывания:

1. Введите одно из следующих чисел:

   - **1**.

     Это значение нужно выбрать при развертывании первого сервера кластера.

   - **2**.

     Это значение нужно выбрать при развертывании сервера, который будет добавлен в существующий кластер.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

Чтобы выбрать диск для установки компонента:

1. Введите номер требуемого диска.
2. Нажмите на клавишу **Enter**.

3. Выполните следующие действия:

   - Введите **y**, если вы хотите подтвердить выбор диска.
   - Введите **n**, если вы хотите выбрать другой диск.

4. Если вы выбрали **n**, повторите шаги 1-2 этой инструкции.

Мастер установки перейдет к следующему шагу.

Шаг 4. Просмотр 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.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности:

1. Нажмите на клавишу **Enter**.
2. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑ и ↓, PageUp и PageDown или клавишу **Enter**.

3. Если вы согласны с Лицензионным соглашением и Политикой конфиденциальности, выберите кнопку **I accept** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации серверов кластера

Чтобы указать маску сети для адресации серверов кластера:

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.

- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор маски сети для адресации компонентов программы

На этом шаге вам нужно указать маску сети для адресации основных компонентов программы (сервисов), которые будут функционировать на серверах с компонентом Central Node.

Сеть для адресации компонентов программы не должна пересекаться с сетью для адресации серверов кластера.

Чтобы указать маску сети для адресации основных компонентов программы:

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.19.0.0/16.

- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор кластерного сетевого интерфейса

Кластерный сетевой интерфейс используется для взаимодействия между серверами кластера.

Чтобы выбрать кластерный сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внутренней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

Чтобы выбрать внешний сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов

Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В открывшемся окне выберите один из следующих вариантов:

   - **dhcp**.
   - **static**.

3. Если вы выбрали **static**, выполните следующие действия:

   a. Выберите строку с параметром и нажмите на клавишу **Enter**.

   b. В открывшемся окне введите требуемые данные и дважды нажмите на клавишу **Enter**.

   > Вам нужно указать значение для каждого параметра.

4. Выберите строку **Save**.

5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Создание учетной записи администратора и аутентификация сервера в кластере

На этом шаге вам нужно выполнить одно из следующих действий:

- Создать учетную запись администратора, если вы разворачиваете первый сервер кластера.
- Аутентифицировать сервер в кластере, если вы разворачиваете дополнительные серверы хранения.

Создание учетной записи администратора

> Создание учетной записи администратора требуется только при развертывании первого сервера кластера. Если вы разворачиваете дополнительный сервер хранения, вместо окна для создания учетной записи администратора программа предлагает аутентифицировать сервер в кластере.

При развертывании первого сервера кластера вам нужно создать учетную запись администратора. Эта учетная запись используется для работы в веб-интерфейсе для управления масштабированием, меню администратора программы и для работы с программой в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

Чтобы задать пароль для учетной записи администратора:

1. В поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В поле **confirm** введите пароль повторно.

3. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Аутентификация сервера в кластере

Аутентификация сервера в кластере требуется только при развертывании дополнительных серверов хранения. Если вы разворачиваете первый сервер кластера, вместо аутентификации сервера программа предлагает создать учетную запись администратора.

Для аутентификации сервера в кластере вам нужно ввести пароль для учетной записи admin, заданный при развертывании первого сервера кластера.

Чтобы аутентифицировать сервер в кластере:

1. В поле **password** введите пароль учетной записи администратора.

2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Для выбора кнопки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

Сервер кластера будет аутентифицирован. Мастер установки перейдет к следующему шагу.

Шаг 11. Добавление адресов DNS-серверов

Настройте параметры DNS для работы серверов с компонентами программы.

Чтобы добавить адреса DNS-серверов:

1. Введите IP-адрес основного DNS-сервера в формате IPv4.

   Вам требуется ввести хотя бы один адрес DNS-сервера.

2. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, нажмите на клавишу **Enter** и введите адрес сервера.

3. Когда вы добавите все DNS-серверы, дважды нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 12. Выбор дисков для Ceph-хранилища

Выберите диски для Ceph-хранилища. Количество дисков определяется в соответствии с руководством по масштабированию.

Чтобы выбрать диски для Ceph-хранилища:

1. Выберите строку с требуемым диском.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

3. Повторите шаги 1–2 для выбора следующих дисков.

Настройка займет какое-то время. После этого установка завершится. Вы можете перейти к настройке конфигурации серверов кластера в веб-интерфейсе для управления масштабированием.

Развертывание обрабатывающего сервера

Для развертывания обрабатывающего сервера вам нужно запустить образ диска с компонентами Central Node и Sensor.

Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки.

Шаг 1. Выбор роли сервера

Чтобы выбрать роль сервера:

1. Введите одно из следующих чисел:

   - 1 – сервер хранения для развертывания компонента Central Node в виде кластера.
   - 2 – обрабатывающий сервер для развертывания компонента Central Node в виде кластера.

     Роль включает также установку и настройку компонента Sensor.

- 3 – компоненты Central Node и Sensor для установки на одном сервере.
- 4 – компонент Sensor для установки на отдельном сервере.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Выбор режима развертывания

Чтобы выбрать режим развертывания:

1. Введите одно из следующих чисел:
   - **1**.

     Это значение нужно выбрать при развертывании первого сервера кластера.
   - **2**.

     Это значение нужно выбрать при развертывании сервера, который будет добавлен в существующий кластер.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

Чтобы выбрать диск для установки компонента:

1. Введите номер требуемого диска.
2. Нажмите на клавишу **Enter**.
3. Выполните следующие действия:
   - Введите **y**, если вы хотите подтвердить выбор диска.
   - Введите **n**, если вы хотите выбрать другой диск.
4. Если вы выбрали **n**, повторите шаги 1-2 этой инструкции.

Мастер установки перейдет к следующему шагу.

Шаг 4. Просмотр 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.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности:

1. Нажмите на клавишу **Enter**.
2. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑ и ↓, PageUp и PageDown или клавишу **Enter**.
3. Если вы согласны с Лицензионным соглашением и Политикой конфиденциальности, выберите кнопку **I accept** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации серверов кластера

Чтобы указать маску сети для адресации серверов кластера:

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.
- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор маски сети для адресации компонентов программы

На этом шаге вам нужно указать маску сети для адресации основных компонентов программы (сервисов), которые будут функционировать на серверах с компонентом Central Node.

Сеть для адресации компонентов программы не должна пересекаться с сетью для адресации серверов кластера.

Чтобы указать маску сети для адресации основных компонентов программы:

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.19.0.0/16.
- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор кластерного сетевого интерфейса

Кластерный сетевой интерфейс используется для взаимодействия между серверами кластера.

Чтобы выбрать кластерный сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внутренней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

Чтобы выбрать внешний сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Выбор способа получения IP-адресов для сетевых интерфейсов

Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В открывшемся окне выберите один из следующих вариантов:

   - **dhcp**.
   - **static**.

3. Если вы выбрали **static**, выполните следующие действия:

   a. Выберите строку с параметром и нажмите на клавишу **Enter**.

   b. В открывшемся окне введите требуемые данные и дважды нажмите на клавишу **Enter**.

   Вам нужно указать значение для каждого параметра.

4. Выберите строку **Save**.

5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 10. Аутентификация сервера в кластере

Для аутентификации сервера в кластере вам нужно ввести пароль для учетной записи admin, заданный при развертывании первого сервера кластера.

Чтобы аутентифицировать сервер в кластере:

1. В поле **password** введите пароль учетной записи администратора.

2. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

   Для выбора кнопки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown.

Сервер кластера будет аутентифицирован. Мастер установки перейдет к следующему шагу.

Шаг 11. Настройка получения зеркалированного трафика со SPAN-портов

Чтобы включить получение зеркалированного трафика со SPAN-портов:

1. Введите **y**.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Чтобы отказаться от получения зеркалированного трафика со SPAN-портов:

1. Введите **n**.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 12. Добавление адресов DNS-серверов

Настройте параметры DNS для работы серверов с компонентами программы.

Чтобы добавить адреса DNS-серверов:

1. Введите IP-адрес основного DNS-сервера в формате IPv4.

> Вам требуется ввести хотя бы один адрес DNS-сервера.

2. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, нажмите на клавишу **Enter** и введите адрес сервера.

3. Когда вы добавите все DNS-серверы, дважды нажмите на клавишу **Enter**.

Установка завершится. Вы можете перейти к настройке конфигурации серверов кластера в веб-интерфейсе для управления масштабированием.

Установка компонентов Central Node и Sensor на сервере

Развертывание компонентов Central Node и Sensor на одном сервере включает следующие этапы:

1. **Установка компонентов Central Node и Sensor**

   Для установки компонентов на физическом сервере вам нужно запустить образ диска с компонентами Central Node и Sensor.

   Для установки компонентов на виртуальном сервере вам нужно подключить образ диска с компонентами Central Node и Sensor к выбранной виртуальной машине и запустить ее. Установка запускается сразу после включения виртуальной машины. Вы можете управлять процессом установки с помощью консоли виртуальной машины.

   > При установке компонентов на виртуальной машине требуется выбрать для виртуальной машины режим загрузки BIOS: Options → Boot Options → Firmware → BIOS.

2. **Настройка параметров масштабирования программы**

   На завершающем этапе развертывания кластера вам нужно настроить параметры масштабирования программы: указать планируемый объем SPAN-трафика, почтового трафика, количество хостов с Kaspersky Endpoint Agent, а также размер Хранилища и базы событий.

> Компонент Central Node всегда устанавливается вместе с компонентом Sensor. Если вам требуется использовать компонент Central Node отдельно, откажитесь от получения зеркалированного трафика со SPAN-портов на шаге 10.

> Если при выполнении шагов мастера установки возникла ошибка, обратитесь в Службу технической поддержки.

Шаг 1. Выбор роли сервера

Чтобы выбрать роль сервера:

1. Введите одно из следующих чисел:

   - 1 – сервер хранения для развертывания компонента Central Node в виде кластера.
   - 2 – обрабатывающий сервер для развертывания компонента Central Node в виде кластера.

     Роль включает также установку и настройку компонента Sensor.

   - 3 – компоненты Central Node и Sensor для установки на одном сервере.
   - 4 – компонент Sensor для установки на отдельном сервере.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Просмотр 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.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности:

1. Нажмите на клавишу **Enter**.
2. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑ и ↓, PageUp и PageDown или клавишу **Enter**.

3. Если вы согласны с Лицензионным соглашением и Политикой конфиденциальности, выберите кнопку **I accept** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

Чтобы выбрать диск для установки компонента:

1. Введите номер требуемого диска.
2. Нажмите на клавишу **Enter**.
3. Выполните следующие действия:
   - Введите **y**, если вы хотите подтвердить выбор диска.
   - Введите **n**, если вы хотите выбрать другой диск.
4. Если вы выбрали **n**, повторите шаги 1-2 этой инструкции.

Мастер установки перейдет к следующему шагу.

Шаг 4. 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 выделить диск для базы данных компонента Targeted Attack Analyzer:

1. Введите **y**.
2. Нажмите на клавишу **Enter**.
3. Введите номер требуемого диска.
4. Нажмите на клавишу **Enter**.
5. Выполните следующие действия:
   - Введите **y**, если вы хотите подтвердить выбор диска.
   - Введите **n**, если вы хотите выбрать другой диск.
6. Если вы выбрали **n**, повторите шаги 4-5 этой инструкции.

Мастер установки перейдет к следующему шагу.

Чтобы отказаться от выделения диска для базы данных компонента Targeted Attack Analyzer:

1. Введите **n**.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Выбор маски сети для адресации серверов кластера

Чтобы указать маску сети для адресации серверов кластера:

- Если вы хотите использовать предустановленное значение для маски сети, нажмите на клавишу **Enter**.

  Значение по умолчанию: 198.18.0.0/16.

- Если вы хотите указать другую маску сети, введите значение и нажмите на клавишу **Enter**.

  Маска должна соответствовать шаблону x.x.0.0/16.

Мастер установки перейдет к следующему шагу.

Шаг 6. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

Чтобы выбрать внешний сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 7. Выбор способа получения IP-адресов для сетевых интерфейсов

Чтобы выбрать способ получения IP-адреса для сетевых интерфейсов:

1. Выберите строку **Configuration type:** и нажмите на клавишу **Enter**.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В открывшемся окне выберите один из следующих вариантов:

   - **dhcp**.
   - **static**.

3. Если вы выбрали **static**, выполните следующие действия:

   a. Выберите строку с параметром и нажмите на клавишу **Enter**.

   b. В открывшемся окне введите требуемые данные и дважды нажмите на клавишу **Enter**.

   > Вам нужно указать значение для каждого параметра.

4. Выберите строку **Save**.

5. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 8. Создание учетной записи администратора

Учетная запись администратора используется для работы в веб-интерфейсе для управления масштабированием, меню администратора программы и для работы с программой в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

Чтобы задать пароль для учетной записи администратора:

1. В поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В поле **confirm** введите пароль повторно.

3. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 9. Добавление адресов DNS-серверов

Настройте параметры DNS для работы серверов с компонентами программы.

Чтобы добавить адреса DNS-серверов:

1. Введите IP-адрес основного DNS-сервера в формате IPv4.

   Вам требуется ввести хотя бы один адрес DNS-сервера.

2. Если вы хотите добавить IP-адрес дополнительного DNS-сервера, нажмите на клавишу **Enter** и введите адрес сервера.

3. Когда вы добавите все DNS-серверы, дважды нажмите на клавишу **Enter**.

   Мастер установки перейдет к следующему шагу.

Шаг 10. Настройка получения зеркалированного трафика со SPAN-портов

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

Чтобы включить получение зеркалированного трафика со SPAN-портов:

1. Введите **y**.

2. Нажмите на клавишу **Enter**.

   Мастер установки перейдет к следующему шагу.

Чтобы отказаться от получения зеркалированного трафика со SPAN-портов:

1. Введите **n**.

2. Нажмите на клавишу **Enter**.

   Мастер установки перейдет к следующему шагу.

Шаг 11. Настройка синхронизации времени с NTP-сервером

Настройте синхронизацию времени сервера с NTP-сервером.

Чтобы настроить синхронизацию времени с NTP-сервером:

1. Введите IP-адрес или имя NTP-сервера.

2. Если вы хотите добавить дополнительный NTP-сервер, нажмите на клавишу **Enter** и введите IP-адрес или имя NTP-сервера.

3. Когда вы добавите все NTP-серверы, дважды нажмите на клавишу **Enter**.

   Настройка займет какое-то время. После этого установка завершится. Вы можете перейти к настройке конфигурации сервера в веб-интерфейсе для управления масштабированием.

Установка компонента Sensor на отдельном сервере

Для установки компонента Sensor на физическом сервере вам нужно запустить образ диска с компонентами Central Node и Sensor.

Для установки компонента Sensor на виртуальном сервере вам нужно подключить образ диска с компонентами Central Node и Sensor к выбранной виртуальной машине и запустить ее. Установка запускается сразу после включения виртуальной машины. Вы можете управлять процессом установки с помощью консоли виртуальной машины.

Шаг 1. Выбор роли сервера

Чтобы выбрать роль сервера:

1. Введите одно из следующих чисел:

   - 1 – сервер хранения для развертывания компонента Central Node в виде кластера.
   - 2 – обрабатывающий сервер для развертывания компонента Central Node в виде кластера.

     Роль включает также установку и настройку компонента Sensor.

   - 3 – компоненты Central Node и Sensor для установки на одном сервере.
   - 4 – компонент Sensor для установки на отдельном сервере.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 2. Просмотр 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.

Чтобы принять условия Лицензионного соглашения и Политики конфиденциальности:

1. Нажмите на клавишу **Enter**.
2. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности.

   Для перемещения вверх и вниз вы можете использовать клавиши ↑ и ↓, PageUp и PageDown или клавишу **Enter**.
3. Если вы согласны с Лицензионным соглашением и Политикой конфиденциальности, выберите кнопку **I accept** и нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 3. Выбор диска для установки компонента

Чтобы выбрать диск для установки компонента:

1. Введите номер требуемого диска.
2. Нажмите на клавишу **Enter**.
3. Выполните следующие действия:
   - Введите **y**, если вы хотите подтвердить выбор диска.
   - Введите **n**, если вы хотите выбрать другой диск.
4. Если вы выбрали **n**, повторите шаги 1-2 этой инструкции.

Мастер установки перейдет к следующему шагу.

Шаг 4. Выбор внешнего сетевого интерфейса

Внешний сетевой интерфейс используется для доступа к серверу по протоколу SSH, работы в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и других внешних подключений.

Чтобы выбрать внешний сетевой интерфейс:

1. Выберите строку с сетевым интерфейсом, который используется для внешней сети.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.
2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 5. Подключение к серверу с компонентом Central Node

Чтобы подключиться к серверу, на котором вы установили компонент Central Node:

1. В поле Central Node введите IP-адрес или URL-адрес сервера с компонентом Central Node.

   Если компонент Central Node развернут в виде кластера, вы можете ввести IP-адрес любого сервера кластера.

2. Нажмите на клавишу **Enter**.

Мастер установки перейдет к следующему шагу.

Шаг 6. Создание учетной записи администратора

Учетная запись администратора используется для работы с компонентом Sensor в меню администратора программы и в режиме Technical Support Mode.

По умолчанию в качестве имени пользователя для учетной записи администратора используется *admin*. Вам требуется задать пароль для этой учетной записи.

Чтобы задать пароль для учетной записи администратора:

1. В поле **password** введите пароль учетной записи администратора.

   Для выбора строки вы можете использовать клавиши ↑, ↓ и PageUp, PageDown. Выбранная строка подсвечивается красным.

2. В поле **confirm** введите пароль повторно.

3. Выберите кнопку **Ok** и нажмите на клавишу **Enter**.

Установка будет завершена.

Настройка параметров масштабирования программы

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Вы можете изменить объем нагрузки на компонент Central Node. Например, подключить к нему дополнительные хосты с программой Kaspersky Endpoint Agent или серверы с компонентом Sensor. В этом случае вам нужно указать планируемый объем SPAN-трафика, почтового трафика, количество хостов с Kaspersky Endpoint Agent, а также размер Хранилища и базы событий. Kaspersky Anti Targeted Attack Platform определит оптимальную конфигурацию сервера Central Node с учетом указанных параметров.

Если компонент Central Node развернут в виде кластера, программа определяет оптимальную конфигурацию всех серверов кластера.

Чтобы настроить конфигурацию серверов Central Node:

1. Выполните вход в веб-интерфейс для управления масштабированием.
2. Перейдите в раздел **Конфигурация серверов**.

   Если компонент Central Node развернут на одном сервере, отображается только этот раздел.

3. В поле **Количество Endpoint Agents** укажите количество хостов с установленной программой Kaspersky Endpoint Agent, которые вы планируете использовать.

   Подробнее о том, как рассчитать количество хостов с компонентом Endpoint Agent см. в руководстве по масштабированию

   .

   Если вы не используете лицензионный ключ KEDR, укажите 0.

4. В поле **Почтовый трафик, сообщений в секунду** укажите планируемое количество сообщений электронной почты в секунду.

   Если вы не используете лицензионный ключ KATA, укажите 0.

5. В поле **SPAN-трафик, Мбит/с** укажите планируемое количество трафика со SPAN-портов на серверах с компонентом Sensor.

   Если вы не используете лицензионный ключ KATA, укажите 0.

6. Если вы установили компонент Central Node на сервере, в разделе **Объем диска** в полях **База событий, ГБ** и **Хранилище, ГБ** оставьте значения по умолчанию.

7. Если вы установили компонент Central Node в виде кластера, в разделе **Доступный объем диска** задайте размер базы событий и Хранилища одним из следующих способов:

   - Переместите ползунок, разделяющий части **База событий** и **Хранилище**, влево или вправо.

     Вам нужно учитывать, что при уменьшении размера базы событий и Хранилища самые старые данные удаляются безвозвратно в соответствии с правилами ротации. При увеличении размера базы событий и Хранилища данные сохраняются.

   - Укажите значения в полях **База событий, ГБ** и **Хранилище, ГБ**.

     Для расчета размера базы событий используйте руководство по масштабированию.

     > Обратите внимание: если пространство на диске, выделенное под базу событий, заполнено, компонент Central Node не получает данные от компонента Endpoint Agent. При заполнении дискового пространства убедитесь, что вы указали верное значение размера базы событий. Kaspersky Anti Targeted Attack Platform не проверяет на корректность введенные данные.

   - При необходимости вы можете оставить свободное пространство на диске, переместив последний ползунок справа.

8. Нажмите на кнопку **Настроить**.

Если компонент Central Node установлен на сервере, Kaspersky Anti Targeted Attack Platform определит оптимальную конфигурацию сервера в соответствии с заданными параметрами. Если компонент Central Node установлен в виде кластера, приложение настроит серверы кластера. При успешном выполнении настройки отобразится окно входа в веб-интерфейс приложения.

Настройка интеграции Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent. Вам понадобится выполнить действия и на стороне Kaspersky Anti Targeted Attack Platform через веб-интерфейс и меню администратора программы, и на стороне Kaspersky Endpoint Agent через консоль администрирования KSC.

Настройка доверенного соединения Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent

Вам понадобится настроить доверенное соединение Kaspersky Anti Targeted Attack Platform с Kaspersky Endpoint Agent и на стороне Kaspersky Anti Targeted Attack Platform через веб-интерфейс и меню администратора программы, и на стороне Kaspersky Endpoint Agent через консоль администрирования KSC.

Вы можете использовать один из следующих вариантов доверенного соединения:

1. С использованием TLS-сертификата Kaspersky Anti Targeted Attack Platform. Без проверки TLS-сертификата Kaspersky Endpoint Agent на стороне Kaspersky Anti Targeted Attack Platform.

    a. Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

    Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

    b. Настройка соединения с сервером Sensor без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

    В Kaspersky Anti Targeted Attack Platform настроено перенаправление трафика на сервер Sensor. Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Sensor. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

2. С использованием TLS-сертификатов Kaspersky Anti Targeted Attack Platform и Kaspersky Endpoint Agent. С проверкой TLS-сертификата Kaspersky Endpoint Agent на стороне Kaspersky Anti Targeted Attack Platform.

   a. Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

      Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

   b. Настройка соединения с сервером Sensor с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

      В Kaspersky Anti Targeted Attack Platform настроено перенаправление трафика на сервер Sensor. Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Sensor. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

Настройка соединения с сервером Central Node без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

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

1. **Генерация или загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node в веб-интерфейсе Central Node (если TLS-сертификат сервера Central Node не создан ранее).**
2. **Скачивание TLS-сертификата сервера Central Node на компьютер.**
3. **Загрузка TLS-сертификата сервера Central Node в Kaspersky Endpoint Agent через консоль администрирования KSC.**

Настройка соединения с сервером Sensor без проверки TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

В Kaspersky Anti Targeted Attack Platform настроено перенаправление трафика на сервер Sensor. Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Sensor. Kaspersky Anti Targeted Attack Platform не проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

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

1. Включение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor.
2. Авторизация компонента Sensor на сервере Central Node.
3. Генерация или загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor.
4. Скачивание TLS-сертификата сервера Sensor на компьютер.
5. Загрузка TLS-сертификата сервера Sensor в Kaspersky Endpoint Agent через консоль администрирования KSC.

Настройка соединения с сервером Central Node с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Central Node. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

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

1. Генерация или загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node в веб-интерфейсе Central Node (если TLS-сертификат сервера Central Node не создан ранее).
2. Скачивание TLS-сертификата сервера Central Node на компьютер.
3. Загрузка TLS-сертификата сервера Central Node в Kaspersky Endpoint Agent через консоль администрирования KSC.
4. Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.
5. Генерация и скачивание криптоконтейнера с TLS-сертификатом Kaspersky Endpoint Agent или загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

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

6. Загрузка криптоконтейнера с сертификатом Kaspersky Endpoint Agent в Kaspersky Endpoint Agent через консоль администрирования KSC.

Настройка соединения с сервером Sensor с проверкой TLS-сертификата Kaspersky Endpoint Agent в Kaspersky Anti Targeted Attack Platform

В Kaspersky Anti Targeted Attack Platform настроено перенаправление трафика на сервер Sensor. Kaspersky Endpoint Agent устанавливает доверенное соединение с Kaspersky Anti Targeted Attack Platform с использованием TLS-сертификата сервера Sensor. В Kaspersky Endpoint Agent настроена дополнительная защита соединения и загружен TLS-сертификат Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform проверяет TLS-сертификат Kaspersky Endpoint Agent при попытке подключения Kaspersky Endpoint Agent.

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

1. **Включение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor**.
2. **Авторизация компонента Sensor на сервере Central Node**.
3. **Генерация** или **загрузка самостоятельно подготовленного TLS-сертификата сервера Sensor через меню администратора сервера Sensor**.
4. **Скачивание TLS-сертификата сервера Sensor на компьютер**.
5. **Загрузка TLS-сертификата сервера Sensor в Kaspersky Endpoint Agent через консоль администрирования KSC**.
6. **Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform**.
7. **Генерация и скачивание криптоконтейнера с TLS-сертификатом Kaspersky Endpoint Agent** или **загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform**.

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

8. **Загрузка криптоконтейнера с сертификатом Kaspersky Endpoint Agent в Kaspersky Endpoint Agent через консоль администрирования KSC**.

Скачивание TLS-сертификата сервера Central Node на компьютер

Чтобы скачать TLS-сертификат сервера на компьютер:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты**.
2. В разделе **Сертификат сервера** нажмите на кнопку **Скачать**.

Файл сертификата сервера будет сохранен в папке загрузки браузера.

Генерация TLS-сертификата сервера Central Node в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Если вы уже используете TLS-сертификат сервера Central Node и сгенерируете новый сертификат, сертификат, который используется в программе, будет удален и заменен на сгенерированный сертификат.

Вам потребуется указать данные нового сертификата везде, где использовался старый.

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

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node.
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox.
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent.
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory).

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

Чтобы сгенерировать TLS-сертификат сервера Central Node:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Сгенерировать**.

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

Kaspersky Anti Targeted Attack Platform сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Загрузка самостоятельно подготовленного TLS-сертификата сервера Central Node через веб-интерфейс Kaspersky Anti Targeted Attack Platform

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

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

- Файл должен содержать сам сертификат и закрытый ключ шифрования соединения.
- Файл должен иметь формат PEM.

  Программа не работает с сертификатами другого формата.

  Если вы подготовили сертификат в другом формате, вам нужно конвертировать его в формат PEM.
- Длина закрытого ключа должна быть 2048 бит или более.

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

Если вы уже используете TLS-сертификат сервера Central Node и загрузите новый сертификат, сертификат, который используется в программе, будет удален и заменен на загруженный сертификат.

Вам потребуется указать данные нового сертификата везде, где использовался старый.

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

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node.
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox.
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent.
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory).

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

Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Загрузить**.

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

   Окно выбора файлов закроется.

- TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent.
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory).

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

Загрузка TLS-сертификата сервера Central Node или Sensor в Kaspersky Endpoint Agent

Чтобы загрузить TLS-сертификат сервера Central Node или Sensor в Kaspersky Endpoint Agent:

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

   Откроются свойства выбранной политики.
4. В разделе **Интеграция с KATA** выберите подраздел **Параметры интеграции с KATA**.
5. Установите флажок **Включить интеграцию с KATA**.
6. В поле **Адрес** введите адрес сервера Central Node программы Kaspersky Anti Targeted Attack Platform, с которым вы хотите настроить интеграцию, и выберите порт подключения. По умолчанию используется порт 443.
7. Установите флажок **Использовать закрепленный сертификат для защиты соединения**.
8. Нажмите на кнопку **Добавить TLS-сертификат...**.

   Откроется окно **Добавление TLS-сертификата**.

9. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Anti Targeted Attack Platform и скачанного на компьютер:

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

   В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Anti Targeted Attack Platform. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

   Если вы настроили перенаправление трафика на сервер с компонентом Sensor, вам нужно загрузить TLS-сертификат сервера Sensor, предварительно скачанный на компьютер.

10. Нажмите на кнопку **Добавить**.

    Информация о добавленном TLS-сертификате отобразится в разделе интеграции с Kaspersky Anti Targeted Attack Platform.

11. Убедитесь, что переключатель в правом верхнем углу блока параметров находится в положении **Политика применяется**.

12. Нажмите на кнопку **OK**.

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

Включение проверки TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Чтобы включить использование доверенного соединения с Kaspersky Endpoint Agent:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** включите переключатель **Проверять TLS-сертификаты Endpoint Agent**.

Kaspersky Anti Targeted Attack Platform будет проверять данные TLS-сертификата при попытках подключения Kaspersky Endpoint Agent к Kaspersky Anti Targeted Attack Platform.

Генерация TLS-сертификата Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform и скачивание криптоконтейнера

Чтобы сгенерировать TLS-сертификат соединения Kaspersky Anti Targeted Attack Platform с Kaspersky Endpoint Agent:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** нажмите на кнопку **Сгенерировать**.

   Kaspersky Anti Targeted Attack Platform сгенерирует новый TLS-сертификат. Страница автоматически обновится.

На ваш локальный компьютер в папку загрузки браузера будет загружен файл криптоконтейнера с сертификатом Kaspersky Endpoint Agent в формате PFX.

Вы можете использовать криптоконтейнер для настройки проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node при попытке подключения к Kaspersky Anti Targeted Attack Platform.

По умолчанию криптоконтейнер не защищен паролем. Вы можете установить пароль криптоконтейнера. Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

В криптоконтейнере содержится только файл сертификата и не содержится файл закрытого ключа. Kaspersky Anti Targeted Attack Platform не хранит закрытые ключи TLS-шифрования соединения.

Загрузка самостоятельно подготовленного TLS-сертификата Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

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

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

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

Если вы подготавливаете TLS-сертификат Kaspersky Endpoint Agent самостоятельно, вам нужно создать криптоконтейнер формата PFX с этим сертификатом и загрузить криптоконтейнер в Kaspersky Endpoint Agent.

Вы можете использовать криптоконтейнер для настройки проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node при попытке подключения к Kaspersky Anti Targeted Attack Platform.

Подробнее о работе с TLS-сертификатами см. в документации OpenSSL.

В криптоконтейнере должен содержится только файл сертификата и не должен содержится файл закрытого ключа. Kaspersky Anti Targeted Attack Platform не хранит закрытые ключи TLS-шифрования соединения.

Чтобы загрузить самостоятельно подготовленный TLS-сертификат Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** нажмите на кнопку **Загрузить**.

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

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.

Просмотр таблицы TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Чтобы просмотреть список TLS-сертификатов соединения с Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.

3. В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов со следующими данными по каждому сертификату:

   - **TLS-сертификат** - отпечаток сертификата.
   - **Серийный номер** - серийный номер сертификата.
   - **Истекает** - дата истечения срока действия сертификата.

Фильтрация и поиск TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Вы можете отфильтровать TLS-сертификаты для отображения в таблице по одной или обеим столбцам **TLS-сертификат** и **Серийный номер** или выполнить поиск TLS-сертификатов по этим столбцам таблицы по указанным вами показателям.

Чтобы выполнить фильтрацию и поиск TLS-сертификатов в таблице:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов со следующими данными по каждому сертификату:

   - **TLS-сертификат** - отпечаток сертификата.
   - **Серийный номер** - серийный номер сертификата.
   - **Истекает** - дата истечения срока действия сертификата.

4. Если вы хотите отфильтровать или найти TLS-сертификаты по отпечатку сертификата:

   a. По ссылке **TLS-сертификат** откройте окно настройки фильтрации.

   b. В поле **TLS-сертификат** введите несколько символов отпечатка сертификата.

   c. Нажмите на кнопку **Применить**.

5. Если вы хотите отфильтровать или найти TLS-сертификаты по серийному номеру:

   a. По ссылке **Серийный номер** откройте окно настройки фильтрации.

   b. В поле **Серийный номер** введите несколько символов серийного номера.

   c. Нажмите на кнопку **Применить**.

В таблице отобразятся только TLS-сертификаты, соответствующие заданным вами условиям.

Чтобы сбросить фильтр по одному или нескольким условиям фильтрации,

нажмите на кнопку справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

Удаление TLS-сертификатов Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform

Чтобы удалить один или несколько TLS-сертификатов соединения с Kaspersky Endpoint Agent через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса Kaspersky Anti Targeted Attack Platform выберите раздел **Параметры**, подраздел **Сертификаты Endpoint Agent**.

   В разделе **Сертификаты Endpoint Agent** отобразится список TLS-сертификатов.
3. Установите флажки рядом с одним или несколькими TLS-сертификатами, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

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

Выбранные TLS-сертификаты будут удалены.

Настройка проверки TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузка криптоконтейнера в Kaspersky Endpoint Agent

Чтобы настроить проверку TLS-сертификата Kaspersky Endpoint Agent сервером Central Node и загрузить криптоконтейнер с сертификатом Kaspersky Endpoint Agent в Kaspersky Endpoint Agent:

1. Откройте консоль KSC.
2. В дереве консоли откройте папку **Политики**.

3. В блоке политик Kaspersky Endpoint Agent выберите нужную политику и откройте ее свойства двойным щелчком мыши.

   Откроются свойства выбранной политики.

4. В разделе **Интеграция с KATA** выберите подраздел **KATA Central Node**.

5. Нажмите на кнопку **Настроить дополнительную защиту**.

6. В открывшемся окне установите флажок **Защита подключения с помощью клиентского сертификата**.

7. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла на вашем локальном компьютере.

8. Выберите файл криптоконтейнера сертификата Kaspersky Endpoint Agent, сгенерированного на сервере Kaspersky Anti Targeted Attack Platform и скачанного на жесткий диск вашего компьютера.

9. Нажмите на кнопку **OK**.

   Окно закроется.

10. Убедитесь, что переключатель в правом верхнем углу блока параметров находится в положении **Политика применяется**.

11. Нажмите на кнопку **OK**.

    Крипто-контейнер с сертификатом Kaspersky Endpoint Agent будет загружен в Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform будет проверять TLS-сертификат Kaspersky Endpoint Agent при попытке подключения.

Настройка перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor

Вы можете использовать сервер с компонентом Sensor в качестве прокси-сервера при обмене данными между программой Kaspersky Endpoint Agent и компонентом Central Node, чтобы снизить нагрузку на компонент Central Node.

При настройке перенаправления трафика учитывайте следующие ограничения:

- Максимальный объем входящего трафика для компонента Sensor не должен превышать 1 Гбит/с.
- Рекомендуемая ширина канала между серверами с компонентами Central Node и Sensor составляет 15% от трафика на SPAN-порте.
- Максимально допустимые потери пакетов, пересылаемых между серверами с компонентами Sensor и Central Node, составляют 10% при задержке отправки пакетов до 100 мс.

Вы можете использовать компонент Sensor в качестве прокси-сервера, только если компоненты Sensor и Central Node расположены на разных серверах.

Если вы используете компонент Sensor в качестве прокси-сервера, убедитесь, что при интеграции Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent на стороне Kaspersky Endpoint Agent вместо IP-адреса Central Node вы указали IP-адрес компонента Sensor.

Включение перенаправления трафика от Kaspersky Endpoint Agent на сервер Sensor

Чтобы включить использование компонента Sensor в качестве прокси-сервера при обмене данными между программой Kaspersky Endpoint Agent и компонентом Central Node, выполните следующие действия в меню администратора сервера с компонентом Sensor:

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

   Откроется следующее окно меню администратора.
3. Выберите пункт **Configure Central Node**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно с информацией о текущем состоянии подключения компонента Sensor к компоненту Central Node.
5. Нажмите на кнопку **Change**.
6. В окне **Input Central Node IP address** укажите IP-адрес сервера с компонентом Central Node.
7. Нажмите на кнопку **Ok**.

   Откроется окно с информацией о сертификате компонента Central Node.
8. Убедитесь, что отображаемый сертификат совпадает с сертификатом компонента Central Node.

9. Нажмите на кнопку **Ok**.

   Откроется окно с информацией о текущем состоянии подключения компонента Sensor к компоненту Central Node.

10. Нажмите на кнопку **Cancel**.

Использование компонента Sensor в качестве прокси-сервера будет включено после подтверждения авторизации на сервере с компонентом Central Node.

Авторизация компонента Sensor на сервере Central Node

Чтобы авторизовать компонент Sensor на сервере с компонентом Central Node, выполните следующие действия в веб-интерфейсе программы под учетной записью локального администратора:

1. В окне веб-интерфейса приложения выберите раздел **Серверы Sensor**.

   В таблице **Список серверов** отобразятся уже подключенные компоненты Sensor, а также запросы на подключение.

2. Выберите IP-адрес сервера с компонентом Sensor, запрос на авторизацию от которого вы хотите подтвердить или отклонить.

3. Выполните одно из следующих действий:

   - Если вы хотите авторизовать выбранный сервер с компонентом Sensor, нажмите кнопку **Принять**.
   - Если вы хотите отклонить авторизацию выбранного сервера с компонентом Sensor, нажмите кнопку **Отклонить**.

Запрос на авторизацию будет принят или отклонен.

Генерация TLS-сертификата сервера Sensor в меню администратора сервера Sensor

Чтобы сгенерировать TLS-сертификат сервера с компонентом Sensor, выполните следующие действия в меню администратора сервера с компонентом Sensor:

1. В главном окне меню администратора выберите пункт **Program settings**.

2. Нажмите на клавишу **ENTER**.

   Откроется следующее окно меню администратора.

3. Выберите пункт **Manage server certificate**.

4. Нажмите на клавишу **ENTER**.

   Откроется окно **Certificate management**.

5. В нижней части окна выберите пункт **New**.

6. Нажмите на клавишу **ENTER**.

   Откроется окно с информацией о новом сертификате.

7. Нажмите на кнопку **Continue**.

   Откроется окно подтверждения действия.

8. Нажмите на кнопку **Generate**.

   Начнется создание сертификата.

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

   Откроется окно с информацией об установленном сертификате.

10. Нажмите на кнопку **Continue**.

    Откроется окно подтверждения действия.

11. Нажмите на кнопку **Ok**.

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

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

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его на сервер с компонентом Sensor по протоколу SCP. Подробнее о способах загрузки файлов по протоколу SCP см. в документации к операционной системе, установленной на том компьютере, с которого вы хотите загрузить TLS-сертификат.

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

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

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

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

1. Выполните команду `scp kata.pem admin@<IP-адрес сервера с компонентом Sensor>:`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Sensor, заданный при установке.

TLS-сертификат будет загружен на сервер с компонентом Sensor.

Чтобы применить загруженный TLS-сертификат на сервере с компонентом Sensor, выполните следующие действия в меню администратора сервера с компонентом Sensor:

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

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

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

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

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

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

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

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

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

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

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

Скачивание TLS-сертификата сервера Sensor на компьютер

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

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

1. Выполните команду `scp admin@<IP-адрес сервера с компонентом Sensor>:ssl/kata.crt .`
2. На приглашение ввести пароль введите пароль администратора для работы в меню администратора сервера с компонентом Sensor, заданный при установке.

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

Настройка интеграции и доверенного соединения с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent

Чтобы настроить интеграцию с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent:

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

   Откроются свойства выбранной политики.
4. В разделе **Интеграция с KATA** выберите подраздел **Параметры интеграции с KATA**.
5. Установите флажок **Включить интеграцию с KATA**.
6. В поле **Адрес** введите адрес сервера Central Node программы Kaspersky Anti Targeted Attack Platform, с которым вы хотите настроить интеграцию, и выберите порт подключения. По умолчанию используется порт 443.
7. Установите флажок **Использовать закрепленный сертификат для защиты соединения**.
8. Нажмите на кнопку **Добавить TLS-сертификат...**.

   Откроется окно **Добавление TLS-сертификата**.
9. Выполните одно из следующих действий по добавлению TLS-сертификата, созданного на стороне Kaspersky Anti Targeted Attack Platform и скачанного на компьютер:

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

В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера Kaspersky Anti Targeted Attack Platform. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

Если вы настроили перенаправление трафика на сервер с компонентом Sensor, вам нужно загрузить TLS-сертификат сервера Sensor, предварительно скачанный на компьютер.

10. Нажмите на кнопку **Добавить**.

    Информация о добавленном TLS-сертификате отобразится в разделе интеграции с Kaspersky Anti Targeted Attack Platform.

11. Нажмите на кнопку **Добавить сертификат клиента...**.

12. В открывшемся окне установите флажок **Защита подключения с помощью сертификата клиента**.

13. Нажмите на кнопку **Загрузить**.

    Откроется окно выбора файла на вашем локальном компьютере.

14. Выберите файл криптоконтейнера сертификата Kaspersky Endpoint Agent, сгенерированного на сервере Kaspersky Anti Targeted Attack Platform и скачанного на жесткий диск вашего компьютера.

15. Нажмите на кнопку **OK**.

    Окно закроется.

16. В поле **Время ожидания (сек.):** укажите максимальное время ожидания ответа сервера Central Node программы Kaspersky Anti Targeted Attack Platform в секундах.

17. В поле **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)** укажите интервал в минутах.

18. Если вы хотите, чтобы Kaspersky Endpoint Agent не отправлял на сервер Kaspersky Anti Targeted Attack Platform информацию о процессах, которые запускаются повторно, установите флажок **Использовать период TTL при отправке событий**. Kaspersky Endpoint Agent не считает запуск процесса повторным, если запуск происходит после окончания очередного периода TTL.

19. Если вы установили флажок Использовать период TTL при отправке событий, укажите время в поле **Период TTL (мин.)**.

20. Убедитесь, что переключатель в правом верхнем углу блока параметров находится в положении **Политика применяется**.

21. Нажмите на кнопку **OK**.

Интеграция с Kaspersky Anti Targeted Attack Platform на стороне Kaspersky Endpoint Agent будет настроена.

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 для управления масштабированием

Веб-интерфейс Kaspersky Anti Targeted Attack Platform для управления масштабированием 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.

В веб-интерфейсе для управления масштабированием вы можете выполнять следующие действия:

- Управлять серверами кластера Central Node.
- Настраивать конфигурацию серверов с компонентом Central Node.

Чтобы начать работу в веб-интерфейсе для управления масштабированием:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, в адресной строке браузера введите IP-адрес сервера с компонентом Central Node.

   Если вы используете отказоустойчивую версию программы, вы можете ввести IP-адрес любого сервера кластера Central Node или **полное доменное имя (FQDN) кластера**.

   Для обеспечения бесперебойного доступа к веб-интерфейсу программы вы можете настроить на сервере DNS функцию Round Robin. В этом случае осуществляется вход в веб-интерфейс первого работоспособного сервера кластера Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. Введите имя учетной записи администратора admin и пароль, заданный при установке программы.
3. Установите флажок **Локальный администратор**.
4. Нажмите на кнопку **Войти**.

Вы можете начать работу в веб-интерфейсе для управления масштабированием.

Для отказоустойчивой версии программы в веб-интерфейсе отображаются разделы **Кластер** и **Конфигурация серверов**.

Если вы используете неотказоустойчивую версию программы, в веб-интерфейсе отображается только раздел **Конфигурация серверов**.

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

Начало работы в веб-интерфейсе программы под учетной записью локального администратора

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.

После установки Kaspersky Anti Targeted Attack Platform вам требуется настроить параметры масштабирования программы в веб-интерфейсе для управления масштабированием.

Если параметры масштабирования Kaspersky Anti Targeted Attack Platform не настроены, вход в веб-интерфейс под учетной записью локального администратора недоступен.

Чтобы начать работу в веб-интерфейсе программы под учетной записью локального администратора:

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, в адресной строке браузера введите IP-адрес сервера с компонентом Central Node.

   Если вы используете отказоустойчивую версию программы, вы можете ввести IP-адрес любого сервера кластера Central Node или **полное доменное имя (FQDN) кластера**.

   Для обеспечения бесперебойного доступа к веб-интерфейсу программы вы можете настроить на сервере DNS функцию Round Robin. В этом случае осуществляется вход в веб-интерфейс первого работоспособного сервера кластера Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. Введите имя учетной записи Administrator и пароль Administrator.

   Пароль Administrator используется по умолчанию. Настоятельно рекомендуется изменить пароль для этой учетной записи после входа в веб-интерфейс программы.

3. Установите флажок **Локальный администратор**.

4. Нажмите на кнопку **Войти**.

   Откроется страница **Мониторинг** веб-интерфейса программы.

Вы можете начать работу с программой под учетной записью локального администратора.

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

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.

Убедитесь что доступ к меню администратора и консоли управления серверами Kaspersky Anti Targeted Attack Platform есть только с тех компьютеров, которым вы разрешили этот доступ.

Убедитесь, что компьютеры, которым вы разрешаете доступ, находятся в защищенном периметре вашей сети.

Вы можете настроить доступ к меню администратора и консоли управления серверами Kaspersky Anti Targeted Attack Platform с определенных компьютеров, с помощью утилиты командной строки iptables. Подробнее о работе с iptables см. документацию к iptables.

Чтобы начать работу в меню администратора компонента Sandbox, Sensor или Central Node в консоли управления сервером с нужным компонентом:

1. Войдите в консоль управления того сервера, параметры которого вы хотите изменить, по протоколу SSH или через терминал.

   Отобразится меню администратора компонента программы.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке программы.

   Отобразится меню администратора компонента программы.

Вы можете начать работу в меню администратора программы.

Начало работы с программой в режиме Technical Support Mode

Любые действия в режиме технической поддержки, не согласованные и / или не рекомендованные специалистами технической поддержки, запрещены и являются основанием для отказа в технической поддержке.

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 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. Такие файлы хранятся бессрочно и могут быть удалены администратором Kaspersky Anti Targeted Attack Platform вручную. Путь к папке для записи файлов трассировки указывает администратор Kaspersky Anti Targeted Attack Platform.

Чтобы начать работу с компонентами Central Node, Sensor или Sandbox в режиме Technical Support Mode:

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 компонента.

   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. Подтвердите, что хотите выполнять действия с программой в режиме Technical Support Mode. Для этого выберите **Yes** и нажмите на клавишу **ENTER**.

Вы можете начать работу с компонентами Sensor или Sandox в режиме Technical Support Mode.

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 после установки.

  - Учетная запись администратора веб-интерфейса программы.

  - Учетные записи пользователей веб-интерфейса программы с ролями **Аудитор**, **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 и мультитенантности 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 требуется 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 режиме распределенного решения и мультитенантности 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**.

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 тенантами в разделе **Режим работы**.

Под учетной записью с ролью **Аудитор** вы можете просматривать все разделы веб-интерфейса, доступные локальному администратору и сотрудникам службы безопасности. Пользователь с ролью **Аудитор** может просматривать данные без возможности редактирования.

Роли **Старший сотрудник службы безопасности** и **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. Пользователи с ролью **Старший сотрудник службы безопасности** доступны все операции. Ограничения доступа для пользователей с ролями **Сотрудник службы безопасности** представлены в таблице ниже.

Ограничения доступа для пользователей программы с ролью **Сотрудник службы безопасности**

Функциональная область / Раздел веб-интерфейса	Ограничения
Мониторинг	Недоступны виджеты событий группы VIP. Нет возможности перейти по ссылке на виджет 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.
Пользовательские правила	Доступ на чтение.
Хранилище	Нет доступа к объектам, помещенным в Хранилище в результате выполнения задач. Полный доступ к объектам, загруженным пользователем вручную.
Endpoint Agents	Доступ к просмотру таблиц компьютеров с Kaspersky Endpoint Agent, ограничения по просмотру данных о задачах, политиках и сетевой изоляции.
Сетевая изоляция хостов	Нет доступа.
Отчеты	Нет доступа.
Параметры: Расписание IOC-проверки	Доступ на чтение.
Параметры: Endpoint Agents	Доступ на чтение.
Параметры: Репутационная база KPSN	Нет доступа.
Параметры: Правила уведомлений	Нет доступа к правилам для отправки уведомлений об обнаружениях. Полный доступ к правилам для отправки уведомлений о проблемах в работе программы.
Параметры: Статус VIP	Доступ на чтение.
Пользовательские правила: YARA	Доступ только на экспорт правил.

Функциональная область / Раздел веб-интерфейса	Ограничения
Параметры: Исключения ТАА	Доступ на чтение и экспорт.
Параметры: Пароли к архивам	Нет доступа.
Параметры: Лицензия	Доступ на чтение.

Если вы используете режим распределенного решения и мультитенантности, то для каждой учетной записи вы можете разрешить или запретить доступ к тенантам 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 тенантами в разделе **Режим работы**.

Чтобы создать учетную запись администратора веб-интерфейса программы:

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 блоке параметров **Тип аутентификации** выберите один из вариантов:

   - **Учетная запись KATA**.

     В этом случае для подключения к веб-интерфейсу программы пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.
   - **Доменная учетная запись**.

     В этом случае для подключения к веб-интерфейсу программы пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.

   > Поля **Учетная запись KATA** и **Доменная учетная запись** доступны, если настроена интеграция с Active Directory.

7. Если вы выбрали **Учетная запись KATA**, выполните следующие действия:

   a. 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).

   b. 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.

   c. В поле **Подтвердите пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.

8. Если вы выбрали **Доменная учетная запись**, в поле **Имя пользователя** укажите доменное имя пользователя.

9. Нажмите на кнопку **Добавить**.

Учетная запись администратора веб-интерфейса программы будет создана.

Если вы используете режим распределенного решения и мультитенантности, учетная запись администратора веб-интерфейса сервера PCN имеет доступ к данным всех тенантов, связанных с этим сервером.

Создание учетной записи пользователя веб-интерфейса программы

Вы можете создавать учетные записи пользователей с ролями **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** и **Аудитор**.

Чтобы создать учетную запись пользователя веб-интерфейса программы:

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. При необходимости с помощью переключателя **Состояние** отключите учетную запись пользователя.

   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 блоке параметров **Тип аутентификации** выберите один из вариантов:

   - **Учетная запись KATA**.

     В этом случае для подключения к веб-интерфейсу программы пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.
   - **Доменная учетная запись**.

     В этом случае для подключения к веб-интерфейсу программы пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.

     Если вы выбрали тип аутентификации **Доменная учетная запись**, требуется учитывать, что пользователь не сможет войти в веб-интерфейс программы под другой учетной записью.

   Поля **Учетная запись KATA** и **Доменная учетная запись** доступны, если настроена интеграция с Active Directory.
6. В раскрывающемся списке **Роль** выберите одну из следующих ролей:

   - **Старший сотрудник службы безопасности**.
   - **Сотрудник службы безопасности**.
   - **Аудитор**.
7. Если вы выбрали **Учетная запись KATA**, выполните следующие действия:

   a. 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).

b. 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.

c. В поле **Подтвердите пароль** повторно введите пароль доступа пользователя к веб-интерфейсу.

8. Если вы выбрали **Доменная учетная запись**, в поле **Имя пользователя** укажите доменное имя пользователя.
9. В разделе **Доступ** настройте права доступа:

a. С помощью переключателя включите параметр **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 **Тенанты** установите флажки рядом с названиями одного или нескольких тенантов, к веб-интерфейсам серверов которых вы хотите предоставить доступ.

Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех тенантов.

10. Нажмите на кнопку **Добавить**.

Настройка отображения таблицы учетных записей пользователей

Вы можете настроить отображение столбцов, а также порядок их следования в таблице учетных записей пользователей.

Чтобы настроить отображение таблицы учетных записей пользователей:

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.
4. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.
5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.
6. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
7. Нажмите на кнопку **Применить**.

Отображение таблицы учетных записей пользователей будет настроено.

Просмотр таблицы учетных записей пользователей

Таблица событий отображается в разделе **Параметры**, подразделе **Пользователи** окна веб-интерфейса программы. Вы можете сортировать события в таблице по столбцам **Имя пользователя**, **Роль**, **Тенанты** и **Состояние**.

В таблице содержится следующая информация:

1. **Имя пользователя** – имя пользователя, заданное при создании учетной записи.
2. **Тип аутентификации** – тип аутентификации пользователя. Может иметь следующие значения:

   - **Учетная запись KATA**.

     Если выбран этот тип аутентификации, для подключения к веб-интерфейсу программы пользователю потребуется ввести имя пользователя и пароль, которые были указаны при создании учетной записи.

   - **Доменная учетная запись**.

     Если выбран этот тип аутентификации, для подключения к веб-интерфейсу программы пользователю не требуется вводить имя пользователя и пароль: аутентификация осуществляется с помощью доменной учетной записи пользователя.
3. **Роль** – роль, назначенная пользователю.
4. **Тенанты** – тенанты, к которым пользователь имеет доступ.

   Столбец отображается только в режиме распределенного решения и мультитенантности.

5. **Состояние** – статус учетной записи. может иметь следующие значения:

   - **Включено**.

     Если учетная запись включена, доступ к веб-интерфейсу программы разрешен.

   - **Отключено**.

     Если учетная запись отключена, доступ к веб-интерфейсу программы запрещен.

Фильтрация учетных записей

Чтобы отфильтровать или найти учетные записи пользователей по требуемым критериям, 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. Выполните следующие действия в зависимости от критерия фильтрации:

   - **По имени пользователя**

     a. По ссылке **Имя пользователя** откройте меню фильтрации.

     b. В раскрывающемся списке выберите один из следующих операторов фильтрации:

        - **Содержит**.
        - **Не содержит**.

     c. В поле ввода введите имя пользователя или несколько символов из имени пользователя.

     d. Нажмите на кнопку **Применить**.

   - **По типу аутентификации**

     a. По ссылке **Тип аутентификации** откройте меню фильтрации.

     b. Установите флажок напротив типа учетной записи, которую вы хотите включить в критерии фильтрации:

        - **Учетная запись KATA**.
        - **Доменная учетная запись**.

     c. Нажмите на кнопку **Применить**.

- **По роли**

  a. По ссылке **Роль** откройте меню фильтрации.

  b. Установите флажки напротив тех ролей, которые вы хотите включить в критерии фильтрации:

  - **Администратор**.
  - **Старший сотрудник службы безопасности**.
  - **Сотрудник службы безопасности**.
  - **Аудитор**.

  Вы можете установить несколько флажков.

  c. Нажмите на кнопку **Применить**.

- **По названию тенантов, к которым у пользователя есть доступ**

  a. По ссылке **Тенанты** откройте меню фильтрации.

  b. Установите флажки напротив тенантов, которые вы хотите включить в критерии фильтрации.
  Вы можете установить несколько флажков.

  c. Нажмите на кнопку **Применить**.

- **По состоянию**

  a. По ссылке **Состояние** раскройте список настройки фильтрации.

  b. Выберите один из следующих вариантов:

  - **Все**.
  - **Включено**.
  - **Отключено**.

В таблице отобразятся учетные записи, соответствующие заданным критериям фильтрации.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра учетных записей

Чтобы сбросить фильтр учетных записей по одному или нескольким условиям фильтрации:

1. Войдите в веб-интерфейс под учетной записью администратора приложения.
2. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Пользователи**.

3. Нажмите на кнопку справа от того заголовка столбца таблицы учетных записей, 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 учетные записи, соответствующие заданным условиям.

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 тенантов, 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**.Выберите учетную запись, права доступа которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
3. Если вы хотите включить или отключить учетную запись, измените положение переключателя **Состояние**.
4. 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.
5. Справа от названия параметра **Тенанты** установите или снимите флажки рядом с названиями тенантов, к веб-интерфейсам серверов которых вы хотите изменить доступ.

   Вы можете использовать ссылки **Выбрать все** и **Отменить выбор** для выбора или отмены выбора всех тенантов.
6. 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**.В списке учетных записей выберите учетную запись пользователя, которую вы хотите включить или отключить.
3. Выполните одно из следующих действий в столбце **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.
4. Нажмите на кнопку **Да**.

Состояние учетной записи будет изменено.

Изменение пароля учетной записи администратора или пользователя программы

Изменение пароля учетной записи доступно только для пользователей с типом аутентификации **Учетная запись KATA**.

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**.В списке учетных записей выберите учетную запись, пароль которой вы хотите изменить.

   Откроется окно **Изменить учетную запись**.
3. 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.

4. В поле **Подтвердите пароль** повторно введите новый пароль.
5. Нажмите на кнопку **Сохранить**.

Пароль учетной записи администратора или пользователя программы будет изменен.

Изменение пароля своей учетной записи

Изменение пароля учетной записи доступно только для пользователей с типом аутентификации **Учетная запись KATA**.

Чтобы изменить пароль своей учетной записи:

1. Войдите в веб-интерфейс под своей учетной записью.
2. В нижней части окна веб-интерфейса программы по ссылке с именем вашей учетной записи раскройте список действий.
3. Выберите действие **Изменить пароль**.

   Откроется окно **Изменить пароль**.
4. В поле **Старый пароль** введите текущий пароль доступа к веб-интерфейсу программы.
5. В поле **Новый пароль** введите новый пароль доступа к веб-интерфейсу программы.

   Пароль должен удовлетворять следующим требованиям:

   - не должен совпадать с именем пользователя;
   - не должен содержать словарные слова, распространенные сочетания букв или примеры раскладки клавиатуры (например, Qwerty или passw0rd);
   - должен содержать минимум 8 символов;

- должен содержать символы минимум трех типов:
  - символ верхнего регистра (A–Z);
  - символ нижнего регистра (a–z);
  - цифру;
  - специальный символ.

6. В поле **Подтвердите пароль** повторно введите новый пароль.

7. Нажмите на кнопку **Изменить пароль**.

Пароль доступа к веб-интерфейсу программы вашей учетной записи будет изменен.

Аутентификация с помощью доменных учетных записей

Если аутентификация с помощью доменных учетных записей настроена, пользователям не требуется вводить данные учетной записи Kaspersky Anti Targeted Attack Platform для подключения к веб-интерфейсу программы.

Для включения аутентификации с помощью доменных учетных записей вам требуется:

1. Настроить интеграцию с Active Directory.

   Для настройки интеграции с Active Directory требуется создать keytab-файл, содержащий имя субъекта-службы (далее также "SPN") для сервера Central Node, на котором выполняется настройка интеграции.

2. Выбрать для пользователя тип аутентификации **Доменная учетная запись** при создании учетной записи.

Создание keytab-файла

Вы можете использовать одну учетную запись для аутентификации на нескольких серверах Central Node. Для этого требуется создать keytab-файл, содержащий *имена субъекта-службы (далее также "SPN")* для каждого из этих серверов. При создании keytab-файла потребуется использовать атрибут для генерации *соли* (salt, модификатор входа хеш-функции).

Сгенерированную соль необходимо сохранить любым удобным способом для дальнейшего добавления новых SPN в keytab-файл.

Вы также можете создать отдельную учетную запись Active Directory для каждого сервера Central Node, для которого вы хотите настроить Kerberos-аутентификацию.

Чтобы создать keytab-файл, используя одну учетную запись:

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте учетную запись пользователя (например, с именем `control-user`).

2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:

   a. Откройте свойства созданной учетной записи.

   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.

3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь к файлу>\<имя файла>.keytab
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлено SPN выбранного сервера. На экране отобразится сгенерированная соль: `Hashing password with salt "<хеш-значение>".`

4. Добавьте в keytab-файл запись SPN для каждого следующего сервера Central Node. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab -setupn -setpass -rawsalt "<хеш-значение соли, полученное при создании keytab-файла на шаге 3>"
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN выбранных серверов.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 серверов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN сервера, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

Допустим, вы получили соль `"TEST.LOCALHTTPcontrol-01.test.local"`.

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

Чтобы создать keytab-файл, используя отдельную учетную запись для каждого сервера Central Node:

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя для каждого сервера (например, учетные записи с именами `control-user`, `secondary1-user`, `secondary2-user` и т.д.).

2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:

   a. Откройте свойства созданной учетной записи.

   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.

3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out <путь к файлу>\<имя файла>.keytab
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

   В созданный keytab-файл будет добавлено SPN выбранного сервера.

4. Добавьте в keytab-файл запись SPN для каждого следующего сервера Central Node. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) сервера Central Node>@<realm имя домена Active Directory в верхнем регистре> -mapuser secondary1-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab
   ```

   Утилита запросит пароль пользователя `secondary1-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN выбранных серверов.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 серверов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN сервера, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

Настройка интеграции с Active Directory

Чтобы настроить интеграцию с Active Directory:

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. Перейдите на закладку **Интеграция с Active Directory**.
4. Установите флажок **Интеграция**, если вы хотите включить интеграцию с Active Directory.
5. Нажмите на кнопку **Обзор**, чтобы загрузить keytab-файл.
6. Выберите keytab-файл и нажмите на кнопку **Открыть**.

После загрузки файла отобразятся следующие поля:

- **Статус keytab-файла**. Может принимать следующие значения:
  - **Файл содержит SPN-идентификатор для этого сервера** – в загруженном keytab-файле есть SPN для этого сервера Kaspersky Anti Targeted Attack Platform.
  - **Отсутствует SPN-идентификатор для этого сервера** – в загруженном keytab-файле отсутствует SPN для этого сервера Kaspersky Anti Targeted Attack Platform.
- **Файл содержит** – список SPN, которые содержит файл.

7. Нажмите на кнопку **Применить**.

Интеграция с Active Directory будет настроена.

В режиме распределенного решения и мультитенантности настройки интеграции с Active Directory, заданные на сервере PCN, **не** распространяются на подключенные к нему серверы SCN. Если вы хотите настроить интеграцию с Active Directory на серверах SCN, вам требуется выполнить описанные выше шаги на каждом выбранном сервере SCN.

Отключение интеграции с Active Directory

При отключении интеграции с Active Directory аутентификация пользователей с помощью доменных учетных данных будет недоступна.

Чтобы отключить интеграцию с Active Directory:

1. Войдите в веб-интерфейс под учетной записью администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Пользователи**.
3. Перейдите на закладку **Интеграция с Active Directory**.
4. Снимите флажок **Интеграция**.
5. Нажмите на кнопку **Применить**.

Интеграция с Active Directory будет отключена. Загруженный keytab-файл будет удален без возможности восстановления.

В режиме распределенного решения и мультитенантности настройки интеграции с Active Directory, заданные на сервере PCN, **не** распространяются на подключенные к нему серверы SCN. Если вы хотите отключить интеграцию с Active Directory на отдельных серверах SCN, вам требуется выполнить описанные выше шаги на каждом выбранном сервере SCN.

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.

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

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.

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 со своих компьютеров в Kaspersky Security Network.

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 мультитенантности, 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:

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
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:

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
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 мультитенантности, 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:

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 MD5- и SHA256-хеши объектов, обнаруженных компонентом Sandbox, в локальную репутационную базу KPSN. В этом случае объектам присваивается статус *Недоверенный*. Данные локальных репутационных баз доступны только для компьютеров локальной сети организации.

Чтобы настроить сохранение информации об обнаружениях в локальную репутационную базу KPSN:

1. Войдите в веб-интерфейс программы под учетной записью старшего сотрудника службы безопасности.
2. Выберите раздел **Параметры**, подраздел **Репутационная база KPSN**.

3. Выполните одно из следующих действий:

   - Включите переключатель **Присваивать объектам статус "Недоверенный"**, если вы хотите, чтобы программа присваивала обнаружениям статус *Недоверенный* и сохраняла информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN.

   - Выключите переключатель **Присваивать объектам статус "Недоверенный"**, если вы не хотите сохранять информацию об обнаружениях компонента Sandbox в локальную репутационную базу KPSN.

4. Нажмите на кнопку **Сохранить**.

Настройка сохранения информации в локальную репутационную базу KPSN будет выполнена.

Отказ от участия в KSN и использования KPSN

Чтобы отказаться от участия в Kaspersky Security Network и использования KPSN:

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

2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.

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.

   Откроется окно ввода учетных данных администратора компонента Sandbox.

2. Введите имя пользователя и пароль администратора компонента Sandbox, который вы задали при установке компонента Sandbox.

Вы можете начать работу в веб-интерфейсе Sandbox.

Если вы используете несколько серверов с компонентом Sandbox, производите настройку параметров каждого компонента Sandbox из веб-интерфейса Sandbox этого сервера.

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:

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.

   В блоке параметров **Последнее обновление** отобразятся время и статус последней попытки обновления баз Sandbox.

2. Нажмите на кнопку **Запустить**.

Выбор источника обновления баз

Чтобы выбрать источник обновления баз:

1. В окне веб-интерфейса Sandbox выберите раздел **Обновление баз**.

2. В блоке параметров **Источник обновлений** выберите источник, из которого вы хотите получать пакет обновлений:

   - **Сервер обновлений "Лаборатории Касперского"**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.

   - **Сервер обновлений "Лаборатории Касперского" (безопасное подключение)**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется выполнять обновления баз по протоколу HTTPS.

   - **Другой сервер**.

     Программа будет подключаться к вашему FTP- или HTTP-серверу или к папке с базами программы на вашем компьютере и загружать актуальные базы.

3. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите полный путь к папке с пакетом обновлений баз программы.

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:

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:

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 веб-интерфейсе программы создается запрос на подключение к компоненту Sandbox.
2. В веб-интерфейсе Sandbox отображаются запросы на подключение.

   Вы можете принять или отклонить запрос.

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:

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

   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:

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.

Вы также можете настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox.

Чтобы настроить управляющий сетевой интерфейс в веб-интерфейсе Sandbox:

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:

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.

Вы также можете добавить, удалить или изменить статические сетевые маршруты в веб-интерфейсе Sandbox.

Чтобы добавить статический сетевой маршрут:

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:

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:

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:

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 ISO-образы следующих операционных систем: Windows XP SP3, 64-разрядной Windows 7, 64-разрядной Windows 10, CentOS 7.8, Astra Linux 1.7, и программ, необходимых для работы компонента Sandbox. Вам не требуется активировать эти операционные системы и программы. В поставляемых образах уже добавлен лицензионный ключ.

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**.

   При установке виртуальных машин с операционными системами Windows XP SP3, Windows 7, Windows 10 и Astra Linux 1.7 открывается окно **Лицензионное соглашение**, содержащее тексты следующих лицензионных соглашений:

   - Для операционных систем Windows XP SP3, Windows 7 и Windows 10:
     - 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.

- Для операционной системы Astra Linux 1.7:
  - ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ДЛЯ ПО ASTRA LINUX в составе Kaspersky Anti Targeted Attack Platform.

При установке виртуальной машины с операционной системой CentOS 7.8 окно **Лицензионное соглашение** не открывается, так как для использования этой операционной системы не требуется принимать условия лицензионного соглашения.

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:

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:

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 логических ядер нужно умножить на 1,5.

Чтобы установить максимальное количество одновременно запускаемых виртуальных машин:

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:

1. В окне веб-интерфейса Sandbox выберите раздел **Администрирование**.
2. В группе параметров **Журнал системы** нажмите на кнопку **Скачать**.
3. Журнал системы Sandbox загрузится на жесткий диск вашего компьютера в ту директорию, которая указана в качестве директории загрузки файлов из интернета в параметрах браузера, который вы используете для работы с программой.

Экспорт параметров Sandbox

Чтобы экспортировать параметры системы Sandbox:

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:

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:

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:

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:

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 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 тенантами в режиме распределенного решения и мультитенантности.

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/Аудитор**.

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** содержит следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.
- **Режим работы**. Содержит информацию о серверах PCN и SCN и о тенантах в режиме распределенного решения и мультитенантности.
- **Endpoint Agents**. Содержит информацию о подключенных компьютерах с программой Kaspersky Endpoint Agent и их параметрах.
- **Отчеты**: **Журнал активности**. Содержит информацию о параметрах записи информации о действиях пользователей в веб-интерфейсе программы.
- **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.

Пользователи с ролью **Аудитор** также могут просматривать эти разделы веб-интерфейса программы.

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью виджетов в разделе **Мониторинг** окна веб-интерфейса программы. Вы можете добавлять, удалять, перемещать виджеты, настраивать масштаб отображения виджетов и выбирать период отображения данных.

О виджетах и схемах расположения виджетов

С помощью виджетов вы можете осуществлять мониторинг работы программы.

Схема расположения виджетов – вид рабочей области окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать виджеты на схеме расположения виджетов.

В программе доступны следующие виджеты:

- **Обработано**. Отображение состояния обработки трафика, поступающего от компонента Sensor и программы Kaspersky Endpoint Agent на сервер с компонентом Central Node.
- **Очереди**. Отображение сведений о количестве и объеме объектов, ожидающих проверки модулями и компонентами программы.
- **Время обработки в Sandbox**. Отображение среднего времени, за которое были получены результаты проверки объектов компонентом Sandbox.

Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту и серверу.

Выбор тенанта и сервера для работы в разделе Мониторинг

Если вы используете режим распределенного решения и мультитенантности, перед началом работы в разделе **Мониторинг** вам нужно выбрать тенант и сервер, данные по которым вы хотите просмотреть.

*Чтобы выбрать тенант и сервер для отображения данных в разделе **Мониторинг**:*

1. В правой верхней части окна веб-интерфейса программы нажмите на стрелку рядом с именем сервера.
2. В раскрывшемся меню выберите тенант и нужный вам сервер из списка.

Отобразятся данные по выбранному вами серверу. Если вы хотите изменить тенант и сервер, вам нужно повторить действия по выбору тенанта и сервера.

Добавление виджета на текущую схему расположения виджетов

Чтобы добавить виджет на текущую схему расположения виджетов:

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 **Виджеты**.
5. В появившемся окне **Настроить виджеты** выполните следующие действия:
   - Если вы хотите добавить виджет **Очереди**, включите переключатель рядом с названием этого виджета.
   - Если вы хотите добавить виджет **Время обработки в Sandbox**, включите переключатель рядом с названием этого виджета.
   - Если вы хотите добавить виджет **Обработано**, нажмите на кнопку + рядом с названием этого виджета.

Выбранный виджет будет добавлен на текущую схему расположения виджетов.

Перемещение виджета на текущей схеме расположения виджетов

Чтобы переместить виджет на текущей схеме расположения виджетов:

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 виджет, который вы хотите переместить на схеме расположения виджетов.

5. Нажав и удерживая левую клавишу мыши на верхней части виджета, перетащите виджет на другое место схемы расположения виджетов.

6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения виджетов будет сохранена.

Удаление виджета с текущей схемы расположения виджетов

Чтобы удалить виджет с текущей схемы расположения виджетов:

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 виджета, который вы хотите удалить со схемы расположения виджетов.

   Виджет будет удален из рабочей области окна веб-интерфейса программы.

5. Нажмите на кнопку **Сохранить**.

Виджет будет удален с текущей схемы расположения виджетов.

Сохранение схемы расположения виджетов в PDF

Чтобы сохранить схему расположения виджетов в PDF:

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 виджетов в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.

6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на виджетах

Вы можете настроить отображение данных на виджетах за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

Чтобы настроить отображение данных на виджетах за сутки (с 00:00 до 23:59):

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 виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Чтобы настроить отображение данных на виджетах за неделю (с понедельника по воскресенье):

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 виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Чтобы настроить отображение данных на виджетах за месяц (календарный месяц):

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 виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Мониторинг приема и обработки входящих данных

На виджете **Обработано** вы можете оценить статус обработки данных, поступающих от компонента Sensor и программного компонента Kaspersky Endpoint Agent на сервер с компонентом Central Node, и отследить ошибки обработки данных.

Вы можете выбрать компонент (Sensor или Kaspersky Endpoint Agent), поступление данных с которого вы хотите оценить, в раскрывающемся списке справа от названия виджета **Обработано**.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия компонента (Sensor или Kaspersky Endpoint Agent):

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на виджетах.

В левой части каждого виджета отображается легенда виджета по цветам, которые используются на самих виджетах.

Если выбран тип отображения данных **Текущая загрузка**, справа от легенды отображается средняя скорость обработки данных за последние 5 минут.

Пример:
На виджете **Обработано**, где выбран Sensor типа **(SPAN)** или **(ICAP)** и тип отображения данных **Текущая загрузка**, отображается скорость обработки данных SPAN- и ICAP-трафика, поступающих от компонента Sensor на сервер с компонентом Central Node в определенное время.
Отображаются следующие данные:

- **Трафик** – скорость поступления трафика на сервер с компонентом Central Node зеленым цветом (Мбит/сек.).
- **Файлы** – скорость обработки файлов серым цветом (объектов/сек.).
- **URL-адреса** – скорость обработки URL-адресов синим цветом (объектов/сек.).
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.
  На виджете **Обработано**, где выбран Sensor типа **(SMTP)** и тип отображения данных **Текущая загрузка**, отображается скорость обработки данных почтового трафика, поступающих от почтового сенсора на сервер с компонентом Central Node в определенное время.
  Отображаются следующие данные:
- **Трафик** – скорость поступления трафика на сервер с компонентом Sensor зеленым цветом (сообщений/сек.).
- **Файлы** – скорость обработки файлов серым цветом (объектов/сек.).
- **URL-адреса** – скорость обработки URL-адресов синим цветом (объектов/сек.).
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость обработки данных в определенное время.
  На виджете **Обработано**, где выбран Sensor типа **(LOAD) Endpoint Agents** и тип отображения данных **Текущая загрузка**, отображается скорость обработки событий, поступающих от компонентов Endpoint Agent на сервер с компонентом Central Node в определенное время (Событий/сек.).
  При наведении курсора мыши на виджет 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 виджете **Обработано**, где выбран Sensor типа **(SPAN)** или **(ICAP)** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается скорость поступления SPAN- и ICAP-трафика 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 (объектов/сек.).
- **Файлы** – количество извлеченных файлов серым цветом.
- **URL-адреса** – количество извлеченных URL-адресов синим цветом.
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов в определенное время.
  На виджете **Обработано**, где выбраны Sensor типа **(SMTP)** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается скорость обработки данных почтового трафика, поступающих от почтового сенсора 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 (объектов/сек.).
- **Файлы** – количество извлеченных файлов серым цветом.
- **URL-адреса** – количество извлеченных URL-адресов синим цветом.
- **Не обработано** – количество необработанных объектов вертикальными линиями красного цвета.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается скорость поступления трафика на сервер с компонентом Central Node и количество обработанных объектов в определенное время.
  На виджете **Обработано**, где выбран Sensor типа **(LOAD) Endpoint Agents** и тип отображения данных **Выбранный период** с настроенным периодом отображения данных **Месяц**, отображается количество событий, поступивших от хостов с программой Kaspersky Endpoint Agent на сервер с компонентом Central Node за выбранный месяц.
  При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается количество событий, поступивших в определенное время.

Мониторинг очередей обработки данных модулями и компонентами программы

На виджете **Очереди** вы можете оценить статус обработки данных модулями программы YARA, AM Engine, компонентом Sandbox и отследить объем необработанных данных.

Передача данных в очереди измеряется сообщениями.

Вы можете выбрать тип отображения данных в раскрывающемся списке справа от названия виджета **Очереди**:

- **Текущая загрузка** – 5 минут до текущего момента.
- **Выбранный период**. В этом случае вы также можете настроить период отображения данных на виджетах.

В левой части виджета отображается легенда виджета по цветам, которые используются на виджете.

На виджете **Очереди** отображаются следующие данные:

- **Количество сообщений** и **Объем данных**, обработанных модулями и компонентами программы:
  - **YARA** – синим цветом.
  - **Sandbox** – фиолетовым цветом.
  - **AM Engine** – зеленым цветом.
- **Не обработано** – объем необработанных данных вертикальными линиями красного цвета.

При наведении курсора мыши на виджет появляется всплывающее окно, в котором отображается статус обработки данных модулями программы **YARA**, **AM Engine** и компонентом **Sandbox**, а также объем необработанных данных в определенное время.

Мониторинг обработки данных компонентом Sandbox

На виджете **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 виджетах **Месяц**, на виджете **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 и распределив по этим серверам данные, предназначенные для обработки.

Просмотр состояния работоспособности модулей и компонентов программы

Если в работе модулей и компонентов программы возникли проблемы, на которые администратору рекомендуется обратить внимание, в верхней части окна раздела **Мониторинг** веб-интерфейса программы отображается рамка желтого цвета с предупреждениями.

Пользователю с ролью **Локальный администратор**, **Администратор** или **Аудитор** доступна информация о работоспособности того сервера Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** или **Аудитор** доступна следующая информация о работоспособности:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о работоспособности того сервера Central Node, на котором он сейчас работает.
- Если вы используете режим режим распределенного решения и мультитенантности и пользователь работает на сервере SCN, пользователю доступна информация о работоспособности этого сервера SCN в рамках тех тенантов, к данным которых у него есть доступ.
- Если вы используете режим режим распределенного решения и мультитенантности и пользователь работает на сервере PCN, пользователю доступна информация о работоспособности этого сервера PCN и всех серверов SCN, подключенных к этому серверу, в рамках тех тенантов, к данным которых у него есть доступ.

Чтобы получить более подробную информацию о работоспособности модулей и компонентов программы,

по ссылке **Просмотреть сведения** откройте окно **Работоспособность системы**.

В окне **Работоспособность системы** в зависимости от работоспособности модулей и компонентов программы отображается один из следующих значков:

- Значок OK, если модули и компоненты программы работают нормально.
- Значок с количеством проблем (например, 1), если обнаружены проблемы, на которые администратору рекомендуется обратить внимание. В этом случае в правой части окна **Работоспособность системы** отображается подробная информация о проблемах.

Окно **Работоспособность системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов программы, карантина, а также обновления баз на всех серверах, на которых работает программа.

  Пример:
  Если базы одного или нескольких компонентов программы не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок !.
  Для решения проблемы убедитесь, что серверы обновлений доступны. Если для соединения с серверами обновлений вы используете прокси-сервер, убедитесь, что на прокси-сервере нет ошибок, связанных с подключением к серверам Kaspersky Anti Targeted Attack Platform.

- **Обработано** – статус приема и обработки входящих данных. Статус формируется на основе следующих критериев:
  - Состояние получения данных с серверов с компонентом Sensor, с сервера или виртуальной машины с почтовым сенсором, с хостов с программой Kaspersky Endpoint Agent.
  - Информация о превышении максимально допустимого времени, которое объекты ожидают в очереди на проверку модулями и компонентами программы.
- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и мультитенантности).

В случае обнаружения проблем в работоспособности модулей и компонентов программы, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Управление серверами Central Node, PCN или SCN с помощью веб-интерфейса программы

С помощью веб-интерфейса программы вы можете выполнять следующие действия с сервером, на котором установлен компонент Central Node:

- настраивать дату и время сервера;
- выключать и перезагружать сервер;
- генерировать или загружать самостоятельно подготовленный сертификат сервера;
- настраивать сетевые параметры сервера;
- контролировать уровень заполнения дискового пространства сервера.

Если вы используете режим распределенного решения и мультитенантности, 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 мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить дату и время сервера:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Дата и время**.
2. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, в котором находится сервер с компонентом Central Node.

   Вы можете указать страну и часовой пояс, выбрав нужный регион на карте под раскрывающимися списками.
3. 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 .

4. Нажмите на кнопку **Применить**.

Дата и время сервера будут настроены.

Генерация или загрузка TLS-сертификата сервера

Если вы уже используете TLS-сертификат сервера и сгенерируете или загрузите новый сертификат, сертификат, который используется в программе, будет удален и заменен на новый сертификат.

Вам потребуется указать данные нового сертификата везде, где использовался старый.

Если вы замените TLS-сертификат на новый, вам потребуется

- Повторно авторизовать почтовые сенсоры (KSMG, KLMS) на Central Node.
- Повторно настроить соединение Central Node, PCN и SCN с Sandbox.
- Повторно настроить перенаправление трафика от Endpoint Agent на Sensor и доверенное соединение с Endpoint Agent.
- Загрузить новый сертификат в Active Directory (если вы используете Active Directory).

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

Вы можете сгенерировать новый сертификат через веб-интерфейс сервера Central Node или загрузить самостоятельно созданный сертификат.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы сгенерировать TLS-сертификат сервера Central Node:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты**.

3. В разделе **Сертификат сервера** нажмите на кнопку **Сгенерировать**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Kaspersky Anti Targeted Attack Platform сгенерирует новый TLS-сертификат. Страница автоматически обновится.

Связь с почтовыми сенсорами, компонентом Sandbox, программой Kaspersky Endpoint Agent будет прервана до повторной авторизации.

Вы можете самостоятельно подготовить TLS-сертификат и загрузить его через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

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

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

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

Выполняйте действия по загрузке TLS-сертификат в веб-интерфейсе того сервера, на который вы хотите загрузить сертификат.

Чтобы загрузить самостоятельно подготовленный TLS-сертификат через веб-интерфейс Kaspersky Anti Targeted Attack Platform:

1. Войдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform под учетной записью администратора.
2. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты**.
3. В разделе **Сертификат сервера** нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

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

   Окно выбора файлов закроется.

TLS-сертификат будет добавлен в Kaspersky Anti Targeted Attack Platform.

Связь с почтовыми сенсорами, компонентом Sandbox, программой Kaspersky Endpoint Agent будет прервана до повторной авторизации.

Скачивание TLS-сертификата сервера на компьютер

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы скачать TLS-сертификат сервера на компьютер:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сертификаты**.
2. В разделе **Сертификат сервера** нажмите на кнопку **Скачать**.

   Файл сертификата сервера будет сохранен в папке загрузки браузера.

Назначение DNS-имени сервера

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы назначить имя сервера для использования DNS-серверами:

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 сервера будет назначено.

Настройка параметров DNS

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить параметры DNS:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Сетевые параметры**.
2. В блоке параметров **Параметры DNS** в поле **Главный и дополнительный DNS-серверы** введите IP-адреса DNS-серверов.
3. Нажмите на кнопку **Применить**.

   Параметры DNS будут настроены.

Настройка параметров сетевого интерфейса

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить параметры сетевого интерфейса:

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 блоке параметров **Состояние** выберите один из следующих вариантов:
   - **Отключено**.
   - **Включено, используется DHCP-сервер**, если вы хотите, чтобы для сетевого интерфейса использовались параметры, полученные от DHCP-сервера.
   - **Включено, настройка вручную**, если вы хотите, чтобы для сетевого интерфейса использовались параметры, заданные вручную.
4. Если вы выбрали **Включено, настройка вручную**, укажите значения для следующих параметров:
   a. В поле **IP** укажите IP-адрес сетевого интерфейса.
   b. В поле **Маска подсети** укажите маску подсети сетевого интерфейса.
   c. В поле **Шлюз** введите IP-адрес шлюза.
5. Нажмите на кнопку **Сохранить**.

Параметры сетевого интерфейса будут настроены.

Настройка сетевого маршрута для использования по умолчанию

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить сетевой маршрут для использования по умолчанию:

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 поле **Шлюз** введите IP-адрес шлюза.
4. 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 мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить параметры соединения с прокси-сервером:

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.

Настройка параметров соединения с почтовым сервером

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Программа может отправлять уведомления об обнаружениях и работе системы. Для этого необходимо настроить параметры сервера для отправки уведомлений.

Чтобы настроить параметры сервера для отправки уведомлений:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на вкладку **Конфигурация почтового сервера**.
3. В поле **Хост** укажите IP-адрес почтового сервера.
4. В поле **Порт** укажите порт подключения к почтовому серверу.
5. В поле **Отправлять с адреса** укажите адрес электронной почты, с которого будут отправляться уведомления.

6. Если вы хотите включить проверку подлинности на почтовом сервере, установите флажок **Использовать SMTP-проверку подлинности получателей сообщений**.

7. В поле **Имя пользователя** укажите имя пользователя для аутентификации на сервере для отправки уведомлений.

8. В поле **Пароль** укажите пароль для аутентификации на сервере для отправки уведомлений.

9. Если вы хотите использовать TLS-шифрование при отправке уведомлений, установите флажок **Использовать TLS-шифрование**.

10. 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.

11. Нажмите на кнопку **Применить**.

Параметры сервера для отправки уведомлений будут настроены.

Выбор операционных систем для проверки объектов в Sandbox

> Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Вы можете выбрать набор операционных систем, на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox. Вам потребуется установить виртуальные машины с операционными системами, которые соответствуют выбранному набору, на сервере Sandbox.

Чтобы выбрать набор операционных систем:

1. В окне веб-интерфейса программы выберите раздел **Серверы Sandbox**.

2. Выберите закладку **Параметры**.

3. В блоке параметров **Набор ОС** выберите один из вариантов:

- Windows XP, Windows 7, Windows 10.
- CentOS 7.8, Windows XP, Windows 7, Windows 10.
- Astra Linux 1.7, Windows XP, Windows 7, Windows 10.

Kaspersky Anti Targeted Attack Platform будет создавать задачи на проверку объектов в Sandbox в соответствии с выбранным набором.

Если набор операционных систем, установленных на сервере Sandbox, не совпадает с набором, выбранным на сервере Central Node, объекты не отправляются на проверку этому серверу Sandbox. При подключении к серверу Central Node нескольких серверов Sandbox программа отправляет объекты на проверку тем серверам Sandbox, на которых установлены операционные системы, соответствующие выбранному на Central Node набору.

Вы можете изменить набор операционных систем в ходе эксплуатации программы. В этом случае вам нужно убедиться, что конфигурация сервера Sandbox соответствует аппаратным требованиям.

В режиме распределенного решения и мультитенантности настройки набора операционных систем, заданные на сервере PCN, не распространяются на подключенные к нему серверы SCN. Вы можете выбрать набор операционных систем для каждого сервера PCN и SCN отдельно.

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 мультитенантности, выполняйте действия по подключению к серверам PCN или SCN.

Просмотр таблицы серверов с компонентом Sensor

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.

Обработка запроса на подключение от компонента Sensor

Если вы используете режим распределенного решения и мультитенантности, 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.

Настройка максимального размера проверяемого файла

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить максимальный размер проверяемого файла:

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 мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить получение зеркалированного трафика со SPAN-портов:

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 столбце **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 мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить интеграцию с почтовым сервером по протоколу SMTP:

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.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с почтовым сервером.

Чтобы настроить отказоустойчивую интеграцию с почтовым сервером:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.

2. В параметрах почтового сервера укажите это доменное имя.

   Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

Настройка TLS-шифрования соединений с почтовым сервером по протоколу SMTP

Если вы используете режим распределенного решения и мультитенантности, 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:

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. 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 мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

При использовании отдельного прокси-сервера Kaspersky Anti Targeted Attack Platform не обеспечивает шифрование ICAP-трафика и аутентификацию ICAP-клиентов по умолчанию. Администратору программы необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Anti Targeted Attack Platform с помощью туннелирования трафика или средствами iptables.

Чтобы включить интеграцию с прокси-сервером по протоколу ICAP:

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.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с прокси-сервером.

Чтобы настроить отказоустойчивую интеграцию с прокси-сервером:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.

2. В параметрах прокси-сервера укажите это доменное имя.

Интеграция с прокси-сервером будет настроена по доменному имени. Прокси-сервер обратится к случайному серверу кластера. При отказе этого сервера прокси-сервер будет обращаться к другому работоспособному серверу кластера.

Настройка интеграции с почтовым сервером по протоколу POP3

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Чтобы настроить интеграцию с почтовым сервером по протоколу POP3:

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.

    Почтовый сервер должен поддерживать базовую аутентификацию (Basic Authentication).

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.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с почтовым сервером.

Чтобы настроить отказоустойчивую интеграцию с почтовым сервером:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.

2. В параметрах почтового сервера укажите это доменное имя.

Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

Управление кластером

Этот раздел содержит информацию об управлении серверами кластера.

Просмотр таблицы серверов кластера

Чтобы просмотреть таблицу серверов кластера:

1. Выполните вход в веб-интерфейс для управления масштабированием.

2. Перейдите в раздел **Кластер**.

Откроется окно с таблицей.

В таблице содержится следующая информация:

- **Тип сервера** – тип сервера в зависимости от его роли в кластере.

Могут отображаться следующие значения:

- **Хранение**.
- **Обработка**.

- **Состояние** – состояние сервера.
  Могут отображаться следующие значения:
  - **Подключен**.
  - **Не подключен**.
- **Имя хоста** – имя сервера.
- **IP** – IP-адрес сервера.
- **ОЗУ** – уровень загрузки оперативной памяти сервера.
- **ЦП** – уровень загрузки процессора сервера.
- **Действие** – действия, которые вы можете выполнить с сервером.
  Доступно следующее действие: **Удалить**.

Добавление сервера в кластер

Для добавления сервера в кластер вам нужно запустить установку Kaspersky Anti Targeted Attack Platform на этом сервере и выполнить шаги по установке компонентов. Добавленный сервер отобразится в списке серверов кластера.

Увеличение дискового пространства сервера хранения

Вы можете увеличить дисковое пространство функционирующего сервера хранения, установив дополнительный диск.

> Для увеличения дискового пространства сервера хранения с помощью дополнительного диска вам требуется обратиться в Службу технической поддержки.

Настройка сервера производится в режиме Technical Support Mode.

Вывод серверов из эксплуатации

> Для вывода из эксплуатации функционирующего сервера вам требуется обратиться в Службу технической поддержки.

При отказе сервера вы можете вывести его из эксплуатации самостоятельно.

Чтобы вывести из эксплуатации неработоспособный обрабатывающий сервер:

1. Удалите сервер из кластера.
2. Настройте параметры масштабирования программы для новой конфигурации.

   Обрабатывающий сервер будет выведен из эксплуатации.

Чтобы вывести из эксплуатации неработоспособный сервер хранения:

1. Добавьте новый сервер хранения в кластер.
2. Удалите неработоспособный сервер хранения из кластера.

   Сервер хранения будет выведен из эксплуатации.

Удаление сервера из кластера

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Удаленный сервер нельзя восстановить. Убедитесь, что выбранный сервер не функционирует.

Чтобы удалить сервер из кластера:

1. Выполните вход в веб-интерфейс для управления масштабированием.
2. Перейдите в раздел **Кластер**.
3. В столбце **Действие** нажмите на ссылку **Удалить** напротив того сервера, который вы хотите удалить.
4. Нажмите на кнопку **Продолжить**.

   Процесс удаления будет запущен. Удаление может занять около суток. Информация об удаленном сервере не будет отображаться в таблице серверов.

После удаления сервера вы можете изменить конфигурацию серверов кластера или добавить сервер с аналогичной ролью, чтобы сохранить производительность программы на прежнем уровне.

Включение и выключение кластера

Для выключения и включения кластера вам рекомендуется обратиться в Службу технической поддержки. Не выполняйте выключение и включение кластера при возникновении проблем с работоспособностью приложения.

Если вы хотите отключить питание работоспособных серверов кластера, вам нужно предварительно выключить кластер, чтобы избежать потери данных.

Чтобы выключить кластер:

1. Выполните вход в веб-интерфейс для управления масштабированием.
2. Перейдите в раздел **Кластер**.
3. Нажмите на кнопку **Выключить**.

   Работа основных компонентов программы будет остановлена. Вы можете отключить питание серверов кластера.

Чтобы запустить серверы кластера:

1. Отключите питание серверов, если оно не было отключено ранее.
2. Включите питание сервера хранения.
3. Включите питание остальных серверов.

   Серверы кластера будут запущены.

Веб-интерфейс для управления масштабированием становится доступным, когда запускается больше половины серверов кластера. Например, если в кластере 7 серверов, веб-интерфейс будет доступен при включении 4 серверов кластера.

Уведомления о максимальной загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor

Высокая загрузка центрального процессора и оперативной памяти серверов Central Node и Sensor может привести к неработоспособности компонентов программы.

Вы можете настроить максимальные допустимые значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor, при превышении которых в верхней части окна раздела **Мониторинг** веб-интерфейса программы для пользователей с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Администратор** и **Локальный администратор** отобразится рамка желтого цвета с предупреждением. Также вы можете настроить отправку уведомлений на адрес или адреса электронной почты и соединение с протоколом SNMP для отправки данных об уровне загрузки центрального процессора и оперативной памяти во внешние системы, поддерживающие этот протокол.

Если вы развернули компоненты Central Node и Sensor в виде кластера, предупреждения отображаются отдельно для каждого сервера кластера.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** также могут создавать правила для отправки уведомлений. В этом случае для корректной отправки уведомлений вам требуется предварительно настроить максимальные допустимые значения загрузки центрального процессора и оперативной памяти серверов, а также параметры сервера для отправки уведомлений.

В существующих правилах для отправки уведомлений о работе компонентов программы функция уведомления о загрузке центрального процессора и оперативной памяти серверов будет включена автоматически, если при создании правила в блоке параметров **Компоненты** был установлен флажок **Все**.

Настройка максимального допустимого значения загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor

В режиме распределенного решения и мультитенантности вам нужно задать максимальные допустимые значения загрузки центрального процессора и оперативной памяти на каждом сервере Central Node, с которого вы хотите получать уведомления. Если вы используете кластер Central Node, вы можете настроить эти параметры на любом сервере кластера.

Чтобы настроить максимальное допустимое значение загрузки центрального процессора и оперативной памяти серверов Central Node и Sensor:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке параметров **Мониторинг** выполните следующие действия:
   - В поле **Уведомление о загрузке ЦП более чем на N % в течение M минут** укажите максимальное допустимое значение загрузки центрального процессора и время, в течение которого указанная загрузка считается допустимой.

     По умолчанию максимальное допустимое значение загрузки центрального процессора составляет 95% в течение 5 минут.

- В поле **Уведомление о загрузке ОЗУ более чем на N % в течение M минут** укажите максимальное допустимое значение загрузки оперативной памяти и время, в течение которого указанная загрузка считается допустимой.

  По умолчанию максимальное допустимое значение загрузки оперативной памяти составляет 95% в течение 5 минут.

3. Нажмите на кнопку **Применить**.

Максимальное значение загрузки центрального процессора и оперативной памяти серверов будет настроено. При превышении одного из заданных показателей на сервере Central Node и/или Sensor, в верхней части окна раздела **Мониторинг** веб-интерфейса программы для пользователей с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Администратор** и **Локальный администратор** отобразится рамка желтого цвета с предупреждением.

Настройка соединения с протоколом SNMP

Вы можете отправлять данные о загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor во внешние системы, поддерживающие протокол SNMP. Для этого вам требуется настроить параметры соединения с протоколом.

Если компонент Central Node развернут в виде кластера, во внешние системы отправляются данные о загрузке центрального процессора и оперативной памяти каждого сервера кластера.

Чтобы настроить параметры соединения с протоколом SNMP на сервере Central Node:

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

2. В блоке параметров **SNMP** установите флажок **Использовать SNMP**.

3. В поле **Версия протокола** выберите одну из следующих версий протокола:

   - **v2c**.

   - **v3**.

4. Если вы выбрали версию протокола **v2c**, в поле **Строка сообщества** укажите пароль, который будет использоваться для подключения к Kaspersky Anti Targeted Attack Platform.

5. Если вы выбрали **v3**, выполните следующие действия:

   a. В поле **Протокол аутентификации** выберите один из следующих вариантов проверки достоверности и целостности данных, переданных во внешнюю систему:

      - **MD5**.

      - **SHA256**.

   b. В поле **Имя пользователя** укажите имя пользователя.

c. В поле **Пароль** укажите пароль для аутентификации.

> Имя пользователя и пароль, заданные в полях **Имя пользователя** и **Пароль** должны совпадать с именем пользователя и паролем, заданными при создании учетной записи во внешней системе. Если данные не совпадают, соединение не будет установлено.

d. В поле **Протокол шифрования** выберите один из следующих типов шифрования:

- **DES**.
- **AES**.

e. В поле **Пароль** укажите пароль для шифрования.

> Пароль, заданный в этом поле, должен совпадать с паролем, заданным во внешней системе.

Параметры соединения с протоколом на сервере Central Node будут настроены. При успешной обработке запроса на получение данных на сервере внешней системы отобразится информация о загрузке центрального процессора и оперативной памяти сервера Central Node.

Чтобы настроить параметры соединения с протоколом SNMP на сервере Sensor:

1. Войдите в консоль управления сервера Sensor 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 компонента программы.
3. Выполните шаги 2 – 5 инструкции, приведенной выше.

Параметры соединения с протоколом на сервере Sensor будут настроены. При успешной обработке запроса на сервере внешней системы отобразится информация о загрузке центрального процессора и оперативной памяти сервера Sensor.

> В режим распределенного решения и мультитенантности параметры соединения с протоколом SNMP для каждого сервера PCN, SCN и Sensor настраиваются отдельно.

Описание объектов MIB Kaspersky Anti Targeted Attack Platform

В таблице ниже приведена информация об объектах MIB Kaspersky Anti Targeted Attack Platform.

Данные о загрузке жесткого диска, центрального процессора и оперативной памяти серверов Central Node и Sensor

Данные о загрузке жесткого диска, центрального процессора и оперативной памяти серверов Central Node и Sensor

Символьное имя	Описание	Идентификатор (OID)
dskTotal	Размер диска или тома, КБ.	1.3.6.1.4.1.2021.9.1.6
dskAvail	Свободное пространство на диске, КБ.	1.3.6.1.4.1.2021.9.1.7
dskUsed	Используемое пространство на диске, КБ.	1.3.6.1.4.1.2021.9.1.8
dskPercent	Процент используемого пространства на диске, %.	1.3.6.1.4.1.2021.9.1.9
laLoad	Среднее значение загрузки системы (load average) в течение 1, 5 и 15 минут.	1.3.6.1.4.1.2021.10.1.3
memTotalReal	Размер оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.5
memAvailReal	Количество используемой оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.6
memTotalFree	Количество свободной оперативной памяти, КБ.	1.3.6.1.4.1.2021.4.11

Работа с информацией о хостах с Kaspersky Endpoint Agent

Программа Kaspersky Endpoint Agent устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации. Программа осуществляет постоянное наблюдение за процессами, запущенными на этих хостах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор**, **Локальный администратор** и **Администратор** могут оценить регулярность получения данных с хостов, на которых установлена программа Kaspersky Endpoint Agent, на закладке **Endpoint Agents** окна веб-интерфейса программы в рамках тех тенантов, к данным которых у них есть доступ. Если вы используете режим распределенного решения и мультитенантности, то в веб-интерфейсе сервера PCN отображается список хостов с программой Kaspersky Endpoint Agent для PCN и всех подключенных SCN.

Пользователи с ролью **Локальный администратор** и **Администратор** могут настроить отображение регулярности получения данных с хостов, на которых установлена программа Kaspersky Endpoint Agent, в рамках тех тенантов, к данным которых у них есть доступ.

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети любой из хостов с программой Kaspersky Endpoint Agent в рамках тех тенантов, к данным которых у него есть доступ. При этом соединение между сервером с компонентом Central Node и хостом с программой Kaspersky Endpoint Agent не будет прервано.

Для оказания поддержки при неполадках в работе программы Kaspersky Endpoint Agent 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.

Специалисты Службы технической поддержки сообщат вам необходимую для выполнения перечисленных действий информацию (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав получаемых в отладочных целях данных. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных 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 настоящем руководстве, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

Выбор тенанта для работы в разделе Endpoint Agents

Если вы используете режим распределенного решения и мультитенантности, перед началом работы в разделе **Endpoint Agents** вам нужно выбрать тенанты, данные по которым вас интересуют.

*Чтобы выбрать тенант для работы в разделе **Endpoint Agents**:*

1. В верхней части меню веб-интерфейса программы нажмите на стрелку рядом с названием тенанта.
2. В раскрывшемся списке выберите тенант.

   Отобразятся данные по выбранному вами тенанту. Если вы хотите изменить тенант, вам нужно повторить действия по выбору тенанта.

Просмотр таблицы хостов с Kaspersky Endpoint Agent на отдельном сервере Central Node

Таблица хостов с программой Kaspersky Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса программы.

Если вы используете отдельный сервер Central Node, не используете режим распределенного решения и мультитенантности, в таблице хостов с программой Kaspersky Endpoint Agent могут отображаться следующие данные:

- Количество хостов и показатели активности программы Kaspersky Endpoint Agent:
  - **Критическое бездействие** – количество хостов, от которых последние данные были получены очень давно.
  - **Предупреждение** – количество хостов, от которых последние данные были получены давно.
  - **Нормальная активность** – количество хостов, от которых последние данные были получены недавно.

- **Хост** – имя хоста с программой Kaspersky Endpoint Agent.
- **IP** – IP-адрес компьютера, на который установлена программа Kaspersky Endpoint Agent.
- **ОС** – версия операционной системы, установленной на компьютере с программой Kaspersky Endpoint Agent.
- **Версия** – версия установленной программы Kaspersky Endpoint Agent.
- **Активность** – показатель активности программы Kaspersky Endpoint Agent. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке в столбцах таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Просмотр таблицы хостов с Kaspersky Endpoint Agent в режиме распределенного решения и мультитенантности

Таблица хостов с программой Kaspersky Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса программы.

Если вы используете режим распределенного решения и мультитенантности, в таблице содержится информация о хостах с программой Kaspersky Endpoint Agent, подключенных к PCN и всем серверам SCN. В таблице могут отображаться следующие данные:

- Количество хостов и показатели активности программы Kaspersky Endpoint Agent:
  - **Критическое бездействие** – количество хостов, от которых последние данные были получены очень давно.
  - **Предупреждение** – количество хостов, от которых последние данные были получены давно.
  - **Нормальная активность** – количество хостов, от которых последние данные были получены недавно.
- **Хост** – имя хоста с программой Kaspersky Endpoint Agent.
- **Серверы** – имена серверов, к которым подключен хост с программой Kaspersky Endpoint Agent.
- **IP** – IP-адрес компьютера, на который установлена программа Kaspersky Endpoint Agent.
- **ОС** – версия операционной системы, установленной на хосте с программой Kaspersky Endpoint Agent.

- **Версия** – версия установленной программы Kaspersky Endpoint Agent.
- **Активность** – показатель активности хоста с программой Kaspersky Endpoint Agent. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылкам в столбцах таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Просмотр информации о хосте

Чтобы просмотреть информацию о хосте с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.
2. Выберите хост, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- В разделе **Хост**:
  - **Имя** – имя хоста с программой Kaspersky Endpoint Agent.
  - **IP** – IP-адрес хоста, на который установлена программа Kaspersky Endpoint Agent.
  - **ОС** – версия операционной системы на хосте, на который установлена программа Kaspersky Endpoint Agent.
  - **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и мультитенантности.
  - **Имя сервера** – имя сервера Central Node.

- В разделе **Endpoint Agent**:
  - **Версия** – версия установленной программы Kaspersky Endpoint Agent.
  - **Активность** – показатель активности программы Kaspersky Endpoint Agent. Может иметь 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.
  - **Подключен к серверу** – имя сервера, Central Node, SCN или PCN, к которому подключен хост.
  - **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
  - **Лицензия** – состояние лицензионного ключа программы Kaspersky Endpoint Agent.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по имени хоста

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по имени хоста:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Agents**.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов имени хоста.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent, изолированных от сети

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent, изолированные от сети:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Хост** откройте окно настройки фильтрации.

3. Установите флажок **Показывать только изолированные Endpoint Agents**.

4. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по именам серверов PCN и SCN

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по именам серверов PCN и SCN, к которым подключены эти хосты.

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по именам серверов PCN и SCN:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Серверы** откройте окно настройки фильтрации.

3. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с программой Kaspersky Endpoint Agent.

4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по IP-адресу компьютера

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по IP-адресу компьютера, на котором установлена программа:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **IP** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по версии операционной системы на компьютере

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по версии операционной системы, установленной на компьютере с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **ОС** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов версии операционной системы.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по версии Kaspersky Endpoint Agent

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по версии программы Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Версия** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов версии программы Kaspersky Endpoint Agent.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по их активности

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по их активности:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Активность** откройте окно настройки фильтрации.

3. Установите флажки рядом с одним или несколькими показателями активности программы Kaspersky Endpoint Agent:

   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.

4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра хостов с Kaspersky Endpoint Agent

Чтобы быстро создать фильтр хостов с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением столбца таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

   Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

   - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
   - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра хостов с Kaspersky Endpoint Agent

Чтобы сбросить фильтр хостов с программой Kaspersky Endpoint Agent по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

2. Нажмите на кнопку справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Настройка показателей активности Kaspersky Endpoint Agent

Пользователи с ролью **Локальный администратор** и **Администратор** могут определить, какой период бездействия программы Kaspersky Endpoint Agent считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности программы Kaspersky Endpoint Agent. Пользователям с ролью **Аудитор** доступен только просмотр параметров показателей активности программы Kaspersky Endpoint Agent. Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут просмотреть показатели активности программы Kaspersky Endpoint Agent в столбце **Активность** таблицы хостов с Kaspersky Endpoint Agent в разделе **Endpoint Agents** окна веб-интерфейса программы.

Чтобы настроить показатели активности программы Kaspersky Endpoint Agent, выполните следующие действия:

1. Войдите в веб-интерфейс программы под учетной записью **Локальный администратор**, **Администратор** или **Старший сотрудник службы безопасности**.
2. В окне веб интерфейса программы выберите раздел **Параметры**, подраздел **Endpoint Agents**.
3. В полях под названием раздела введите количество дней бездействия хостов с программой Kaspersky Endpoint Agent, которое вы хотите отображать как **Предупреждение** и **Критическое бездействие**.
4. Нажмите на кнопку **Применить**.

Показатели активности программы Kaspersky Endpoint Agent будут настроены.

Поддерживаемые интерпретаторы и процессы

Программа Kaspersky Endpoint Agent 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 программой Kaspersky Endpoint Agent, представлена в таблице ниже.

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

Процесс	Расширения файлов
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

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:

1. **Создание запроса на подключение к компоненту Sandbox**

   Вы можете создать запрос в веб-интерфейсе программы под учетной записью администратора. Если у вас есть несколько компонентов Central Node, установленных на сервере, вам нужно создать запрос для каждого сервера с компонентом Central Node, который вы хотите подключить к компоненту Sandbox. Если компонент Central Node развернут в виде кластера, вы можете создать запрос на подключение с любого сервера кластера.

2. **Обработка запроса на подключение в веб-интерфейсе Sandbox**

   Вы можете принять или отклонить каждый запрос.

Если вы хотите подключить несколько компонентов Sandbox к одному компоненту Central Node, убедитесь, что на подключаемых компонентах Sandbox совпадают наборы операционных систем для проверки объектов и максимальное количество одновременно запускаемых виртуальных машин.

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:

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:

1. В окне веб-интерфейса программы выберите раздел **Серверы Sandbox**.

   Отобразится таблица серверов с компонентами Sandbox.

2. В строке с нужным сервером в столбце **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:

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.

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:

1. **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 или Справку Kaspersky Security для Linux Mail Server.

   Для интеграции других внешних систем необходимо использовать REST API.

2. **Подтверждение интеграции на стороне Kaspersky Anti Targeted Attack Platform**

   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.

3. **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 этом столбце 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:

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:

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:

1. В окне веб-интерфейса программы выберите раздел **Внешние системы**.

2. Выполните одно из следующих действий:

   - Включите переключатель рядом с названием параметра **Максимальный приоритет проверки**, если вы хотите включить максимальный приоритет обработки трафика от почтовых сенсоров.
   - Выключите переключатель рядом с названием параметра **Максимальный приоритет проверки**, если вы хотите отключить максимальный приоритет обработки трафика от почтовых сенсоров.

Приоритет обработки трафика от почтовых сенсоров будет настроен.

Настройка интеграции с Kaspersky Managed Detection and Response

Программа Kaspersky Managed Detection and Response (далее также "MDR") предназначена для обнаружения и предотвращения мошеннических действий в инфраструктуре клиента. MDR обеспечивает непрерывную управляемую защиту и позволяет организациям автоматически выявлять труднообнаружимые угрозы и освобождать сотрудников группы IT-безопасности для решения задач, требующих их участия.

Kaspersky Anti Targeted Attack Platform получает данные и отправляет их в Kaspersky Managed Detection and Response с помощью потока Kaspersky Security Network. Поэтому для настройки интеграции с MDR обязательно участие в KSN.

Интеграция с MDR доступна только при наличии хотя бы одной действующей лицензий KATA или EDR. Если в программе добавлен один лицензионный ключ (только KATA или только EDR), то статистика отправляется в рамках функциональности, предусмотренной этой лицензией. Если в программе добавлено оба лицензионных ключа, то статистика отправляется в полном объеме.

Перед настройкой интеграции Kaspersky Anti Targeted Attack Platform с программой MDR требуется получить архив с конфигурационным файлом на портале MDR.

Настройка интеграции с MDR доступна только Локальному администратору и Администратору веб-интерфейса программы.

Включение интеграции с MDR

Убедитесь, что в программе добавлен активный лицензионный ключ и настроено участие в KSN. В противном случае интеграция с MDR будет недоступна.

Чтобы включить интеграцию с MDR:

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. В блоке переметров **Интеграция MDR** нажмите на кнопку **Загрузить**, чтобы загрузить конфигурационный файл.

   Откроется окно выбора файлов.
4. Выберите архив, полученный при регистрации на портале MDR, и нажмите кнопку **Open**.

В окне отобразится следующая информация о лицензии MDR:

- **Серийный номер**.
- **Дата окончания срока действия**.
- **Осталось дней**.

Интеграция с MDR будет включена. Параметры интеграции, указанные в конфигурационном файле, будут распространены на все подключенные компоненты Sensor. Программа MDR начнет использовать статистику о выявленных обнаружениях, отправляемую через поток KSN.

Отключение интеграции с MDR

Чтобы отключить интеграцию с MDR:

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. В блоке переметров **Интеграция MDR** нажмите на кнопку **Удалить файл**.
4. В окне подствержения нажмите на кнопку **Да**.

Конфигурационный файл будет удален, а интеграция с MDR будет отключена. Программа продолжит отправлять статистику на серверы KSN, однако эта информация не будет использоваться программой MDR.

Замена конфигурационного файла MDR

Чтобы заменить конфигурационный файл MDR:

1. Войдите в веб-интерфейс программы под учетной записью администратора.
2. Выберите раздел **Параметры**, подраздел **KSN/KPSN и MDR**.
3. В блоке переметров **Интеграция MDR** нажмите на кнопку **Заменить файл**.

   Откроется окно выбора файла.
4. Выберите новый архив с конфигурационным файлом и нажмите на кнопку **Open**.

   В веб-интерфейсе программы обновится информация о лицензии MDR.

Конфигурационный файл будет заменен. Новые параметры интеграции будут распространены на все подключенные компоненты Sensor.

Настройка интеграции с SIEM-системой

Kaspersky Anti Targeted Attack Platform может публиковать информацию о действиях пользователей в веб-интерфейсе программы и обнаружениях в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

Для передачи данных вы можете использовать TLS-шифрование.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с внешней системой одним из следующих способов:

- Использовать функцию Round Robin.
- Настроить параметры внешней системы, чтобы при возникновении сетевой ошибки внешняя система переключалась между IP-адресами серверов кластера.

Чтобы настроить отказоустойчивую интеграцию с внешней системой:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах почтового сервера укажите это доменное имя.

   Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

Включение и отключение записи информации в удаленный журнал

Вы можете настроить запись информации о действиях пользователей в веб-интерфейсе и обнаружениях в удаленный журнал. Файл журнала хранится на сервере, на котором установлена SIEM-система. Для записи в удаленный журнал необходимо настроить параметры интеграции с SIEM-системой.

Чтобы включить или отключить запись информации о действиях пользователей в веб-интерфейсе и обнаружениях в удаленный журнал:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Если вы хотите включить / отключить запись информации о действиях пользователей в веб-интерфейсе в удаленный журнал, выполните одно из следующих действий:

   - Если вы хотите включить запись информации о действиях пользователей в веб-интерфейсе, установите флажок **Журнал активности**.
   - Если вы хотите отключить запись информации о действиях пользователей в веб-интерфейсе, снимите флажок **Журнал активности**.

3. Если вы хотите включить / отключить запись информации об обнаружениях в удаленный журнал, выполните одно из следующих действий:

   - Если вы хотите включить запись информации об обнаружениях, установите флажок **Обнаружения**.
   - Если вы хотите отключить запись информации об обнаружениях, снимите флажок **Обнаружения**.

   Вы можете установить оба флажка одновременно.

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

Запись информации в удаленный журнал будет включена или отключена.

Пользователи с ролью **Аудитор** могут только просматривать информацию о настройках записи в удаленный журнал.

Настройка основных параметров интеграции с SIEM-системой

Чтобы настроить основные параметры интеграции с SIEM-системой:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Установите флажки **Журнал активности** и / или **Обнаружения**.

   Вы можете установить один из флажков или оба флажка одновременно.

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 хоста** укажите идентификатор хоста. Хост с этим идентификатором в журнале SIEM-системы будет указан как источник обнаружения.
7. В поле **Периодичность сигнала** введите интервал отправки сообщений в SIEM-систему.
8. Нажмите на кнопку **Применить** в нижней части окна.

Основные параметры интеграции с SIEM-системой будут настроены.

Пользователи с ролью **Аудитор** могут только просматривать информацию о настройках интеграции с SIEM-системой.

Загрузка TLS-сертификата

Чтобы загрузить TLS-сертификат для шифрования соединения с SIEM-системой:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. В разделе **TLS-шифрование** нажмите на кнопку **Загрузить**.

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

   Окно выбора файлов закроется.

   TLS-сертификат будет добавлен в программу.
4. Нажмите на кнопку **Применить** в нижней части окна.

Загруженный TLS-сертификат будет использоваться для шифрования соединения с SIEM-системой.

Включение и отключение TLS-шифрования соединения с SIEM-системой

Чтобы включить или отключить TLS-шифрование соединения с SIEM-системой:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **SIEM-система**.
2. Установите флажки **Журнал активности** и / или **Обнаружения**.

   Вы можете установить один из флажков или оба флажка одновременно.
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.

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: `5.0.0-5201`.

- 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 |5.0.0-5201|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.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
`file_web`	`File from web detected` В сетевом трафике обнаружен файл.	• `dvchost` = <имя сервера с компонентом Central Node>. • `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)).
`file_mail`	`File from mail detected` В почтовом трафике обнаружен файл.	• `dvchost` = <имя сервера с компонентом Central Node>. • `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>. • `KasperskyLabKATAmailEnvelopeFrom` = <адрес электронной почты отправителя> (из заголовка Received). • `KasperskyLabKATAmailFor` = <адрес электронной почты получателя> (из заголовка Received). • `KasperskyLabKATAmailRecievedFromIp` = <IP-адрес первого в цепочке отправки сообщения сервера> (из заголовка Received). • `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>.
`ids`	`IDS event detected` Обнаружение выполнено модулем Intrusion Detection System.	• `dvchost` = <имя сервера с компонентом Central Node>. • `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>.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
		• 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 или Sandbox в сетевом трафике.	• dvchost = <имя сервера с компонентом Central Node>. • 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>.
url_mail	URL from mail detected Обнаружение выполнено технологией URL Reputation или Sandbox в почтовом трафике.	• dvchost = <имя сервера с компонентом Central Node>. • eventId = <ID обнаружения>. • rt = <дата и время обнаружения>. • externalId = <ID сообщения электронной почты>. • suser = <адрес электронной почты отправителя>. • duser = <адреса электронной почты получателей>. • KasperskyLabKATAmailEnvelopeFrom = <адрес электронной почты отправителя> (из заголовка Received). • KasperskyLabKATAmailFor = <адрес получателя> (из заголовка Received). • KasperskyLabKATAmailRecievedFromIp = <IP-адрес первого в цепочке отправки сообщения сервера> (из заголовка Received). • 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 Sandbox). • cs1 = <список типов обнаруженных объектов по классификации "Лаборатории Касперского"> (для Sandbox) или <список категорий> (для URL Reputation). • cs3 = <версия баз, с помощью которых проверен файл> (только для Sandbox).
dns	DNS request detected Обнаружение выполнено технологией URL Reputation в DNS-трафике.	• dvchost = <имя сервера с компонентом Central Node>. • 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>.
file_endpoint	File from endpoint detected	• dvchost = <имя сервера с компонентом Central Node>. • eventId = <ID обнаружения>.

Тип обнаружения	Наименование и описание обнаружения	Ключ и описание его значения
	Обнаружение выполнено компонентом Kaspersky Endpoint Agent на хосте пользователя и содержит файл.	• `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>.
`iocScanning`	`IOC has tripped on endpoint` Обнаружение выполнено в результате IOC-проверки хостов с Kaspersky Endpoint Agent для Windows. Этот тип обнаружений доступен, если вы используете функциональность KEDR.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения>. • `src` = <IP-адрес источника>. • `shost` = <имя хоста, на котором обнаружен файл>. • `cs1` = <имя IOC-файла, по которому выполнено обнаружение>.
`taaScanning`	`TAA has tripped on events database` Обнаружение выполнено в результате IOA-анализа событий. Этот тип обнаружений доступен, если вы используете функциональность KEDR.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения>. • `shost` = <имя хоста, на котором выполнено обнаружение>. • `cs1` = <имя IOA-правила, по которому выполнено обнаружение>.
`yaraScanningEP`	`YARA has tripped on endpoint` Обнаружение выполнено в результате YARA-проверки хостов с Kaspersky Endpoint Agent для Windows. Этот тип обнаружений доступен, если вы используете функциональность KEDR.	• `dvchost` = <имя сервера с компонентом Central Node>. • `eventId` = <ID обнаружения>. • `rt` = <дата и время обнаружения>. • `src` = <IP-адрес источника>. • `shost` = <имя хоста, на котором выполнено обнаружение>. • `cs1` = <имя YARA-правила, по которому выполнено обнаружение>.
`heartbeat`	Периодическое сообщение, содержащее статус компонентов.	• `dvchost` = <имя сервера с компонентом Central Node>. • `rt` = <дата и время события>. • `KasperskyLabKATAcomponentName` = <название компонента>. • `KasperskyLabKATAcomponentState` = <статус компонента> (`0` – OK, `>0` – Ошибка).

Управление журналом активности

Некоторые действия пользователей в веб-интерфейсе программы могут привести к ошибкам в работе Kaspersky Anti Targeted Attack Platform. Вы можете включить запись информации о действиях пользователей в веб-интерфейсе программы в журнал и при необходимости просмотреть эту информацию, скачав файлы журнала.

Включение и отключение записи информации в журнал активности

Чтобы включить или отключить запись информации о действиях пользователей в веб-интерфейсе Kaspersky Anti Targeted Attack Platform в журнал активности:

1. В окне веб-интерфейса программы перейдите в раздел **Отчеты**, подраздел **Журнал активности**.
2. Выполните одно из следующих действий:
   - Установите переключатель **Журнал активности** в положение **Включено**, если хотите включить запись информации о действиях пользователей в веб-интерфейсе программы в журнал активности.
   - Установите переключатель **Журнал активности** в положение **Отключено**, если хотите отключить запись информации о действиях пользователей в веб-интерфейсе программы в журнал активности.

     По умолчанию функция включена.

Запись информации производится в течение 30 дней в файл журнала user_actions.log. По истечении 30 дней файл user_actions.log будет сохранен на сервере с компонентом Central Node в директории /var/log/kaspersky/apt-base/ с названием user_actions.log<month>. Для записи информации за текущий месяц будет создан новый файл с названием user_actions.log. Каждый файл хранится 90 дней, после чего удаляется.

Для того, чтобы просмотреть файлы журнала активности, вам нужно предварительно скачать их.

Вы можете настроить запись информации о действиях пользователей в веб-интерфейсе программы 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.

В режиме распределенного решения информация о действиях пользователей в веб-интерфейсе записывается в журнал того сервера, в веб-интерфейсе которого работают пользователи. Информация о действиях пользователей сервера PCN, влияющих на параметры серверов SCN, записывается в журнал сервера PCN.

Пользователи с ролью **Аудитор** могут только просматривать настройки записи информации в журнал активности.

Скачивание файла журналов активности

Чтобы скачать файл журнала активности:

1. В окне веб-интерфейса программы перейдите в раздел **Отчеты**, подраздел **Журнал активности**.
2. Нажмите на кнопку **Скачать**.

Файлы журнала будут сохранены на ваш локальный компьютер в папку загрузки браузера. Файлы загружаются в формате ZIP-архива.

В режиме распределенного решения вы можете скачать файлы журнала активности только для того сервера, в веб-интерфейсе которого работаете.

Содержание и свойства CEF-сообщений о действиях пользователей в веб-интерфейсе

В заголовке каждого сообщения 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: `5.0.0-5201`.

- Тип события.

  См. таблицу ниже.

- Наименование события.

  См. таблицу ниже.

- Важность события.

  Текущее значение поля: `Low`.

  Пример:
  ```
  CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|5.0.0-5201|tasks|Managing tasks|Low|
  ```

Все поля тела CEF-сообщения представлены в формате `"<ключ>=<значение>"`. Ключи, а также их значения, содержащиеся в сообщении, приведены в таблице ниже.

Тип события	Наименование и описание события	Ключ и описание его значения
sensors	Managing the Sensor component Подключение компонента Sensor к серверу Central Node, изменение настроек компонента.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
sb	Configuring integration with the Sandbox component Подключение компонента Sandbox к серверу Central Node.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
ex_integration	Configuring integration with external systems Настройки интеграции с внешними системами.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
ksn_kpsn_mdr	Participation in KSN, KPSN and MDR Настройка участия в Kaspersky Security Network, включение / отключение использования Kaspersky Private Security Network и настройка интеграции с Kaspersky Managed Detection and Response.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
yara	Managing YARA rules Операции с правилами YARA.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>. • device external ID = <идентификатор хоста в режиме распределенного решения>. • cs1label = <имя загружаемого файла>
ioc	Managing indicator of compromise Операции с правилами IOC.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>. • deviceExternalID = <идентификатор хоста в режиме распределенного решения>.
ids	Managing IDS rules Операции с правилами IDS.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>. • deviceExternalID = <идентификатор хоста в режиме распределенного решения>.
taa	Managing TAA rules Операции с правилами TAA (IOA).	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.
prevention	Managing prevention rules Операции с правилами запрета.	• dvs = <IP-адрес сервера>. • eventId = <ID события>. • rt = <дата и время события>. • src = <IP-адрес пользователя>. • user = <имя пользователя>. • cs1 = <тип события>.

Тип события	Наименование и описание события	Ключ и описание его значения
`exclusions`	`Managing scan exclusions` Операции с правилами исключений из проверки.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>.
`tasks`	`Managing tasks` Операции с задачами.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>.
`network_isolation`	`Network isolation of Endpoint Agent hosts` Сетевая изоляция хостов Endpoint Agent.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>.
`settings`	`Settings` Изменение параметров сервера Central Node.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>.
`settings`	`Settings` Набор ОС виртуальных машин изменен на <версия набора ОС>.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>. • `cs1label` = <имя сервера, на котором обновились настройки>.
`mt`	`Managing CN, PCN and SCN servers` Изменение параметров сервера Primary Central Node и Secondary Central Node в режиме распределенного решения и мультитенантности.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>.
`user_account`	`Managing user accounts` Действия с учетными записями пользователей.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>.
`notifications`	`Sending notifications` Настройка отправки уведомлений на электронный адрес почты.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>.
`license`	`License` Управление лицензионным ключом.	• `dvs` = <IP-адрес сервера>. • `eventId` = <ID события>. • `rt` = <дата и время события>. • `src` = <IP-адрес пользователя>. • `user` = <имя пользователя>. • `cs1` = <тип события>.

Если одна операция проводится с более чем 30 объектами одновременно, в журнал записывается одно сообщение об этой операции. В сообщении указывается информация об операции и количество объектов, с которыми она была проведена.

Обновление баз программы

Базы программы (далее также "базы") представляют собой файлы с записями, на основании которых компоненты и модули программы обнаруживают события, происходящие в IT-инфраструктуре вашей организации.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, в том числе угроз "нулевого дня", создают для них идентифицирующие записи и включают их в пакеты обновлений баз (далее также "пакеты обновлений"). *Пакет обновлений* представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента выпуска предыдущего пакета обновлений. Рекомендуется регулярно получать пакеты обновлений. При установке программы дата выпуска баз соответствует дате выпуска программы, поэтому базы нужно обновить сразу после установки программы.

Программа периодически автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского" (с периодичностью один раз в 30 минут). По умолчанию, если базы компонентов программы по каким-либо причинам не обновляются в течение 24 часов, Kaspersky Anti Targeted Attack Platform отображает эту информацию в разделе **Мониторинг** окна веб-интерфейса программы.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN может быть недоступна в программе на территории США.

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:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Общие параметры**.
2. В блоке **Обновление баз** в раскрывающемся списке **Источник обновлений** выберите одно из следующих значений:

   - **Сервер обновлений "Лаборатории Касперского"**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTP и загружать актуальные базы.

   - **Сервер обновлений "Лаборатории Касперского" (безопасное подключение)**.

     Программа будет подключаться к серверу обновлений "Лаборатории Касперского" по протоколу HTTPS и загружать актуальные базы. Рекомендуется выполнять обновления баз по протоколу HTTPS.

   - **Другой сервер**.

     Программа будет подключаться к вашему FTP- или HTTP-серверу или к папке с базами программы на вашем компьютере и загружать актуальные базы.

3. Если вы выбрали **Другой сервер**, в поле под названием этого параметра укажите URL-адрес пакета обновлений на вашем HTTP-сервере или полный путь к папке с пакетом обновлений баз программы на вашем компьютере.

4. Нажмите на кнопку **Применить**.

Источник обновления баз программы будет выбран.

Запуск обновления баз вручную

Чтобы запустить обновление баз программы вручную:

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

2. В блоке **Обновление баз** нажмите на кнопку **Запустить**.

3. Нажмите на кнопку **Применить**.

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:

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.

Пользователи с ролью **Аудитор** могут просматривать список паролей для архивов без возможности редактирования.

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 / Аудитор**.

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**, **Сотрудник службы безопасности** и **Аудитор** содержит следующие разделы:

- **Мониторинг**. Содержит данные мониторинга Kaspersky Anti Targeted Attack Platform.
- **Обнаружения**. Содержит информацию об обнаружениях в сети тенанта, к которому у вас есть доступ.
- **Поиск угроз**. Содержит информацию о событиях, найденных на хостах тенанта, к которому у вас есть доступ.
- **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.
- **Пользовательские правила**: **TAA**, **IDS**, **IOC** и **YARA**. Содержит информацию для работы с пользовательскими правилами.
- **Хранилище**: **Файлы** и **Карантин**. Содержит информацию для работы с объектами на карантине и в Хранилище.

- **Endpoint Agents**. Содержит информацию о компьютерах с программой Kaspersky Endpoint Agent и их параметрах.
- **Отчеты**: **Созданные отчеты** и **Шаблоны**. Содержит конструктор отчетов и список созданных отчетов об обнаружениях.
- **Параметры**: **Расписание IOC-проверки**, **Endpoint Agents**, **Репутационная база KPSN**, **Правила уведомлений**, **Статус VIP**, **Исключения**, **Пароли к архивам** и **Лицензия**. Содержит информацию о расписании IOC-проверки, параметрах публикации объектов в KPSN, присвоении обнаружениям статуса VIP на основе информации, содержащейся в обнаружениях, списке разрешенных объектов и исключениях из проверки правил IDS и TAA (IOA), 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 тенанта для работы в веб-интерфейсе программы

Если вы используете режим распределенного решения и мультитенантности под учетной записью **Старший сотрудник службы безопасности** или **Сотрудник службы безопасности**, перед началом работы с веб-интерфейсом вам нужно выбрать тенант, в рамках которого вы хотите работать с веб-интерфейсом программы.

Чтобы выбрать тенант для работы в веб-интерфейсе программы:

1. В верхней части меню веб-интерфейса программы нажмите на стрелку рядом с названием тенанта.
2. В раскрывающемся меню **Выберите тенант** выберите тенант из списка.

   Вы также можете ввести несколько символов названия тенанта в строку поиска и выбрать его из списка результатов поиска.

Все действия в веб-интерфейсе программы будут связаны с выбранным тенантом. Если вы хотите изменить тенант, вам нужно повторить действия по выбору тенанта.

Выбор тенанта для работы в веб-интерфейсе недоступен для пользователей с ролью **Аудитор**.

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью виджетов в разделе **Мониторинг** окна веб-интерфейса программы. Вы можете добавлять, удалять, перемещать виджеты, настраивать масштаб отображения виджетов и выбирать период отображения данных.

О виджетах и схемах расположения виджетов

С помощью виджетов вы можете осуществлять мониторинг работы программы.

Схема расположения виджетов – вид рабочей области окна веб-интерфейса программы в разделе **Мониторинг**. Вы можете добавлять, удалять и перемещать виджеты на схеме расположения виджетов, а также настраивать масштаб виджетов.

Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту.

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 виджеты:

- Обнаружения:
  - **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.
  - **Обнаружения по вектору атаки**. Отображение обнаруженных объектов по направлению атаки.
  - **VIP-обнаружения по степени важности**. Отображение важности обнаружений со статусом VIP в соответствии с тем, какое влияние они могут оказать на безопасность компьютера или локальной сети организации, по опыту "Лаборатории Касперского".
  - **Обнаружения по степени важности**. Отображение важности обнаружений для пользователя Kaspersky Anti Targeted Attack Platform в соответствии с тем, какое влияние они могут оказать на безопасность компьютеров или локальной сети организации, по опыту "Лаборатории Касперского".

  В левой части каждого виджета перечислены векторы атаки, степени важности обнаружений, состояния обнаружений и технологии, выполнившие обнаружения. В правой части каждого виджета отображается количество раз, которое программа обнаружила их за выбранный период отображения данных на виджетах.

  По ссылке с названием вектора атаки, степенью важности обнаружений, состоянием обнаружений и технологией, выполнившей обнаружения, можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть связанные обнаружения. При этом обнаружения будут отфильтрованы по выбранному элементу.
- Топ 10:
  - **Домены**. 10 доменов, наиболее часто встречающихся в обнаружениях.
  - **IP-адреса**. 10 IP-адресов, наиболее часто встречающихся в обнаружениях.
  - **Адреса отправителей**. 10 отправителей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.

- **Адреса получателей**. 10 получателей сообщений электронной почты, наиболее часто встречающихся в обнаружениях.
- **Хосты TAA**. 10 хостов, наиболее часто встречающихся в событиях и обнаружениях, выполненных технологией Targeted Attack Analyzer (TAA).
- **Правила TAA**. 10 правил TAA (IOA), наиболее часто встречающихся в событиях и обнаружениях, выполненных технологией Targeted Attack Analyzer (TAA).
- **Отправлено в Sandbox по правилам TAA**. 10 правил TAA (IOA), по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox.

В левой части каждого виджета перечислены домены, адреса получателей, IP-адреса и адреса отправителей сообщений, имена хостов и названия правил TAA (IOA). В правой части каждого виджета отображается количество раз, которое программа обнаружила их за выбранный период отображения данных на виджетах.

По ссылке с именем каждого домена, адреса получателя, IP-адреса и адреса отправителя сообщений , именем хоста и названию правила TAA (IOA) можно перейти в раздел **Обнаружения** веб-интерфейса программы и просмотреть связанные обнаружения. При этом обнаружения будут отфильтрованы по выбранному элементу.

Добавление виджета на текущую схему расположения виджетов

Чтобы добавить виджет на текущую схему расположения виджетов:

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 **Виджеты**.
5. В появившемся окне **Настроить виджеты** включите переключатель рядом с виджетом, который вы хотите добавить.

Виджет будет добавлен на текущую схему расположения виджетов.

Перемещение виджета на текущей схеме расположения виджетов

Чтобы переместить виджет на текущей схеме расположения виджетов:

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 виджет, который вы хотите переместить на схеме расположения виджетов.
5. Нажав и удерживая левую клавишу мыши на верхней части виджета, перетащите виджет на другое место схемы расположения виджетов.
6. Нажмите на кнопку **Сохранить**.

Текущая схема расположения виджетов будет сохранена.

Удаление виджета с текущей схемы расположения виджетов

Чтобы удалить виджет с текущей схемы расположения виджетов:

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 виджета, который вы хотите удалить со схемы расположения виджетов.

   Виджет будет удален из рабочей области окна веб-интерфейса программы.
5. Нажмите на кнопку **Сохранить**.

Виджет будет удален с текущей схемы расположения виджетов.

Сохранение схемы расположения виджетов в PDF

Чтобы сохранить схему расположения виджетов в PDF:

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 виджетов в формате PDF будет сохранена на жесткий диск вашего компьютера в папку загрузки браузера.
6. Нажмите на кнопку **Закрыть**.

Настройка периода отображения данных на виджетах

Вы можете настроить отображение данных на виджетах за следующие периоды:

- **День**.
- **Неделя**.
- **Месяц**.

Чтобы настроить отображение данных на виджетах за сутки (с 00:00 до 23:59):

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 виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Чтобы настроить отображение данных на виджетах за неделю (с понедельника по воскресенье):

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 виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Чтобы настроить отображение данных на виджетах за месяц (календарный месяц):

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 виджете.

На всех виджетах страницы **Мониторинг** отобразятся данные за выбранный вами период.

Настройка масштаба отображения виджетов

Вы можете настроить масштаб отображения виджетов типа "Обнаружения". В правом верхнем углу виджетов, масштаб отображения которых можно настроить, есть значок ☰.

Чтобы настроить масштаб отображения виджетов:

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 виджета.
5. В раскрывшемся списке выберите один из следующих размеров отображения виджета:
   - **1x1 размер**.
   - **2x1 размер**.
   - **3x1 размер**.

   Масштаб отображения выбранного виджета изменится.
6. Повторите действия для всех виджетов, масштаб отображения которых вы хотите изменить.
7. Нажмите на кнопку **Сохранить**.

Масштаб отображения виджетов будет настроен.

Основные принципы работы с виджетами типа "Обнаружения"

Для всех виджетов типа "Обнаружения" можно настроить масштаб отображения.

В левой части каждого виджета отображается легенда виджета по цветам, которые используются на виджетах.

Пример:
На виджете **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 виджете **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 виджетах.

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 виджете **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 виджетах.
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 виджетах. Данные будут отфильтрованы по следующим параметрам: **Время**, **Тип объекта**=FILE и **Источник объекта**=MAIL.

В правой части каждого виджета отображаются столбцы данных. На вертикальной оси отображается количество событий, на горизонтальной оси отображаются дата и время обнаружения. Вы можете изменить период отображения данных на виджетах и выбрать тенант, информация о которых должна быть представлена на виджете.

При наведении курсора мыши на каждый столбец данных отображается количество обнаружений, подсчитанных за период, представленный этим столбцом. По умолчанию отображается количество необработанных обнаружений. Вы можете включить отображение обработанных обнаружений, установив флажок **Обработано** в правом верхнем углу окна. В этом случае будет отображаться количество всех обнаружений.

Просмотр состояния работоспособности модулей и компонентов программы

Если в работе модулей и компонентов программы возникли проблемы, на которые администратору рекомендуется обратить внимание, в верхней части окна раздела **Мониторинг** веб-интерфейса программы отображается рамка желтого цвета с предупреждениями.

Пользователю с ролью **Локальный администратор**, **Администратор** или **Аудитор** доступна информация о работоспособности того сервера Central Node, PCN или SCN, на котором он сейчас работает.

Пользователю с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** или **Аудитор** доступна следующая информация о работоспособности:

- Если вы используете отдельный сервер Central Node, пользователю доступна информация о работоспособности того сервера Central Node, на котором он сейчас работает.
- Если вы используете режим распределенного решения и мультитенантности и пользователь работает на сервере SCN, пользователю доступна информация о работоспособности этого сервера SCN в рамках тех тенантов, к данным которых у него есть доступ.
- Если вы используете режим распределенного решения и мультитенантности и пользователь работает на сервере PCN, пользователю доступна информация о работоспособности этого сервера PCN и всех серверов SCN, подключенных к этому серверу, в рамках тех тенантов, к данным которых у него есть доступ.

Чтобы получить более подробную информацию о работоспособности модулей и компонентов программы,

по ссылке **Просмотреть сведения** откройте окно **Работоспособность системы**.

В окне **Работоспособность системы** в зависимости от работоспособности модулей и компонентов программы отображается один из следующих значков:

- Значок OK, если модули и компоненты программы работают нормально.
- Значок с количеством проблем (например, 1), если обнаружены проблемы, на которые администратору рекомендуется обратить внимание. В этом случае в правой части окна **Работоспособность системы** отображается подробная информация о проблемах.

Окно **Работоспособность системы** содержит разделы:

- **Работоспособность компонентов** – статус работы модулей и компонентов программы, карантина, а также обновления баз на всех серверах, на которых работает программа.

  Пример:
  Если базы одного или нескольких компонентов программы не обновлялись в течение 24 часов, рядом с именем сервера, на котором установлены модули и компоненты программы, отображается значок .
  Для решения проблемы убедитесь, что серверы обновлений доступны. Если для соединения с серверами обновлений вы используете прокси-сервер, убедитесь, что на прокси-сервере нет ошибок, связанных с подключением к серверам Kaspersky Anti Targeted Attack Platform.

- **Обработано** – статус приема и обработки входящих данных. Статус формируется на основе следующих критериев:

  - Состояние получения данных с серверов с компонентом Sensor, с сервера или виртуальной машины с почтовым сенсором, с хостов с программой Kaspersky Endpoint Agent.

  - Информация о превышении максимально допустимого времени, которое объекты ожидают в очереди на проверку модулями и компонентами программы.

- **Соединение с серверами** – состояние соединения между сервером PCN и подключенными серверами SCN (отображается, если вы используете режим распределенного решения и мультитенантности).

В случае обнаружения проблем в работоспособности модулей и компонентов программы, которые вы не можете решить самостоятельно, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Просмотр таблицы 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.

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".
  - Google.
  - Apple.
  - Microsoft.

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 мультитенантности, то ротация производится на всех SCN, а затем происходит синхронизация с PCN. После синхронизации все удаленные обнаружения автоматически удаляются также на PCN.

Таблица обнаружений находится в разделе **Обнаружения**.

> По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

Вы можете сортировать обнаружения в таблице по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

В таблице обнаружений содержится следующая информация:

1. **VIP** – наличие у обнаружения статуса с особыми правами доступа. Например, обнаружения со статусом VIP недоступны для просмотра пользователями программы **Сотрудник службы безопасности**.
2. **Создано** – время, в которое программа выполнила обнаружение и **Обновлено** – время, в которое обнаружение было обновлено.
3. – важность обнаружения для пользователя 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 тому тенанту, с которым вы работаете в веб-интерфейсе программы. Информация о серверах отображается только когда вы работаете в режиме распределенного решения и мультитенантности.

9. **Технологии** – названия модулей или компонентов программы, выполнивших обнаружение.

   В столбце **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**.
   - **(IOC) IOC**.

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 этом столбце отображается имя пользователя, которому назначено данное обнаружение. Например, Administrator.

Если информация в столбцах 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 TIP**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- SHA256-хеш:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Найти события**.
  - **Найти на TIP**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.
- IP-адрес назначения: **Найти события**.
- Состояние обнаружения:
  - **Назначить мне**.
  - **Закрыть обнаружение**.

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.

Настройка отображения таблицы обнаружений

Вы можете настроить отображение столбцов, а также порядок их следования в таблице обнаружений.

Чтобы настроить отображение таблицы обнаружений:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.

5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.

6. Нажмите на кнопку **Применить**.

Отображение таблицы обнаружений будет настроено.

Фильтрация, сортировка и поиск обнаружений

Вы можете отфильтровать обнаружения для отображения в таблице обнаружений по одному или нескольким столбцам таблицы или выполнить поиск обнаружений по некоторым столбцам 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 мультитенантности, вы не сможете сохранять фильтры на PCN.

Фильтры сохраняются для каждого из пользователей на том сервере, на котором они созданы.

Вы также можете сортировать обнаружения в таблице по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

По умолчанию в разделе отображается информация только об обнаружениях, не обработанных пользователями. Если вы хотите, чтобы информация об обработанных обнаружениях тоже отображалась, включите переключатель **Обработано** в правом верхнем углу окна.

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:

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:

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.

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:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По значку раскройте список параметров фильтрации.

3. Выберите одну или несколько из следующих степеней важности обнаружений:

   - **Низкая** – обнаружение низкой степени важности.
   - **Средняя** – обнаружение средней степени важности.
   - **Высокая** – обнаружение высокой степени важности.

Если ни одно из значений не выбрано, в таблице отображаются обнаружения всех степеней важности.

4. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по категориям обнаруженных объектов

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Обнаружено** – одна или несколько категорий объекта, обнаруженного в событии. Например, если вы хотите, чтобы программа отображала в таблице обнаружения файлов, зараженных определенным вирусом, вы можете задать фильтр по названию этого вируса.

Чтобы отфильтровать или найти обнаружения по категориям обнаруженных объектов:

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:

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**.
- **Файл**.
- **Тип файла**.
- **MD5**.
- **SHA256**.
- **URL**.
- **Домен**.
- **Агент пользователя**.
- **Тема**.
- **HTTP-статус**.
- **Источник объекта**.
- **Тип объекта**.
- **Автоотправка в Sandbox**.
- **Правило TAA (IOA)**.

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:

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:

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 мультитенантности, серверы относятся к тому тенанту, с которым вы работаете в веб-интерфейсе программы. Фильтрация доступна только на PCN.

Чтобы отфильтровать или найти обнаружения по имени сервера:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке **Серверы** раскройте список серверов, на которых выполнены обнаружения.

3. Установите флажки рядом с одним или несколькими именами серверов.

4. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по названию технологии

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Технологии** – названия модулей или компонентов программы, выполнивших обнаружение.

Чтобы отфильтровать обнаружения по названию технологии:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации обнаружений:

   - **Содержит**, если вы хотите, чтобы программа отображала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Не содержит**, если вы хотите, чтобы программа скрывала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Равняется**, если вы хотите, чтобы программа отображала обнаружения, выполненные модулем или компонентом программы, который вы укажете.
   - **Не равняется**, если вы хотите, чтобы программа скрывала обнаружения, выполненные модулем или компонентом программы, который вы укажете.

4. В раскрывающемся списке справа от выбранного вами оператора фильтрации обнаружений выберите название технологии, по которой вы хотите отфильтровать обнаружения:

   - **(YARA) YARA**.
   - **(SB) Sandbox**.
   - **(URL) URL Reputation**.
   - **(IDS) Intrusion Detection System**.
   - **(AM) Anti-Malware Engine**.
   - **(TAA) Targeted Attack Analyzer**.
   - **(IOC) IOC**.

   Например, если вы хотите, чтобы программа отобразила в списке обнаружения, выполненные компонентом Sandbox, выберите оператор фильтрации **Содержит** и название компонента **(SB) Sandbox**.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице обнаружений отобразятся только обнаружения, соответствующие заданным вами условиям.

Фильтрация и поиск обнаружений по состоянию их обработки пользователем

Вы можете отфильтровать обнаружения, а также осуществить их поиск в таблице обнаружений по показателю **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.

Чтобы отфильтровать или найти обнаружения по состоянию их обработки пользователем Kaspersky Anti Targeted Attack Platform:

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.

Сортировка обнаружений в таблице

Вы можете сортировать обнаружения в таблице по столбцам **Создано** или **Обновлено**, **Важность**, **Адрес источника** и **Состояние**.

Чтобы отсортировать обнаружения в таблице обнаружений:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Если вы хотите отсортировать обнаружения по дате, справа от названия столбца **Создано** (если в таблице отображается дата создания обнаружений) или **Обновлено** (если в таблице отображается дата обновления обнаружений) нажмите на один из значков:

   - ↑ – новые обнаружения отобразятся вверху таблицы.
   - ↓ – старые обнаружения отобразятся вверху таблицы.

3. Если вы хотите отсортировать обнаружения по степени важности, справа от значка ≣ нажмите на один из значков:

   - ↑ – обнаружения высокой степени важности отобразятся вверху таблицы.
   - ↓ – обнаружения низкой степени важности отобразятся вверху таблицы.

4. Если вы хотите отсортировать обнаружения по адресу источника обнаруженного объекта, справа от названия столбца **Адрес источника** нажмите на один из значков:

   - ↑ – сортировка выполнится по алфавиту A–Z.
   - ↓ – сортировка выполнится по алфавиту Z–A.

5. Если вы хотите отсортировать обнаружения по состоянию их обработки пользователем, справа от названия столбца **Состояние** нажмите на один из значков:

   - ↑ – обнаружения будут отсортированы по порядку их обработки **Новое** - **Повторная проверка** - **В обработке** - **Закрыто**.
   - ↓ – обнаружения будут отсортированы по порядку их обработки **Закрыто** - **В обработке** - **Повторная проверка** - **Новое**.

Быстрое создание фильтра обнаружений

Чтобы быстро создать фильтр обнаружений:

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 столбца 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:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Нажмите на кнопку справа от того заголовка столбца 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 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 с помощью программы Kaspersky Endpoint Agent, установленной на компьютеры, входящие в IT-инфраструктуру организации.

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 (32-разрядную), Windows 7 (64-разрядную), Windows 10 (64-разрядную) и CentOS 7.8, 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 проверки интернет-трафика на наличие признаков вторжения в IT-инфраструктуру организации по предустановленным правилам, выполненной модулем Intrusion Detection System (IDS);

- результаты исследования сетевой активности, выполненного по правилам TAA (IOA) "Лаборатории Касперского";

- результаты исследования сетевой активности, выполненного по пользовательским правилам TAA (IOA), IDS, IOC.

Если обнаружены процессы, запущенные на компьютере локальной сети организации, на котором установлена программа Kaspersky Endpoint Agent, в веб-интерфейсе программы может отображаться следующая информация:

- общая информация об обнаружении и процессах, запущенных на этом компьютере;
- результаты исследования сетевой активности компьютера, выполненного по правилам TAA (IOA) "Лаборатории Касперского";
- результаты исследования сетевой активности компьютера, выполненного по пользовательским правилам TAA (IOA), IOC.

Просмотр информации об обнаружении

Чтобы просмотреть информацию об обнаружении:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Левой клавишей мыши нажмите на строку с тем обнаружением, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об обнаружении.

Общая информация об обнаружении любого типа

Независимо от того, какой технологией выполнено обнаружение - в заголовке окна с информацией об обнаружении отображается идентификатор обнаружения. Рядом с состоянием отображается значок ☆ или ★ в зависимости от наличия у обнаружения статуса VIP.

В верхней части окна с информацией об обнаружении может отображаться следующая общая информация об обнаружении:

- **Состояние** – состояние обнаружения в зависимости от того, обработал пользователь Kaspersky Anti Targeted Attack Platform это обнаружение или нет.
- **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 тому тенанту, с которым вы работаете в веб-интерфейсе программы.
- **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 объекте:

- Имя файла.

  По ссылке с именем файла раскрывается действие **Скопировать значение в буфер**.

- Тип файла. Например, ExecutableWin32.

  Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла.

  Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

  Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.

- Размер файла в килобайтах.

- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- **SHA256** – SHA256-хеш файла.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти на virustotal.com**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- **Email отправителя** – адрес электронной почты, с которого было отправлено сообщение, содержащее файл.

- **Email получателя** – один или несколько адресов электронной почты, на которые было отправлено сообщение, содержащее файл.

- **Исходный email отправителя** – исходный адрес электронной почты, с которого было отправлено сообщение, содержащее файл.

  Данные для этого поля берутся из заголовка Received.

- **Исходный email получателя** – исходный адрес или адреса электронной почты, на которые было отправлено сообщение, содержащее файл.

  Данные для этого поля берутся из заголовка Received.

- **Тема** – тема сообщения.

- **IP сервера-отправителя** – IP-адрес первого в цепочке отправки сообщения почтового сервера.

  По ссылке **IP сервера-отправителя** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.

- **Заголовки** – 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.

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, Post или Connect.

- **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 TIP по URL**.
  - **Найти на TIP по имени домена**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **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 TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Имя пользователя** – имя учетной записи пользователя, действия которого привели к возникновению события.
- **Запрос/Ответ** – длина запроса и ответа.

Информация в блоке Результаты проверки

В блоке **Результаты проверки** могут отображаться следующие результаты проверки обнаружения:

- Названия модулей или компонентов программы, выполнивших обнаружение.
- Одна или несколько категорий обнаруженного объекта. Например, может отображаться название вируса Virus.Win32.Chiton.i.
- Версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, выполнивших обнаружение.
- Результаты проверки обнаружений модулями и компонентами программы:
  - **YARA** – результаты потоковой проверки файлов и объектов, поступающих на Central Node, или результаты проверки хостов с Kaspersky Endpoint Agent. Может принимать следующие значения:
    - Категория обнаруженного файла в правилах YARA (например, может отображаться название категории susp_fake_Microsoft_signer).

      Отображается при потоковой проверке.

      Кнопка **Создать правило запрета** позволяет запретить запуск файла.

      Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.
    - Путь к файлу и/или имя дампа памяти.

      Отображается при проверке хостов с Kaspersky Endpoint Agent.

По ссылке с путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

Кнопка **Создать задачу** позволяет создать следующие задачи:

- **Собрать данные** → **Файл**, **Образ диска**, **Дамп памяти**.
- **Удалить файл**.
- **Поместить файл на карантин**.

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Просмотреть на карантине** позволяет просмотреть информацию об объекте, помещенном на карантин.

- **SB** (Sandbox) – результаты исследования поведения файла, выполненного компонентом Sandbox.

  Нажатием на кнопку **Sandbox-обнаружение** вы можете открыть окно с подробной информацией о результатах исследования поведения файла.

  Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

  Кнопка **Создать правило запрета** позволяет запретить запуск файла.

  Вы можете загрузить подробный журнал исследования поведения файла во всех операционных системах нажав на кнопку **Скачать сведения об отладке**.

  Файл загружается в формате ZIP-архива, зашифрованного паролем infected. Имя проверенного файла внутри архива заменено на MD5-хеш файла. Расширение файла внутри архива не отображается.

  > По умолчанию максимальный объем жесткого диска для хранения журналов исследования поведения файлов во всех операционных системах составляет 300 ГБ. По достижении этого ограничения программа удаляет журналы исследования поведения файлов, созданные раньше остальных, и заменяет их новыми журналами.

- **URL** (URL Reputation) – категория обнаруженного вредоносного, фишингового URL-адреса или URL-адреса, который ранее использовался злоумышленниками для целевых атак на IT-инфраструктуру организаций.

- **IDS** (Intrusion Detection System) – категория обнаруженного объекта по базе Intrusion Detection System или название пользовательского правила IDS, по которому было выполнено обнаружение. Например, может отображаться категория Trojan-Clicker.Win32.Cycler.a.

  По ссылке открывается информация о категории объекта в базе угроз "Лаборатории Касперского" Kaspersky Threats.

- **AM** (Anti-Malware Engine) – категория обнаруженного объекта по антивирусной базе. Например, может отображаться название вируса Virus.Win32.Chiton.i.

  По ссылке открывается информация о категории объекта в базе угроз "Лаборатории Касперского" Kaspersky Threats.

  Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

- **TAA** (Targeted Attack Analyzer) – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

- **IOC** – Название IOC-файла, по которому было выполнено обнаружение.

  При выборе IOC-файла открывается окно с результатами IOC-проверки.

  По ссылке **Все события, связанные с обнаружением** в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **MD5**, **FileFullName**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

Информация в блоке Правило IDS

В блоке **Правило IDS** отображается информация об обнаружении, выполненном технологией IDS (Intrusion Detection System), в формате матрицы HEX-редактора.

HEX-редактор (англ. hex-editor), шестнадцатеричный редактор — приложение для редактирования данных, в котором данные представлены как последовательность байтов.

В верхней части матрицы отображается длина правила IDS.

В левой части матрицы отображаются данные правила в текстовом формате.

В разделе **Содержание правила** блока **Правило IDS** отображается заголовок правила IDS и данные IDS-обнаружения в формате Suricata. Например, могут отбражаться данные о направлении трафика (`flow`), метод HTTP-запроса (`http_method`), HTTP-заголовок (`http_header`), идентификатор безопасности (`sid`).

Информация в блоке Сетевое событие

В блоке **Сетевое событие** может отображаться следующая информация о ссылке на веб-сайт, открытой на компьютере:

- **Дата** и **Время** – дата и время сетевого события.
- **Метод** – тип HTTP-запроса, например, GET или POST.
- **IP источника** – IP-адрес компьютера, на котором была открыта ссылка на веб-сайт.
- **IP назначения** – IP-адрес компьютера, с которого была открыта ссылка на веб-сайт.
- **URL** – тип HTTP-запроса, например, GET или POST и URL-адрес веб-сайта.

По ссылке с URL-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP по URL**.
- **Найти на TIP по имени домена**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

- **Агент пользователя** – 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.

Результаты проверки в Sandbox

В окне результатов проверки объекта в Sandbox могут отображаться следующие сведения об обнаружении:

- **Файл** – полное имя и путь проверенного файла.
- **Размер файла** – размер файла.
- **MD5** – MD5-хеш файла.

  По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Создать правило запрета**.
  - **Скопировать значение в буфер**.

- **Обнаружено** – одна или несколько категорий обнаруженных объектов. Например, если программа обнаружила файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** будет указана категория Trojan-Downloader.JS.Cryptoload.ad для этого обнаружения.
- **Время обработки** – время выполнения проверки файла.
- **Версии баз** – версии баз модулей и компонентов Kaspersky Anti Targeted Attack Platform, выполнивших обнаружение.

Кнопка **Новое правило запрета** в правом верхнем углу окна позволяет запретить запуск файла.

Информация о результатах исследования поведения файла приводится для каждой операционной системы, в которой компонент Sandbox выполнил проверку. Для операционной системы Windows 7 (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 в столбце **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.

  По ссылкам в столбце **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти на TIP по URL**.
  - **Найти на TIP по имени домена**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.
- **Журнал действий IDS** – журнал сетевой активности файла. 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.

По ссылкам в столбце **IP назначения** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

По ссылкам в столбце **URL** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP по URL**.
- **Найти на TIP по имени домена**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

- **Журнал DNS-активности** – журнал DNS-активности файла. Содержит следующую информацию:
  - Тип запроса (Request или Response)
  - **DNS-имя** – доменное имя сервера.
  - **Тип** – тип DNS-запроса (например, A или CNAME).
  - **Хост** – имя хоста или IP-адрес, с которым осуществлялось взаимодействие.

  По ссылкам в столбцах **DNS-имя** и **Хост** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - **Найти на TIP**.
  - **Найти события**.
  - **Найти обнаружения**.
  - **Скопировать значение в буфер**.

Кнопка **Скачать полный журнал** в нижней части каждого из режимов проверки **Режим быстрой проверки** и **Режим ведения полного журнала** позволяет скачать журнал исследования поведения файла в каждой операционной системе на компьютер.

Результаты IOC-проверки

В зависимости от типа обработанного объекта, в окне результатов поиска индикаторов компрометации могут отображаться следующие данные:

- **ARP-протокол**:
  - IP-адрес из ARP-таблицы.
  - Физический адрес из ARP-таблицы.
- **DNS-запись**:
  - Тип и имя записи DNS.
  - IP-адрес защищаемого компьютера.
- **Событие в журнале Windows**:
  - Идентификатор записи в журнале событий.
  - Имя источника данных в журнале.
  - Имя журнала.
  - Учетная запись пользователя.
  - Время события.
- **Файл**:
  - MD5-хеш файла.
  - SHA256-хеш файла.
  - Полное имя файла (включая путь).
  - Размер файла.
- **Порт**:
  - Удаленный IP-адрес, с которым было установлено соединение в момент проверки.
  - Удаленный порт, с которым было установлено соединение в момент проверки.
  - IP-адрес локального адаптера.
  - Порт, открытый на локальном адаптере.
  - Протокол в виде числа (в соответствии со стандартом IANA).

- **Процесс**:
  - Имя процесса.
  - Аргументы процесса.
  - Путь к файлу процесса.
  - Windows идентификатор (PID) процесса.
  - Windows идентификатор (PID) родительского процесса.
  - Имя учетной записи пользователя, запустившего процесс.
  - Дата и время запуска процесса.
- **Служба**:
  - Имя службы.
  - Описание службы.
  - Путь и имя DLL-службы (для svchost).
  - Путь и имя исполняемого файла службы.
  - Windows идентификатор (PID) службы.
  - Тип службы (например, драйвер ядра или адаптер).
  - Статус службы.
  - Режим запуска службы.
- **Пользователь**:
  - Имя учетной записи пользователя.
- **Том**:
  - Наименование тома.
  - Буква тома.
  - Тип тома.
- **Реестр**:
  - Значение реестра Windows.
  - Значение куста реестра.
  - Путь к ключу реестра (без куста и без имени значения).
  - Параметр реестра.

- **Переменные окружения**:
  - Физический адрес (MAC) защищаемого компьютера.
  - Система (окружение).
  - Имя ОС с версией.
  - Сетевое имя защищаемого устройства.
  - Домен или группа, к которой принадлежит защищаемый компьютер.

В разделе **IOC** отображается структура IOC-файла. При совпадении обработанного объекта с одним из условий IOC-правила, это условие подсвечивается. Если обработанный объект совпадает с несколькими условиями, выделяется текст всей ветки.

Информация в блоке Хосты

В блоке **Хосты** отображается следующая информация о хостах, на которых сработало правило TAA (IOA):

- **Имя хоста** – IP-адрес или доменное имя компьютера, на котором произошло событие. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного правила и выбранный хост.
- **IP** – IP-адрес компьютера, на котором произошло событие.

  Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный компьютеру на момент создания или обновления обнаружения.

  Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес компьютера не отображается.
- **Количество событий** – количество событий, произошедших на хосте.
- **Найти события**. По ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим ID выбранного правила.

Информация в блоке Журнал изменений

В блоке **Журнал изменений** может отображаться следующая информация об обнаружении:

- Дата и время изменения обнаружения.
- Автор изменений.

  Например, **Система** или имя пользователя программы.

- Изменение, произошедшее с обнаружением.

  Например, обнаружению может быть присвоена принадлежность группе VIP, или оно может быть отмечено как обработанное.

Отправка данных об обнаружении

Вы можете предоставить в "Лабораторию Касперского" данные об обнаружении (кроме технологий URL Reputation и IOC) для дальнейшего исследования.

Для этого необходимо скопировать данные об обнаружении в буфер обмена, а затем отправить их в "Лабораторию Касперского" по электронной почте.

Данные об обнаружении могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Вам необходимо самостоятельно согласовать отправку этих данных для дальнейшего исследования в "Лабораторию Касперского" со Службой безопасности вашей организации.

Чтобы скопировать данные об обнаружении в буфер обмена:

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.

Рекомендации по обработке обнаружений

В составе информации об обнаружениях, выполненных технологиями AM (Anti-Malware Engine), SB (Sandbox), YARA, IOC и IDS (intrusion Detection System) в правой части окна отображаются рекомендации по обработке этих обнаружений.

Чтобы просмотреть информацию об обнаружении:

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.

Рекомендации по обработке AM-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.

  - **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу из обнаружения, над которым вы работаете.

- В разделе **Оценка** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

Рекомендации по обработке TAA-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По имени правила (TAA-обнаружения)**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцам **Обнаружено** и **Технологии** - имени правила TAA (IOA), в соответствии с которым было выполнено обнаружение, и названию технологии **(TAA) Targeted Attack Analyzer**.

  - **По имени правила (SB-обнаружения)**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцам **Обнаружено** и **Технологии** - имени правила TAA (IOA), в соответствии с которым было выполнено обнаружение, и названию технологии **(SB) Sandbox**.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

Рекомендации по обработке SB-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.

  - **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу из обнаружения, над которым вы работаете.

  - **По URL из Sandbox**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу из обнаружения, над которым вы работаете, и всем URL-адресам, связь с которыми нашел компонент Sandbox в процессе обработки обнаружения.

- В разделе **Оценка** выберите **Найти похожие EPP-события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

Рекомендации по обработке IOC-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений, имеющих общие признаки с обнаружением, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** выберите **Найти похожие обнаружения по имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.

- В разделе **Оценка** выберите **Найти похожие обнаружения по IOC**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Обнаружено** - имени IOC-файла из обнаружения, над которым вы работаете.

- В разделе **Сдерживание** выберите **Изолировать <имя хоста>**. Откроется окно создания правила сетевой изоляции.

Чтобы создать правило сетевой изоляции хоста, настройте следующие параметры:

1. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.

2. В блоке параметров **Исключения для правила изоляции хоста** в списке **Направление трафика** выберите направление сетевого трафика, которое не должно быть заблокировано:

   - **Входящее/Исходящее**.

   - **Входящее**.

   - **Исходящее**.

3. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

   Вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

4. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.

5. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**.

6. Нажмите на кнопку **Сохранить**.

Рекомендации по обработке YARA-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

Вы можете выполнить следующие рекомендации:

- В разделе **Оценка** раскройте список **Найти похожие обнаружения**.

  Отобразится список признаков, по которым вы можете найти похожие обнаружения, и количество похожих обнаружений по каждому признаку.

  Выберите один из следующих признаков:

  - **По MD5**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - MD5-хешу. MD5-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По SHA256**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - SHA256-хешу. SHA256-хеш файла из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста из обнаружения, над которым вы работаете, выделено желтым цветом.

  - **По адресу отправителя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Адрес отправителя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По адресу получателя**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес назначения**. Адрес получателя сообщения электронной почты из обнаружения, над которым вы работаете, выделен желтым цветом.

  - **По URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу из обнаружения, над которым вы работаете.

- В разделе **Оценка** выберите выберите **Найти похожие обнаружения по имени хоста**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска выбран тип события **Результат обработки обнаружения** и настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

- В разделе **Расследование** выберите **Найти похожие события**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска, например, по **RemoteIP**, **MD5**, **SHA256**, **URI**. В значениях фильтрации указаны свойства обнаружения, над которым вы работаете. Например, MD5 файла из обнаружения.

  Действие доступно только если вы используете функциональность KEDR и добавили лицензионный ключ KEDR.

- В разделе **Сдерживание** выберите **Изолировать <имя хоста>**. Откроется окно создания правила сетевой изоляции.

Рекомендации по обработке IDS-обнаружений

В правой части окна в блоке **Рекомендации** отображаются рекомендации, которые вы можете выполнить, и количество обнаружений или событий, имеющих общие признаки с обнаружением, над которым вы работаете.

Вы можете выполнить следующие рекомендации::

- В разделе **Оценка** выберите **Найти похожие обнаружения по имени хоста**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Адрес источника**. Имя хоста или IP-адрес из обнаружения, над которым вы работаете, выделено желтым цветом.

- В разделе **Оценка** выберите **Найти похожие обнаружения по URL**. По ссылке в новой вкладке браузера откроется таблица обнаружений **Обнаружения**, отфильтрованных по столбцу **Сведения** - URL-адресу. URL-адрес из обнаружения, над которым вы работаете, выделен желтым цветом.

- В разделе **Оценка** выберите **Добавить в исключения**.

  Откроется окно **Добавить правило IDS в исключения**. Если вы хоте добавить правило IDS, по которому выполнено обнаружение, в исключения, введите комментарий в поле **Описание** и нажмите на кнопку **Добавить**.

  Правило IDS будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса программы, подразделе **Исключения** на закладке **Исключения IDS**.

- В разделе **Расследование** выберите **Найти похожие события по URL**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска по **URI** из обнаружения, над которым вы работаете.

- В разделе **Расследование** выберите **Найти похожие события по имени хоста**. По ссылке в новой вкладке браузера откроется таблица событий **Поиск угроз**. В условиях поиска настроен фильтр поиска по **RemoteIP** из обнаружения, над которым вы работаете.

- В разделе **Расследование** по ссылке **Скачать артефакт IDS** вы можете скачать файл с данными об обнаружении.

- В разделе **Расследование** по ссылке **Скачать PCAP-файл** вы можете скачать файл с данными перехваченного трафика.

Действия пользователей над обнаружениями

При работе в веб-интерфейсе программы под учетной записью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** вы можете выполнять следующие действия над обнаружениями:

- Назначать обнаружение себе или другому пользователю веб-интерфейса программы.

  Вы можете просмотреть все обнаружения, назначенные определенному пользователю, используя фильтр обнаружений по состоянию их обработки пользователем.

- Отметить обнаружение как обработанное.

  Вы можете просмотреть все обнаружения, обработанные определенным пользователем, используя фильтр обнаружений по состоянию их обработки пользователем.

- Добавить комментарий к обнаружению.

  Вы можете найти обнаружения, содержащие комментарий, по ключевым словам комментария, используя фильтр обнаружений по полученной информации.

- 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.

Пользователи с ролью **Аудитор** могут просматривать информацию об обнаружениях без возможности редактирования.

Назначение обнаружений определенному пользователю

Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут назначить обнаружение или несколько обнаружений себе или другому пользователю веб-интерфейса программы с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности**.

Чтобы назначить обнаружение себе или другому пользователю веб-интерфейса программы:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажок напротив обнаружения или 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 нажатием на стрелку справа от кнопки **Назначить** раскройте список пользователей.

4. Выберите пользователя, которому вы хотите назначить обнаружения.

   Откроется окно подтверждения действия. Вы также можете оставить комментарий, который отобразится в истории изменения обнаружения.

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.

Пользователи с ролью **Аудитор** не могут назначать обнаружения себе или другим пользователям веб-интерфейса программы. Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** также не могут назначать обнаружения пользователям с ролью **Аудитор**.

Отметка о завершении обработки одного обнаружения

Чтобы отметить в таблице обнаружений одно обнаружение, назначенное вам, как обработанное:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. В столбце **Состояние** того обнаружения, которое вы хотите отметить как обработанное, левой клавишей мыши нажмите на ваше имя пользователя.

3. В списке действий выберите **Закрыть обнаружение**.

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.

   Раскройте список действий. В правом верхнем углу окна нажмите на стрелку справа от кнопки со статусом обнаружения.

   Откроется список действий.

3. В списке действий выберите **Закрыть обнаружение**.

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.

Если в течение суток (с 00:00 до 23:59) поступит обнаружение по технологии TAA (IOA), IDS, URL, аналогичное обработанному, программа либо создаст новое обнаружение, либо обновит информацию в идентичном обнаружении со статусом **Новое** или **В обработке**.

Для пользователей с ролью **Аудитор** недоступны функции назначения и обработки обнаружений.

Отметка о завершении обработки обнаружений

Чтобы отметить одно или несколько обнаружений как обработанные:

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 **Закрыть обнаружение**.

   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.

Если в течение суток (с 00:00 до 23:59) поступит обнаружение по технологии TAA (IOA), IDS, URL, аналогичное обработанному, программа либо создаст новое обнаружение, либо обновит информацию в идентичном обнаружении со статусом **Новое** или **В обработке**.

Для пользователей с ролью **Аудитор** недоступны функции назначения и обработки обнаружений.

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 для обнаружений:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. Установите флажки напротив обнаружений,для которых вы хотите изменить статус VIP.

   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 **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 для обнаружений будет изменен.

Пользователи с ролью **Старший сотрудник службы безопасности** и **Аудитор** могут просмотреть все обнаружения со статусом VIP, используя фильтр обнаружений по наличию статуса VIP.

Добавление комментария к обнаружению

Пользователи с ролями **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут добавить комментарий к обнаружению.

Чтобы добавить комментарий к обнаружению:

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 блоком **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.

Пользователи с ролью **Аудитор** могут просматривать комментарии к обнаружениям без возможности редактирования.

Поиск угроз по базе событий

При работе в веб-интерфейсе программы вы можете формировать поисковые запросы и использовать IOC-файлы для поиска угроз по базе событий в рамках тех тенантов, к данным которых у вас есть доступ.

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 вы можете создавать и изменять поисковые запросы с помощью текстовых команд.

Вы можете загрузить IOC-файл и искать события по условиям, заданным в этом IOC-файле.

Пользователи с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** также могут создавать правила TAA (IOA) на основе условий поиска событий.

Поиск событий в режиме исходного кода

Чтобы задать условия поиска событий в режиме исходного кода:

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 **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

5. Нажмите на кнопку **Найти**.

   Отобразится таблица событий, соответствующих условиям поиска.

   Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

6. Нажмите на имя того сервера, события по которому вы хотите просмотреть.

Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

Поиск событий в режиме конструктора

Чтобы задать условия поиска событий в режиме конструктора:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.

2. В раскрывающемся списке выберите критерий для поиска событий.

   Доступные критерии для поиска событий

   - В группе **Общие сведения**:
     - Host – имя хоста.
     - HostIP – IP-адрес хоста.
     - EventType – тип события.
     - UserName – имя пользователя.

- OsFamily – семейство операционной системы.
- OsVersion – версия операционной системы, используемой на хосте.

- В группе **Свойства TAA**:
  - IOAId – идентификатор правила TAA (IOA).
  - IOATag – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.
  - IOATechnique – техника MITRE.
  - IOATactics – тактика MITRE.
  - IOAImportance – степень важности, присвоенная событию, выполненному по этому правилу TAA (IOA).
  - IOAConfidence – уровень надежности в зависимости от вероятности ложных срабатываний правила.
- В группе **Свойства файла**:
  - CreationTime – время создания события.
  - FileName – имя файла.
  - FilePath – путь к директории, в которой располагается файл.
  - FileFullName – полный путь к файлу. Включает путь к директории и имя файла.
  - ModificationTime – время изменения файла.
  - FileSize – размер файла.
  - MD5 – MD5-хеш файла.
  - SHA256 – Sha256-хеш файла.
  - SimilarDLLPath – следующая по пути обхода DLL. Вредоносная DLL, помещенная в директорию по стандартному пути обхода, чтобы система загрузила ее раньше, чем исходную DLL.
- В группе **Процессы Linux**:
  - LogonRemoteHost – IP-адрес хоста, с которого был выполнен удаленный вход.
  - RealUserName – имя пользователя, назначенное ему при регистрации в системе.
  - EffectiveUserName – имя пользователя, которое было использовано для входа в систему.
  - Environment – переменные окружения.
  - ProcessType – тип процесса.
  - OperationResult – тип операции.

- В группе **Запущен процесс**:
  - PID – идентификатор процесса.
  - ParentFileFullName – путь к файлу родительского процесса.
  - ParentMD5 – MD5-хеш файла родительского процесса.
  - ParentSHA256 – SHA256-хеш файла родительского процесса.
  - StartupParameters – параметры запуска процесса.
  - ParentPID – идентификатор родительского процесса.
- В группе **Удаленное соединение**:
  - HTTPMethod – метод HTTP-запроса. Например, Get, Post или Connect.
  - ConnectionDirection – направление соединения (входящее или исходящее).
  - LocalIP – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
  - LocalPort – порт локального компьютера, с которого была произведена попытка удаленного соединения.
  - RemoteHostName – имя компьютера, на который была произведена попытка удаленного соединения.
  - RemoteIP – IP-адрес компьютера, на который была произведена попытка удаленного соединения.
  - RemotePort – порт компьютера, на который была произведена попытка удаленного соединения.
  - URI – адрес ресурса, к которому произведен запрос HTTP.
- В группе **Изменение в реестре**:
  - RegistryKey – путь к ключу реестра.
  - RegistryValueName – имя параметра реестра.
  - RegistryValue – значение параметра реестра.
  - RegistryOperationType – тип операции с реестром.
  - RegistryPreviousKey – предыдущий путь к ключу реестра.
  - RegistryPreviousValue – предыдущее имя параметра реестра.
- В группе **Журнал событий ОС**:
  - WinLogEventID – идентификатор типа события безопасности в журнале Windows.
  - LinuxEventType – тип события.

- WinLogName – имя журнала.
- WinLogEventRecordID – идентификатор записи в журнале.
- WinLogProviderName – идентификатор системы, записавшей событие в журнал.
- WinLogTargetDomainName – доменное имя удаленного компьютера.
- WinLogObjectName – имя объекта, инициировавшего событие.
- WinlogPackageName – имя пакета, инициировавшего событие.
- WinLogProcessName – имя процесса, инициировавшего событие.

- В группе **Обнаружение и результат обработки**:
  - DetectName – имя обнаруженного объекта.
  - RecordID – идентификатор сработавшего правила.
  - ProcessingMode – режим проверки.
  - ObjectName – имя объекта.
  - ObjectType – тип объекта.
  - ThreatStatus – режим обнаружения.
  - UntreatedReason – статус обработки события.
  - ObjectContent (for AMSI events too) – содержание скрипта, переданного на проверку.
  - ObjectContentType (for AMSI events too) – тип содержимого скрипта.
- В группе **Интерактивный ввод команд в консоли**:
  - InteractiveInputText – текст, введенный в командную строку.
  - InteractiveInputType – тип ввода (консоль или канал).
- В группе **Изменен файл**:
  - FileOperationType – тип операции с файлом.
  - FilePreviousPath – путь к директории, в которой файл располагался ранее.
  - FilePreviousFullName – полное имя файла, включающее предыдущий путь к директории, в которой файл располагался ранее, и / или предыдущее имя файла.
  - DroppedFileType – тип измененного файла.

3. В раскрывающемся списке выберите оператор сравнения.

Доступные операторы 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 **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

10. Нажмите на кнопку **Найти**.

    Отобразится таблица событий, соответствующих условиям поиска.

    Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

11. Нажмите на имя того сервера, события которого вы хотите просмотреть.

    Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

Сортировка событий в таблице

Вы можете сортировать события в таблице по столбцам **Время события**, **Тип события**, **Хост** и **Имя пользователя**.

Чтобы отсортировать события в таблице событий:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется окно **Поиск угроз**.

2. Задайте условия для поиска событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий, соответствующих условиям поиска.

3. Если вы хотите отсортировать события по времени, справа от названия столбца **Время события** нажмите на один из значков:

   - ↑ – новые события отобразятся вверху таблицы.
   - ↓ – старые события отобразятся вверху таблицы.

4. Если вы хотите отсортировать события по названию типов событий, справа от названия столбца **Тип события** нажмите на один из значков:

   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.

5. Если вы хотите отсортировать события по именам хостов, на которых были выполнены обнаружения, справа от названия столбца **Хост** нажмите на один из значков:

   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.

6. Если вы хотите отсортировать события по именам пользователей хостов, справа от названия **Имя пользователя** нажмите на один из значков:

   - ↑ – сортировка выполнится по алфавиту А–Я.
   - ↓ – сортировка выполнится по алфавиту Я–А.

7. Если вы хотите сгруппировать события по именам хостов или по названию типов событий, выберите в раскрывающемся списке **Группировать по** одно из значений:

   - **Группировать по имени хоста**, если хотите сгруппировать события по именам хостов.
   - **Группировать по типу события**, если хотите сгруппировать события по названиям типов событий.

   Если события были отсортированы по полю **Хост** или **Тип события**, при группировке событий по аналогичному признаку результат сортировки сбрасывается. Чтобы вернуться к результатам сортировки, выберите в раскрывающемся списке **Группировать по** значение **Группировать по**.

По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.

Вы можете отсортировать события только по одному признаку.

При сортировке по типу события на русском языке события сортируются в соответствии с внутренним наименованием типа события на английском языке.

Изменение условий поиска событий

*Чтобы изменить условия поиска событий, выполните следующие действия в разделе **Поиск угроз** окна веб-интерфейса программы:*

1. Нажмите на форму с условиями поиска событий в верхней части окна.
2. Выберите одну из следующих закладок:

   - **Конструктор**, если вы хотите изменить условия поиска событий в режиме конструктора.
   - **Редактор кода**, если вы хотите изменить условия поиска событий в режиме исходного кода.

3. Внесите необходимые изменения.
4. Нажмите на одну из следующих кнопок:

   - **Обновить**, если вы хотите обновить текущий поиск событий новыми условиями.
   - **Новый поиск**, если вы хотите выполнить новый поиск событий.

   Отобразится таблица событий, соответствующих условиям поиска.

Поиск событий по результатам их обработки в программах EPP

Чтобы выполнить поиск событий по результатам их обработки в программах EPP в режиме конструктора:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**, закладку **Конструктор**.

   Откроется форма поиска событий.

2. Если вы хотите выполнить поиск событий по статусу обработки, выполните следующие действия:

   a. В раскрывающемся списке критериев поиска событий в группе **Обнаружение и результат обработки** выберите критерий **ThreatStatus**.

   b. В раскрывающемся списке операторов сравнения выберите один из вариантов:

   - **=** (равно);
   - **!=** (не равно).

   c. В раскрывающемся списке статусов обработки события выберите один из вариантов:

   - **Объект не заражен**.
   - **Объект вылечен**.
   - **Ложное срабатывание**.
   - **Объект добавлен пользователем**.
   - **Объект добавлен в исключения**.
   - **Объект удален**.
   - **Объект помещен на карантин**.
   - **Объект не найден**.
   - **Выполнен откат к предыдущему состоянию**.
   - **Объект не поддается обработке**.
   - **Объект не обработан**.
   - **Обработка прервана**.
   - **Неизвестно**.

3. Если вы хотите выполнить поиск событий по причинам, по которым они не были обработаны, выполните следующие действия:

   a. В раскрывающемся списке критериев поиска событий в группе **Обнаружение и результат обработки** выберите критерий **UntreatedReason**.

   b. В раскрывающемся списке операторов сравнения выберите один из вариантов:

      - **=** (равно);
      - **!=** (не равно).

   c. В раскрывающемся списке причин, по которым события не были обработаны, выберите один из вариантов:

      - **Объект уже был обработан**.
      - **Программа работает в режиме Только отчет**.
      - **Не удалось создать резервную копию объекта**.
      - **Не удалось создать копию объекта**.
      - **Устройство не готово**.
      - **Объект заблокирован**.
      - **Нет прав на выполнение действия**.
      - **Объект невозможно вылечить**.
      - **Объект невозможно перезаписать**.
      - **Объект не найден**.
      - **Нет места на диске**.
      - **Обработка отменена**.
      - **Действие отложено**.
      - **Задача на обработку прервана**.
      - **Ошибка чтения данных**.
      - **Нет данных**.
      - **Объект является критическим системным**.
      - **Ошибка записи данных**.
      - **Запись данных не поддерживается**.
      - **Объект защищен от записи**.

4. Если вы хотите добавить новое условие, используйте логический оператор **AND** или **OR** и повторите действия по добавлению условия.

5. Если вы хотите добавить группу условий, нажмите на кнопку **Group** и повторите действия по добавлению условий.

6. Если вы хотите удалить группу условий, нажмите на кнопку **Remove group**.

7. Если вы хотите выполнить поиск событий за определенный период, в раскрывающемся списке **За все время** выберите один из следующих периодов поиска событий:

   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.

8. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

9. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям поиска.

Загрузка IOC-файла и поиск событий по условиям, заданным в IOC-файле

Чтобы загрузить IOC-файл и искать события по условиям, заданным в этом IOC-файле:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файлов.

3. Выберите IOC-файл, который хотите загрузить, и нажмите на кнопку **Открыть**.

   IOC-файл загрузится.

   На закладке **Редактор кода** в форме с условиями поиска событий отобразятся условия, заданные в загруженном IOC-файле.

Вы можете искать события по этим условиям. Вы также можете изменить условия, заданные в загруженном IOC-файле, или добавить условия поиска событий в режиме исходного кода.

4. Если вы хотите выполнить поиск событий за определенный период, нажмите на кнопку **За все время** и выберите один из следующих периодов поиска событий:

   - **За все время**, если вы хотите, чтобы программа отображала в таблице события, найденные за все время.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий час.
   - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице события, найденные за предыдущий день.
   - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице события, найденные за указанный вами период.

5. Если вы выбрали период отображения найденных событий **Пользовательский диапазон**, выполните следующие действия:

   a. В открывшемся календаре укажите даты начала и конца периода отображения событий.

   b. Нажмите на кнопку **Применить**.

   Календарь закроется.

6. Нажмите на кнопку **Найти**.

Отобразится таблица событий, соответствующих условиям, заданным в IOC-файле.

Создание правила TAA (IOA) на основе условий поиска событий

Чтобы создать правило TAA (IOA) на основе условий поиска событий:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Выполните поиск событий в режиме конструктора или режиме исходного кода.

3. Нажмите на кнопку **Сохранить как правило TAA (IOA)**.

   Откроется окно **Новое правило TAA (IOA)**.

4. В поле **Имя** введите имя правила.

5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В таблице правил TAA (IOA) раздела **Пользовательские правила**, в подразделе **TAA** веб-интерфейса отобразится новое правило с заданным именем.

Не рекомендуется в условиях поиска событий, сохраняемых как пользовательское правило TAA (IOA), использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

На момент сохранения пользовательского правила TAA (IOA) в программе может не быть событий, содержащих данные для этих полей. Когда события с этими данными появятся, пользовательское правило TAA (IOA), созданное ранее, не сможет разметить события по этим полям.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила TAA (IOA) на основе условий поиска событий недоступна.

Информация о событиях

Если вы используете режим распределенного решения и мультитенантности, при работе в веб-интерфейсе программы вы можете просматривать информацию о событиях в рамках тех тенантов, к данным которых у вас есть доступ.

В информации о событиях отображаются локальные метки времени того компьютера с программой Kaspersky Endpoint Agent, на котором было обнаружено событие. Администратору программы требуется контролировать актуальность времени на компьютерах с программой Kaspersky Endpoint Agent.

Чтобы включить отображение событий по всем тенантам, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.
2. Включите переключатель **Искать по всем тенантам**.

   В таблице событий отобразятся события по всем тенантам.

Просмотр таблицы событий

Таблица событий отображается в разделе **Поиск угроз** окна веб-интерфейса программы после выполнения поиска угроз по базе событий. Вы можете сортировать события в таблице по столбцам **Время события**, **Тип события**, **Хост** и **Имя пользователя**.

Если вы используете режим распределенного решения и мультитенантности, события в таблице сгруппированы по хостам выбранных серверов и тенантов.

В таблице событий содержится следующая информация:

1. **Время события** – дата и время обнаружения события.
2. **Тип события** – например, **Запущен процесс**.
3. **Хост** – имя хоста, на котором было выполнено обнаружение.
4. **Сведения** – сведения о событии.
5. **Имя пользователя** – имя пользователя компьютера с программой Kaspersky Endpoint Agent, под учетной записью которого было обнаружено событие.

В таблице событий для каждого типа событий в столбце **Тип события** отображается свой набор данных в столбце **Сведения** (см. таблицу ниже).

Набор данных в столбце **Событие** для каждого типа событий в столбце **Сведения**

Тип события	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.
Заблокирован документ	Имя документа, запуск которого был заблокирован. SHA256- и MD5-хеш.
Изменен файл	Имя созданного файла. SHA256- и MD5-хеш.
Журнал событий ОС	Канал записи событий в системный журнал. 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.
Обнаружение	Обнаружение.
Результат обработки обнаружения	Результат обработки обнаружения.
AMSI-проверка	Результат AMSI-проверки.
Интерпретированный запуск файла	Интерпретированный запуск файла.
Интерактивный ввод команд в консоли	Интерактивный ввод команд в консоли.

Данные о событии **AMSI-проверка** доступны при интеграции Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent для Windows версии 3.10 и выше и при интеграции Kaspersky Endpoint Agent с программой Kaspersky Endpoint Security для Windows версий 11.5 и выше. Если программа Kaspersky Endpoint Security для Windows не установлена на компьютер и не интегрирована с программой Kaspersky Endpoint Agent, информация о событии **AMSI-проверка** не записывается в базу событий и не отображается в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Сервер Central Node формирует событие **Обнаружение** и **Результат обработки обнаружения** на основе данных, полученных от программ EPP. Если программы EPP не установлены на компьютер и не

интегрированы с программой Kaspersky Endpoint Agent, информация об этих событиях не записывается в базу событий и не отображается в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

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 значения в ячейке вы можете выполнить одно из следующих действий:

- Для всех значений в ячейке:
  - **Добавить в фильтр**.
  - **Исключить из фильтра**.
  - **Скопировать значение в буфер**.
- Имя хоста:
  - **Найти события**.
  - **Найти обнаружения**.
  - **Изолировать от сети**.
- Имя файла:
  - **Завершить процесс**.
  - **Завершить по уникальному PID**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Собрать форензику**.
  - **Поместить файл на карантин**.
- MD5-хеш:
  - **Найти события**.
  - **Найти обнаружения**.
  - **Найти на TIP**.
  - **Создать правило запрета**.
  - **Найти в Хранилище**.
- SHA256-хеш:
  - **Найти события**.
  - **Найти обнаружения**.

- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.

Настройка отображения таблицы событий

Вы можете настроить отображение столбцов, а также порядок их следования в таблице событий.

Чтобы настроить отображение таблицы событий:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.

5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.

6. Нажмите на кнопку **Применить**.

Отображение таблицы событий будет настроено.

Просмотр информации о событии

Чтобы просмотреть информацию о событии:

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 мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.

3. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

4. Выберите событие, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о событии.

Информация о событиях в дереве событий

Дерево событий отображается в верхней части окна информации о событии.

В дереве событий содержится следующая информация:

- Событие, информацию о котором вы просматриваете.

  Просматриваемое событие располагается справа.

- Родительский процесс.

  Родительский процесс располагается слева от просматриваемого события. Если для просматриваемого события нет родительского процесса, вместо него отображается имя хоста, на котором было зафиксировано просматриваемое событие.

При нажатии на имя родительского процесса слева отображается процесс, который инициировал появление этого процесса и является родительским по отношению к нему. Если родительского процесса нет, отображается имя хоста.

Справа от имени каждого родительского процесса отображается общее количество событий, вызванных этим процессом. Вы можете просмотреть список событий и информацию о выбранном событии.

Просмотр информации о родительском процессе в дереве событий

Чтобы просмотреть информацию о родительском процессе для просматриваемого события:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна отобразится дерево событий.

3. Нажмите на имя родительского процесса.

   В нижней части окна на закладке **Сведения** отобразится информация о процессе, который является родительским по отношению к просматриваемому событию.

Просмотр информации о событиях, инициированных родительским процессом, в дереве событий

Чтобы просмотреть таблицу всех событий, инициированных родительским процессом:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна информации о событии отобразится дерево событий.

3. Нажмите на имя родительского процесса в дереве событий.

   В нижней части окна на закладке **Сведения** отобразится информация о событии, которое является родительским по отношению к просматриваемому событию.

4. Перейдите на закладку **События**.

   Отобразится таблица всех событий, инициированных родительским процессом. По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.

   Вы можете просмотреть информацию о событии, нажав на строку с этим событием. Узел события отобразится в дереве событий.

Чтобы просмотреть таблицу событий, сгруппированных по типу, выполните следующие действия:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна информации о событии отобразится дерево событий.

3. Нажмите на раскрывающийся список справа от имени узла родительского процесса в дереве событий.

   Отобразится список всех событий, инициированных родительским процессом. По умолчанию события в списке сгруппированы по типу.

4. В дереве событий в раскрывающемся списка справа от имени родительского процесса выберите один из следующих элементов:

   - Если вы хотите просмотреть все события, инициированные родительским процессом, выберите **Все события**.

     Отобразится таблица всех событий, инициированных родительским процессом. По умолчанию события в таблице отсортированы по времени: новые события располагаются вверху таблицы.

   - Если вы хотите просмотреть все события одного типа, инициированные родительским процессом, выберите имя нужного типа событий.

     Отобразится таблица всех событий, инициированных родительским процессом и сгруппированных по типу.

   Вы можете просмотреть информацию о событии, нажав на строку с этим событием. Событие отобразится в дереве событий.

Просмотр информации о хосте в дереве событий

Если для просматриваемого события или родительского процесса нет процесса, инициировавшего его появление, вместо узла процесса в дереве событий отображается узел хоста, на котором было зафиксировано событие или был запущен родительский процесс.

Чтобы просмотреть информацию о хосте, на котором было зафиксировано событие или был запущен родительский процесс:

1. Выполните поиск событий в режиме конструктора или режиме исходного кода.

   Отобразится таблица событий.

2. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии. В верхней части окна отобразится дерево событий.

3. Нажмите на имя хоста в дереве событий.

   В нижней части окна отобразится информация о хосте, на котором было зафиксировано событие или был запущен родительский процесс.

Рекомендации по обработке событий

В окне события в рамке между деревом событий и текстовой информацией для пользователей с ролью **Старший сотрудник службы безопасности** отображаются рекомендации по обработке этого события.

Вы можете выполнить следующие рекомендации:

- **Изолировать <имя хоста>** – изолировать хост с программой Kaspersky Endpoint Agent, на котором обнаружено событие, от сети. Применяется для всех типов событий.
- **Создать правило запрета** – запретить запуск файла, обнаруженного в событии. Применяется для всех типов событий кроме **Журнал событий ОС** и **Изменено имя хоста**.
- **Создать задачу** – создать задачу. Применяется для всех типов событий кроме **Журнал событий ОС** и **Изменено имя хоста**.

Кроме того, вы можете выполнить действия по обработке события по ссылкам с именем файла, путем к файлу, MD5-хешем, SHA256-хешем файла и именем хоста при просмотре текстовой информации о событии в нижней части окна.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.

- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- Найти на TIP.
- Найти события.
- Найти обнаружения.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.

- Выполнить задачи:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Собрать форензику**.
  - **Поместить файл на карантин**.
  - **Выполнить программу**.
- **Скопировать значение в буфер**.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** рекомендации по обработке событий не отображаются.

Выполнение рекомендации по изоляции хоста

Чтобы выполнить рекомендацию по изоляции хоста от сети:

1. В рамке с рекомендациями выберите **Изолировать <имя хоста>**.

   Откроется окно параметров изоляции хоста из события, с которым вы работаете.

2. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.

3. В блоке параметров **Исключения для правила изоляции хоста** в списке **Направление трафика** выберите направление сетевого трафика, которое не должно быть заблокировано:
   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.

4. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

   Вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

5. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.

6. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**.

7. Нажмите на кнопку **Сохранить**.

Информация об изоляции хоста отобразится в разделе **Endpoint Agents** веб-интерфейса.

Вы также можете создать правило сетевой изоляции по ссылке **Изолировать <имя хоста>** в информации об обнаружении и в разделе **Endpoint Agents** веб-интерфейса.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изоляции хоста от сети недоступна.

Выполнение рекомендации по запрету запуска файла

Чтобы выполнить рекомендацию по запрету запуска файла:

1. В рамке с рекомендациями выберите **Создать правило запрета**.

   Откроется окно создания правила запрета с MD5- или SHA256-хешем файла из события, с которым вы работаете.

2. Задайте значения следующих параметров:

   a. **Состояние** – состояние правила запрета:

   - Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
   - Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.

   b. **Имя** – имя правила запрета.

   c. Если вы хотите, чтобы программа выводила уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

   d. Если вы хотите изменить область применения правила запрета, настройте параметр **Запрет для**:

   - Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.
   - Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

     Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
   - Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

3. Нажмите на кнопку **Добавить**.

Запрет на запуск файла будет создан.

Информация о созданном запрете отобразится в разделе **Политики** веб-интерфейса.

Если вы установили флажок **Показывать пользователю уведомление о блокировке запуска файла**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция запрета запуска файла недоступна.

Выполнение рекомендации по созданию задачи

Чтобы выполнить рекомендацию по созданию задачи:

1. В рамке с рекомендациями по ссылке **Создать задачу** раскройте список типов задач.
2. Выберите один из типов задач:
   - **Завершить процесс**.
   - **Собрать форензику**.
   - **Запустить YARA-проверку**.
   - **Управление службами**.
   - **Получить дамп памяти процесса**.
   - **Получить метафайлы NTFS**.
   - **Выполнить программу**.
   - **Получить файл**.
   - **Удалить файл**.
   - **Поместить файл на карантин**.
   - **Восстановить файл из карантина**.

   Откроется окно создания задачи с предзаполненными данными (например, именем хоста, путем к файлу, MD5- или SHA256-хешем файла) из события, с которым вы работаете.
3. Если вы хотите изменить предзаполненные данные из события, внесите изменения в соответствующие поля.
4. Если вы хотите добавить комментарий к задаче, введите его в поле **Описание**.

5. Если вы создаете задачу **Завершить процесс**, **Удалить файл**, **Запустить YARA-проверку** или **Управление службами** и хотите изменить область применения задачи, настройте параметр **Задача для**:

   - Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
   - Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

     Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
   - Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

6. Нажмите на кнопку **Добавить**.

Задача будет создана.

Информация о созданной задаче отобразится в разделе **Задачи** веб-интерфейса.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания задачи недоступна.

Информация о событии Запущен процесс

В окне с информацией о событиях типа **Запущен процесс** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Запущен процесс**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Параметры запуска** – параметры запуска процесса.
  - **MD5** – MD5-хеш файла процесса.
  - **SHA256** – SHA256-хеш файла процесса.
  - **Размер** – размер файла процесса.

- **Время события** – время запуска процесса.
- **Время создания** – время создания файла процесса.
- **Время изменения** – время последнего изменения файла процесса.

Если событие было записано в базу событий программой Kaspersky Endpoint Agent для Linux, в разделе **Запущен процесс** также отображается поле **Команда** – команда, с помощью которой был запущен процесс.

- Раздел **Сведения**:
  - **Название программы** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Недействительна" или "OK".
  - **Свойства** – атрибут файла по классификации Windows. Например, A (архив), D (директория) или S (системный).

  Если событие было записано в базу событий программой Kaspersky Endpoint Agent для Linux, в разделе **Сведения** также отображаются следующие поля:

  - **Свойства** – свойства файла процесса.
  - **Тип процесса** – например, exec.
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.
  - **Действующее имя пользователя** – имя пользователя, которое использовалось для входа в систему.
  - **Действующее имя группы** – группа, к которой принадлежит пользователь, чье имя использовалось для входа в систему.
  - **Имя пользователя-владельца** – имя пользователя, создавшего файл процесса.
  - **Имя группы-владельца** – название группы, пользователи которой могут изменить или удалить файл процесса.
  - **Разрешенные привилегии файла** – разрешения, которые могут использоваться для доступа к файлу процесса.

- **Наследуемые привилегии файла** – разрешения, которые есть у группы пользователей для выполнения операций с родительским каталогом файла процесса.
- **Актуальные привилегии файла** – разрешения, которые актуальны для файла процесса на данный момент.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

    Если событие было записано в базу событий программой Kaspersky Endpoint Agent для Linux, в разделе **Родительский процесс** также отображается поле **Команда** – команда, с помощью которой был запущен родительский процесс.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен процесс.
  - **IP хоста** – IP-адрес хоста, на котором был запущен процесс.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

  - **Тип учетной записи** – тип учетной записи, под которой был запущен процесс. Например, администратор.
  - **Тип входа в систему** – например, с помощью запущенной службы.
  - **Имя пользователя** – имя пользователя, запустившего процесс.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

    Если событие было записано в базу событий программой Kaspersky Endpoint Agent для Linux, в разделе **Сведения о системе** также отображается поле **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.

- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий программой Kaspersky Endpoint Agent для Linux, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.
  - Поместить файл на карантин.
  - Выполнить программу.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий программой Kaspersky Endpoint Agent для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.

- Выполнить задачи:
  - **Получить файл**.
  - **Выполнить программу**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Завершен процесс

В окне с информацией о событиях типа **Завершен процесс** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.

- Раздел **Завершен процесс**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Параметры запуска** – параметры запуска процесса.
  - **MD5** – MD5-хеш файла процесса.
  - **SHA256** – SHA256-хеш файла процесса.
  - **Размер** – размер файла процесса.
  - **Время события** – время завершения процесса.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
  - **Параметры запуска** – параметры запуска родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен процесс.
  - **IP хоста** – IP-адрес хоста, на котором был запущен процесс.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Тип учетной записи** – тип учетной записи, под которой был завершен процесс. Например, администратор.
  - **Тип входа в систему** – например, с помощью запущенной службы.

- **Имя пользователя** – имя пользователя, запустившего процесс.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Загружен модуль

В окне с информацией о событиях типа **Загружен модуль** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Загружен модуль**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла загруженного модуля.
  - **MD5** – MD5-хеш файла загруженного модуля.
  - **SHA256** – SHA256-хеш файла загруженного модуля.
  - **Размер** – размер загруженного модуля.
  - **Время события** – время загрузки модуля.
- Раздел **Сведения**:
  - **Название программы** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, Example File.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись OK".
  - **Время создания** – время создания загруженного модуля.
  - **Время изменения** – дата последнего изменения загруженного модуля.
  - **Следующая по пути обхода DLL** – поле содержит путь к библиотеке DLL, которая могла быть загружена вместо существующей библиотеки.

Поле отображается при выполнении следующих условий:

- Источник загруженной библиотеки DLL не является доверенным.
- В папке по стандартному пути обхода есть одноименная библиотека с другим хешем.

Kaspersky Anti Targeted Attack Platform получает данные, необходимые для заполнения поля **Следующая по пути обхода DLL**, только при интеграции Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent для Windows версии 3.10. При интеграции программы с предыдущими версиями Kaspersky Endpoint Agent указанное поле не будет отображаться в информации о событии.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был загружен модуль.
  - **IP хоста** – IP-адрес хоста, на котором был загружен модуль.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

  - **Имя пользователя** – имя пользователя, загрузившего модуль.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.

    - Получить файл.
    - Собрать форензику.
    - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
    - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
    - Завершить процесс.
    - Удалить файл.
    - Поместить файл на карантин.
    - Выполнить программу.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.

- **Скопировать значение в буфер**.

Информация о событии Удаленное соединение

В окне с информацией о событиях типа **Удаленное соединение** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Удаленное соединение**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Направление соединения** – направление соединения (входящее или исходящее).
  - **Удаленный IP-адрес** – IP-адрес хоста, на который была произведена попытка удаленного соединения.
  - **Локальный IP-адрес** – IP-адрес локального компьютера, с которого была произведена попытка удаленного соединения.
  - **Время события** – время попытки удаленного соединения.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, с которого была произведена попытка удаленного соединения.
  - **IP хоста** – IP-адрес хоста, с которого была произведена попытка удаленного соединения.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, который пытался установить удаленное соединение.
- **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.
  - Поместить файл на карантин.
  - Выполнить программу.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- Найти в Хранилище.

- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Правило запрета

В окне с информацией о событиях, в которых сработали правила запрета – событиях типа **Правило запрета** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Правило запрета**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **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 события** – время срабатывания запрета запуска файла.

- Раздел **Сведения**:
  - **Название программы** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.
  - **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
  - **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись OK".
  - **Время создания** – время создания файла, запуск которого был запрещен.
  - **Время изменения** – дата последнего изменения файла, запуск которого был запрещен.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором сработал запрет запуска файла.
  - **IP хоста** – IP-адрес хоста, на котором сработал запрет запуска файла.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, под учетной записью которого был произведен запуск файла.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.

- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.
  - Поместить файл на карантин.
  - Выполнить программу.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.

- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Заблокирован документ

В окне с информацией о событиях типа **Заблокирован документ** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Заблокирован документ**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя заблокированного документа.
  - **MD5** – MD5-хеш заблокированного документа.
  - **SHA256** – SHA256-хеш заблокированного документа.
  - **Время события** – время блокирования 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.
- Раздел **Инициатор события**:
  - **Файл** – имя файла родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был заблокирован документ.
  - **IP хоста** – IP-адрес хоста, на котором был заблокирован документ.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, попытавшегося открыть документ.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.

- Поместить файл на карантин.
- Выполнить программу.

- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

Информация о событии Изменен файл

В окне с информацией о событиях типа **Изменен файл** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- В зависимости от типа операции, которая была проведена с файлом, в информации о событии отображается одно из следующих названий раздела:
  - **Создан файл**.
  - **Изменен файл**.
  - **Переименован файл**.
  - **Удален файл**.

- **Изменены атрибуты файла**.
- **Прочитан файл**.

В разделе отображается следующая информация:

- **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

  По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

  Поле отображается, если при создании события сработало правило TAA (IOA).

- **Файл** – имя созданного, удаленного или измененного файла.
- **MD5** – MD5-хеш созданного, удаленного или измененного файла.
- **SHA256** – SHA256-хеш созданного, удаленного или измененного файла.
- **Размер** – размер созданного, удаленного или измененного файла.
- **Время события** – время обнаружения события.
- **Время создания** – время создания файла.
- **Время изменения** – время последнего изменения файла.
- **Предыдущая версия** – имя предыдущей версии файла.

  > Поле **Предыдущая версия** отображается в информации о событии только для операции типа **Переименован файл**.

- **Удалить после перезагрузки** – статус файла, предназначенного к удалению.

  Если файл, к которому была применена операция "удалить", открыт в какой-либо программе или задействован в других процессах, он будет удален по завершении этих процессов после перезагрузки хоста. В этом случае в поле **Удалить после перезагрузки** отображается Да.

  Если файл, к которому была применена операция "удалить", был удален сразу, в поле **Удалить после перезагрузки** отображается Нет.

  > Поле **Удалить после перезагрузки** отображается в информации о событии только для операции типа **Удален файл**.

Если событие было записано в базу событий программой Kaspersky Endpoint Agent для Linux, в разделе также отображаются следующие поля:

- **Тип файла** – расширение созданного, удаленного или измененного файла.
- **Флаги открытия файла** – значение флагов открытия созданного, удаленного или измененного файла.
- **Имя пользователя-владельца** – имя пользователя, создавшего файл.
- **Имя группы-владельца** – название группы, пользователи которой могут изменить или удалить файл.

- **Разрешенные привилегии файла** – разрешения, которые могут использоваться для доступа к созданному, удаленному или измененному файлу.
- **Наследуемые привилегии файла** – разрешения, которые есть у группы пользователей для выполнения операций с родительским каталогом созданного, удаленного или измененного файла.
- **Актуальные привилегии файла** – разрешения, которые актуальны для созданного или измененного файла на данный момент.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.

  Если событие было записано в базу событий программой Kaspersky Endpoint Agent для Linux, в разделе **Инициатор события** также отображаются следующие поля:
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное ему при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.
  - **Действующее имя пользователя** – имя пользователя, которое было использовано для входа в систему.
  - **Действующее имя группы** – группа, к которой принадлежит пользователь, имя которого использовалось для входа в систему.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был создан файл.
  - **IP хоста** – IP-адрес хоста, на котором был создан файл.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, создавшего файл.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

  Если событие было записано в базу событий программой Kaspersky Endpoint Agent для Linux, в разделе **Сведения о системе** также отображается поле **Вход с удаленного хоста** – имя хоста, с которого был совершен удаленный вход в систему.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий программой Kaspersky Endpoint Agent для Linux, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.
  - Поместить файл на карантин.
  - Выполнить программу.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий программой Kaspersky Endpoint Agent для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Получить файл.
  - Выполнить программу.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

Информация о событии Журнал событий ОС

В окне с информацией о событиях типа **Журнал событий ОС** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.

- Раздел **Журнал событий ОС**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Время события** – время обнаружения события.
  - **ID события безопасности** – идентификатор типа события безопасности в журнале Windows.

  Если событие было записано в базу событий программой Kaspersky Endpoint Agent для Linux, в разделе **Журнал событий ОС** также отображаются следующие поля:
  - **Тип события** – тип события.
  - **Результат операции** – например, **Успешно** или **Сбой**.
- Раздел **Информация о событии**, содержащий данные из системного журнала. Состав данных зависит от типа события Windows.

  > Раздел **Информация о событии** не отображается в информации о событиях, записанных в базу событий программой Kaspersky Endpoint Agent для Linux.
- Раздел **Инициатор события**:
  - **Файл** – имя файла процесса.
  - **ID процесса** – идентификатор процесса.
  - **Команда** – команда, с помощью которой был запущен родительский процесс.
  - **Переменные окружения** – переменные окружения процесса.
  - **Настоящее имя пользователя** – имя пользователя, назначенное при регистрации в системе.
  - **Настоящее имя группы** – группа, к которой принадлежит пользователь.

  > Раздел **Инициатор события** не отображается в информации о событиях, записанных в базу событий программой Kaspersky Endpoint Agent для Windows.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором произошло событие.
  - **IP хоста** – IP-адрес хоста, на котором произошло событие.

    > Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, который запустил процесс, инициировавший запись в системный журнал.
- **Версия ОС** – версия операционной системы, используемой на хосте.

  В информации о событии, записанном в базу событий программой Kaspersky Endpoint Agent для Linux, также отображается поле **Вход с удаленного хоста** – имя компьютера, с которого был совершен удаленный вход в систему.

В информации о событии, записанном в базу событий программой Kaspersky Endpoint Agent для Linux, по ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачу Получить файл.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.
  - Поместить файл на карантин.
  - Выполнить программу.
- **Скопировать значение в буфер**.

В информации о событии, записанном в базу событий программой Kaspersky Endpoint Agent для Linux, по ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.

- Выполнить задачи:
  - **Получить файл**.
  - **Выполнить программу**.
- **Скопировать значение в буфер**.

Информация о событии Изменение в реестре

В окне с информацией о событиях типа **Изменение в реестре** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Изменение в реестре**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Путь к ключу** – путь к разделу реестра, в котором произошло изменение.
  - **Имя параметра** – например, RegistrySizeLimit.
  - **Значение параметра** – значение параметра реестра.
  - **Тип параметра** – например, REG_DWORD.
  - **Время события** – время внесения изменения в реестр.

    При изменении имени или параметра ключа реестра могут отображаться дополнительные поля с информацией о состоянии ключа реестра до его изменения:
    - поле **Предыдущий путь к ключу** отображается при изменении имени ключа реестра;
    - поле **Предыдущее значение параметра** отображается при изменении значения параметра реестра;
    - поле **Предыдущий тип параметра** отображается при изменении типа параметра реестра.

      Kaspersky Anti Targeted Attack Platform получает данные, необходимые для заполнения полей **Предыдущий путь к ключу**, **Предыдущее значение параметра**, **Предыдущий тип параметра**, только при интеграции Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent для Windows версии 3.10 и выше. При интеграции программы с предыдущими версиями Kaspersky Endpoint Agent указанные поля не будут отображаться в информации о событии.

- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - Найти обнаружения.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - Завершить процесс.
    - Завершить по уникальному PID.
    - Удалить файл.
    - Получить файл.
    - Собрать форензику.
    - Поместить файл на карантин.
  - **MD5** – MD5-хеш файла родительского процесса.

    По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - Найти обнаружения.
    - Найти на TIP.
    - Найти в Хранилище.
    - Создать правило запрета.

    Скопировать значение в буфер.
  - **SHA256** – SHA256-хеш файла родительского процесса.

    По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - Найти обнаружения.
    - Найти на TIP.
    - Найти в Хранилище.

- Создать правило запрета.
- **Скопировать значение в буфер**.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором было произведено изменение в реестре.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - Найти обнаружения.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
    - Завершить процесс.
    - Удалить файл.
    - Поместить файл на карантин.
    - Выполнить программу.
  - **IP хоста** – IP-адрес хоста, на котором было произведено изменение в реестре.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, совершившего изменение в реестре.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

Вы можете получать информацию о модификации выбранного ключа реестра, отредактировав или заменив конфигурационный файл Kaspersky Anti Targeted Attack Platform. Для редактирования и замены конфигурационного файла программы требуется обратиться в Службу технической поддержки.

Настоятельно не рекомендуется выполнять какие-либо операции с конфигурационным файлом Kaspersky Anti Targeted Attack Platform в режиме Technical Support Mode без консультации или указания сотрудников Службы технической поддержки.

Информация о событии Прослушан порт

В окне с информацией о событиях типа **Прослушан порт** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Прослушан порт**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Локальный порт** – порт, который был прослушан.
  - **Локальный IP-адрес** – IP-адрес сетевого интерфейса, порт которого был прослушан.
  - **Время события** – время прослушивания порта.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, порт которого был прослушан.
  - **IP хоста** – IP-адрес хоста, порт которого был прослушан.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, от имени которого было совершено прослушивание порта.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.
  - Поместить файл на карантин.
  - Выполнить программу.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Загружен драйвер

В окне с информацией о событиях типа **Загружен драйвер** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Загружен драйвер**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла загруженного драйвера.
  - **MD5** – MD5-хеш файла загруженного драйвера.
  - **SHA256** – SHA256-хеш файла загруженного драйвера.
  - **Размер** – размер загруженного драйвера.
  - **Время события** – время загрузки драйвера.
- Раздел **Сведения**:
  - **Название программы** – например, название операционной системы.
  - **Производитель** – например, производитель операционной системы.
  - **Описание файла** – например, Example File.
  - **Исходное имя файла** – например, ExampleFile.exe.

- **Получатель сертификата** – организация, выпустившая цифровой сертификат файла.
- **Результат проверки подписи** – например, "Подпись недействительна" или "Подпись OK".
- **Время создания** – время создания загруженного драйвера.
- **Время изменения** – время последнего изменения загруженного драйвера.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на который был загружен драйвер.
  - **IP хоста** – IP-адрес хоста, на который был загружен драйвер.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – имя пользователя, загрузившего драйвер.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.

- Выполнить задачи:
  - **Собрать данные** → **Файл**, **Форензика**, **Образ диска**, **Дамп памяти**.
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Поместить файл на карантин**.
  - **Выполнить программу**.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии Обнаружение

В окне с информацией о событии типа **Обнаружение** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.

- На закладке **Сведения** в разделе **Обнаружение**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Обнаружено** – имя обнаруженного объекта.

    По ссылке с именем объекта раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события**.
    - **Просмотреть на Kaspersky Threats**.
    - **Скопировать значение в буфер**.
  - **Последнее действие** – последнее действие над обнаруженным объектом.
  - **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.
  - **Тип объекта** – тип объекта (например, файл).
  - **Режим обнаружения** – режим проверки, в котором выполнено обнаружение.
  - **Время события** – дата и время события.
  - **ID записи** – идентификатор записи об обнаружении в базе.
  - **Версия баз** – версия баз, с помощью которых выполнено обнаружение.
  - **Содержание** – содержание скрипта, переданного на проверку.

    Вы можете скачать эти данные, нажав на кнопку **Сохранить в файл**.
- На закладке **Сведения** в разделе **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события**.
    - Найти обнаружения.
    - **Скопировать значение в буфер**.

Выполнить задачи:

- Завершить процесс.
- Завершить по уникальному PID.
- Удалить файл.
- Получить файл.
- Собрать форензику.
- Поместить файл на карантин.

- **ID процесса** – идентификатор родительского процесса.
- **Параметры запуска** – параметры запуска родительского процесса.
- **MD5** – MD5-хеш файла родительского процесса.
- **SHA256** – SHA256-хеш файла родительского процесса.

- На закладке **Сведения** в разделе **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - Найти обнаружения.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
    - Завершить процесс.
    - Удалить файл.
    - Поместить файл на карантин.
    - Выполнить программу.
  - **IP хоста** – IP-адрес хоста, на котором выполнено обнаружение.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
- **Версия ОС** – версия операционной системы, используемой на хосте.

- На закладке **История** в таблице:
  - **Тип** – тип события: **Обнаружение** или **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время обнаружения и результата обработки обнаружения.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

Информация о событии Результат обработки обнаружения

В окне с информацией о событии типа **Результат обработки обнаружения** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- На закладке **Сведения** в блоке параметров **Результат обработки обнаружения**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Обнаружено** – имя обнаруженного объекта.

    По ссылке с именем объекта раскрывается список, в котором вы можете выбрать одно из следующих действий:
    - **Найти события**.
    - **Просмотреть на Kaspersky Threats**.
    - **Скопировать значение в буфер**.
  - **Последнее действие** – последнее действие над обнаруженным объектом.
  - **MD5** – MD5-хеш файла, в котором обнаружен объект.
  - **SHA256** – SHA256-хеш файла, в котором обнаружен объект.
  - **Тип объекта** – тип объекта (например, файл).
  - **Имя объекта** – полное имя файла, в котором обнаружен объект.
  - **Режим обнаружения** – режим проверки, в котором выполнено обнаружение.
  - **Время события** – дата и время события.
  - **ID записи** – идентификатор записи об обнаружении в базе.
  - **Версия баз** – версия баз, с помощью которых выполнено обнаружение.
- На закладке **Сведения** в блоке параметров **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.

- **Параметры запуска** – параметры запуска родительского процесса.
- **MD5** – MD5-хеш файла родительского процесса.
- **SHA256** – SHA256-хеш файла родительского процесса.

- На закладке **Сведения** в блоке параметров **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.
  - **IP хоста** – IP-адрес хоста, на котором выполнено обнаружение.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – учетная запись пользователя, от имени которой было совершено действие над обнаруженным объектом.
  - **Версия ОС** – версия операционной системы, используемой на хосте.
- На закладке **История** в таблице:
  - **Тип** – тип события **Результат обработки обнаружения**.
  - **Описание** – описание события.
  - **Время** – дата и время результата обработки обнаружения.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.
  - Поместить файл на карантин.
  - Выполнить программу.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Найти на TIP.
- **Найти на virustotal.com**.
- Найти в Хранилище.
- Создать правило запрета.
- **Скопировать значение в буфер**.

Информация о событии Интерпретированный запуск файла

В окне с информацией о событиях типа **Интерпретированный запуск файла** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Интерпретированный запуск файла**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Файл** – имя файла.
  - **MD5** – MD5-хеш файла.
  - **SHA256** – SHA256-хеш файла.
  - **Размер** – размер файла.
  - **Время создания** – время создания файла.
  - **Время изменения** – время последнего изменения файла.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.
  - **MD5** – MD5-хеш файла родительского процесса.
  - **SHA256** – SHA256-хеш файла родительского процесса.
  - **ID процесса** – идентификатор родительского процесса.
- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором был запущен файл.
  - **IP хоста** – IP-адрес хоста, на котором был запущен файл.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – имя пользователя, под учетной записью которого был запущен файл.
- **Версия ОС** – версия операционной системы, используемой на хосте.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - Завершить процесс.
  - Завершить по уникальному PID.
  - Удалить файл.
  - Получить файл.
  - Собрать форензику.
  - Поместить файл на карантин.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- Выполнить задачи:
  - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
  - Завершить процесс.
  - Удалить файл.
  - Поместить файл на карантин.
  - Выполнить программу.
- **Скопировать значение в буфер**.

По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти в Хранилище**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Информация о событии AMSI-проверка

В окне с информацией о событии типа **AMSI-проверка** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- В разделе **AMSI-проверка**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Время события** – дата и время события.
  - **Тип содержимого** – тип скрипта.

В программе предусмотрено два типа скриптов:

- Если скрипт представлен в виде текста, в поле **Тип содержимого** отображается тип скрипта *Текст*.
- Если скрипт представлен в другой форме, в поле **Тип содержимого** отображается тип скрипта *Двоичный код*.

- **Содержание** – содержание скрипта, переданного на проверку.

  Вы можете скопировать эти данные, нажав на кнопку **Скопировать в буфер**, если данные представлены в виде текста, или скачать файл с данными, нажав на кнопку **Сохранить в файл**, если данные представлены в другой форме.

  > Поле **Содержание** отображается в информации о событии, если программа регистрирует признаки целевых атак.

- В разделе **Инициатор события**:

  - **Файл** – путь к файлу родительского процесса.

    По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти обнаружения**.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Завершить процесс**.
    - **Завершить по уникальному PID**.
    - **Удалить файл**.
    - **Получить файл**.
    - **Собрать форензику**.
    - **Поместить файл на карантин**.

  - **MD5** – MD5-хеш файла родительского процесса.

    По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - **Найти обнаружения**.
    - **Найти на TIP**.
    - **Найти в Хранилище**.

- Создать правило запрета.
- **Скопировать значение в буфер**.

- **SHA256** – SHA256-хеш файла родительского процесса.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - Найти обнаружения.
  - Найти на TIP.
  - Найти в Хранилище.
  - Создать правило запрета.
  - **Скопировать значение в буфер**.

- В разделе **Сведения о системе**:

  - **Имя хоста** – имя хоста, на котором выполнено обнаружение.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - Найти обнаружения.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
    - Завершить процесс.
    - Удалить файл.
    - Поместить файл на карантин.
    - Выполнить программу.

  - **IP хоста** – IP-адрес хоста, на котором выполнено обнаружение.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.

- **Имя пользователя** – учетная запись пользователя, от имени которой было совершено изменение в реестре.
- **Версия ОС** – версия операционной системы, используемой на хосте.

Информация о событии Интерактивный ввод команд в консоли

В окне с информацией о событиях типа **Интерактивный ввод команд в консоли** содержатся следующие сведения:

- Дерево событий.
- Рекомендации по обработке события.
- Раздел **Интерактивный ввод команд в консоли**:
  - **Теги IOA** – информация о результатах исследования файла с помощью технологии Targeted Attack Analyzer: название правила TAA (IOA), по которому было выполнено обнаружение.

    По ссылке открывается информация о правиле TAA (IOA). Если правило предоставлено специалистами "Лаборатории Касперского", то оно содержит сведения о сработавшей технике MITRE, а также рекомендации по реагированию на событие.

    Поле отображается, если при создании события сработало правило TAA (IOA).
  - **Тип ввода** – тип ввода команд, которые были переданы консольному приложению.

    В программе предусмотрено два типа ввода команд:
    - Если команды в консольном приложении были введены пользователем, в поле **Тип ввода** отображается тип ввода команд *Консоль*.
    - Если команды были переданы в консольное приложение из другого приложения через коммуникационный шлюз (пайп), в поле **Тип ввода** отображается тип ввода команд *Канал*.

    > Kaspersky Anti Targeted Attack Platform получает данные, необходимые для заполнения поля **Команда**, только при интеграции Kaspersky Anti Targeted Attack Platform с программой Kaspersky Endpoint Agent для Windows версии 3.10. При интеграции программы с предыдущими версиями программы Kaspersky Endpoint Agent указанное поле не будет отображаться в информации о событии.

    - **Текст команды** – текст, введенный в командную строку (например, CMD) на хосте с программой Kaspersky Endpoint Agent.

    Вы можете скопировать этот текст, нажав на кнопку **Скопировать в буфер**, расположенную в поле **Текст команды**.
  - **Время события** – время обнаружения события.
- Раздел **Инициатор события**:
  - **Файл** – путь к файлу родительского процесса.

По ссылкам с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- Найти обнаружения.
- **Скопировать значение в буфер**.

Выполнить задачи:

- Завершить процесс.
- Завершить по уникальному PID.
- Удалить файл.
- Получить файл.
- Собрать форензику.
- Поместить файл на карантин.

- **MD5** – MD5-хеш файла родительского процесса.

  По ссылке **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - Найти обнаружения.
  - Найти на TIP.
  - Найти в Хранилище.
  - Создать правило запрета.
  - **Скопировать значение в буфер**.

- **SHA256** – SHA256-хеш файла родительского процесса.

  По ссылке **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

  - **Найти события**.
  - Найти обнаружения.
  - Найти на TIP.
  - Найти в Хранилище.
  - Создать правило запрета.
  - **Скопировать значение в буфер**.

- Раздел **Сведения о системе**:
  - **Имя хоста** – имя хоста, на котором была введена команда.

    По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

    - **Найти события**.
    - Найти обнаружения.
    - **Скопировать значение в буфер**.

    Выполнить задачи:

    - **Собрать данные** → Файл, Форензика, Образ диска, Дамп памяти.
    - Завершить процесс.
    - Удалить файл.
    - Поместить файл на карантин.
    - Выполнить программу.
  - **IP хоста** – IP-адрес хоста, на котором была введена команда.

    Если вы используете динамические IP-адреса, в поле отображается IP-адрес, присвоенный хосту на момент создания события.

    Программа не поддерживает работу с IPv6. Если вы используете IPv6, IP-адрес хоста не отображается.
  - **Имя пользователя** – учетная запись пользователя, от имени которой была введена команда.
  - **Версия ОС** – версия операционной системы, используемой на хосте.

Работа с информацией о хостах с Kaspersky Endpoint Agent

Программа Kaspersky Endpoint Agent устанавливается на отдельные компьютеры (далее также "хосты"), входящие в IT-инфраструктуру организации. Программа осуществляет постоянное наблюдение за процессами, запущенными на этих хостах, открытыми сетевыми соединениями и изменяемыми файлами.

Пользователи с ролью **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности**, **Аудитор**, **Локальный администратор** и **Администратор** могут оценить регулярность получения данных с хостов, на которых установлена программа Kaspersky Endpoint Agent, на закладке **Endpoint Agents** окна веб-интерфейса программы в рамках тех тенантов, к данным которых у них есть доступ. Если вы используете режим распределенного решения и мультитенантности, то в веб-интерфейсе сервера PCN отображается список хостов с программой Kaspersky Endpoint Agent для PCN и всех подключенных SCN.

Пользователи с ролью **Локальный администратор** и **Администратор** могут настроить отображение регулярности получения данных с хостов, на которых установлена программа Kaspersky Endpoint Agent, в рамках тех тенантов, к данным которых у них есть доступ.

В случае возникновения подозрительной сетевой активности пользователь с ролью **Старший сотрудник службы безопасности** может изолировать от сети любой из хостов с программой Kaspersky Endpoint Agent в рамках тех тенантов, к данным которых у него есть доступ. При этом соединение между сервером с компонентом Central Node и хостом с программой Kaspersky Endpoint Agent не будет прервано.

Для оказания поддержки при неполадках в работе программы Kaspersky Endpoint Agent 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.

Специалисты Службы технической поддержки сообщат вам необходимую для выполнения перечисленных действий информацию (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав получаемых в отладочных целях данных. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных 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 настоящем руководстве, 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 хостов с Kaspersky Endpoint Agent на отдельном сервере Central Node

Таблица хостов с программой Kaspersky Endpoint Agent находится в разделе **Endpoint Agents** окна веб-интерфейса программы.

В таблице могут отображаться следующие данные:

- Количество хостов и показатели активности программы Kaspersky Endpoint Agent:
  - **Критическое бездействие** – количество хостов, от которых последние данные были получены очень давно.
  - **Предупреждение** – количество хостов, от которых последние данные были получены давно.
  - **Нормальная активность** – количество хостов, от которых последние данные были получены недавно.
- **Хост** – имя хоста с программой Kaspersky Endpoint Agent.

- **Серверы** – имя сервера, к которому подключен хост с программой Kaspersky Endpoint Agent.
- **IP** – IP-адрес хоста, на который установлена программа Kaspersky Endpoint Agent.
- **ОС** – версия операционной системы, установленной на компьютере с программой Kaspersky Endpoint Agent.
- **Версия** – версия установленной программы Kaspersky Endpoint Agent.
- **Активность** – показатель активности программы Kaspersky Endpoint Agent. Может принимать следующие значения:
  - **Нормальная активность** – хосты, от которых последние данные были получены недавно.
  - **Предупреждение** – хосты, от которых последние данные были получены давно.
  - **Критическое бездействие** – хосты, от которых последние данные были получены очень давно.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- Выполнить задачи:
  - Завершить процесс.
  - Удалить файл.
  - Завершить по уникальному PID.
  - Получить файл.
  - Собрать форензику
  - Поместить файл на карантин.
  - Выполнить программу.
- Новое правило запрета.
- Изолировать от сети.
- Найти события.
- Найти обнаружения.
- **Скопировать значение в буфер**.

Список доступных действий зависит от типа (для Windows или Linux), версии и показателя активности Kaspersky Endpoint Agent.

По ссылке с IP-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- Найти обнаружения.
- **Скопировать значение в буфер**.

По ссылке в любом другом столбце таблицы раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скопировать значение в буфер**.

Настройка отображения таблицы хостов с Kaspersky Endpoint Agent

Вы можете настроить отображение столбцов, а также порядок их следования в таблице хостов с Kaspersky Endpoint Agent.

Чтобы настроить отображение таблицы хостов с Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. В заголовочной части таблицы нажмите на кнопку .
3. Отобразится окно **Настройка таблицы**.
4. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.
6. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.

Нажмите на кнопку **Применить**.Отображение таблицы хостов с Kaspersky Endpoint Agent будет настроено.

Просмотр информации о хосте

Чтобы просмотреть информацию о хосте с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.
2. Выберите хост, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о хосте.

Окно содержит следующую информацию:

- Блок рекомендаций:
  - **Обнаружения** – ссылка, по которой открывается раздел **Обнаружения** с условием поиска, содержащим выбранный хост.
  - **События** – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный хост.
  - **События, по которым сработали правила запрета** – ссылка, по которой открывается раздел **Поиск угроз** с условием поиска, содержащим выбранный хост и тип события **Правило запрета**.

  > Ссылка **События, по которым сработали правила запрета** не отображается в информации о хостах с программой Kaspersky Endpoint Agent для Linux.

- На закладке **Сведения**, в разделе **Хост** отображается следующая информация:
  - **Имя** – имя хоста с программой Kaspersky Endpoint Agent.
  - **IP** – IP-адрес хоста, на который установлена программа Kaspersky Endpoint Agent.
  - **ОС** – версия операционной системы хоста, на который установлена программа Kaspersky Endpoint Agent.
- На закладке **Сведения**, в разделе **Endpoint Agent** отображается следующая информация:
  - **Версия** – версия установленной программы Kaspersky Endpoint Agent.
- **Активность** – показатель активности программы Kaspersky Endpoint Agent. Может иметь 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.
- **Сервер** – имя сервера SCN или PCN. Отображается только в режиме распределенного решения и мультитенантности.

- **Подключен к серверу** – имя сервера Central Node.
- **Последнее подключение** – время последнего соединения с сервером Central Node, SCN или PCN.
- **Лицензия** – например, "OK".
- На закладке **Правила запрета** вы можете просмотреть, запуск или открытие файлов с какими MD5- или SHA256-хешами были запрещены на хосте. Отображается следующая информация:
  - **Имя** – имя файла.
  - **Состояние** – состояние правила запрета.
  - **Хеш** – алгоритм хеширования.

  Закладка **Правила запрета** не отображается в информации о хостах с программой Kaspersky Endpoint Agent для Linux.
- На закладке **Задачи** вы можете просмотреть, какие задачи были запущены на хосте. Отображается следующая информация:
  - **Время создания** – дата и время создания задачи.
  - **Имя** – название задачи.
  - **Сведения** – полный путь к файлу или потоку данных, для которого создана задача.
  - **Состояние** – статус выполнения задачи.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Выполнить задачи:
  - **Завершить процесс**.
  - **Удалить файл**.
  - **Получить файл**.
  - **Собрать форензику**.
  - **Поместить файл на карантин**.
  - **Выполнить программу**.
- **Новое правило запрета**.
- **Изолировать от сети**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

Для хостов с программой Kaspersky Endpoint Agent для Linux в списке, который раскрывается по ссылке с именем хоста, отображаются только **Получить файл**, **Выполнить программу**, **Найти события** и **Найти обнаружения**.

По ссылке с IP-адресом раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти обнаружения.
- **Скопировать значение в буфер**.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по имени хоста

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по имени хоста:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Хост** откройте окно настройки фильтрации.
3. Если вы хотите, чтобы отобразились только изолированные хосты, установите флажок **Показывать только изолированные Endpoint Agents**.
4. В раскрывающемся списке выберите один из следующих операторов фильтрации:
   - **Содержит**.
   - **Не содержит**.
5. В поле ввода укажите один или несколько символов имени хоста.
6. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
7. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.
8. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent, изолированных от сети

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent, изолированные от сети:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Хост** откройте окно настройки фильтрации.

3. Установите флажок **Показывать только изолированные Endpoint Agents**.

4. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по именам серверов PCN и SCN

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по именам серверов PCN и SCN, к которым подключены эти хосты.

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по именам серверов PCN и SCN:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Серверы** откройте окно настройки фильтрации.

3. Установите флажки рядом с теми именами серверов, по которым вы хотите отфильтровать или найти хосты с программой Kaspersky Endpoint Agent.

4. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по IP-адресу компьютера

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по IP-адресу компьютера, на котором установлена программа:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **IP** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов IP-адреса компьютера. Вы можете ввести IP-адрес компьютера или маску подсети в формате IPv4 (например, `192.0.0.1` или `192.0.0.0/16`).

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по версии операционной системы на компьютере

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по версии операционной системы, установленной на компьютере с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **ОС** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов версии операционной системы.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по версии Kaspersky Endpoint Agent

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по версии программы Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Версия** откройте окно настройки фильтрации.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов версии программы Kaspersky Endpoint Agent.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Если вы хотите удалить условие фильтрации, нажмите на кнопку справа от поля.

7. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск хостов с Kaspersky Endpoint Agent по их активности

Чтобы отфильтровать или найти хосты с программой Kaspersky Endpoint Agent по их активности:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. По ссылке **Активность** откройте окно настройки фильтрации.

3. Установите флажки рядом с одним или несколькими показателями активности программы Kaspersky Endpoint Agent:

   - **Нормальная активность**, если вы хотите найти хосты, от которых последние данные были получены недавно.
   - **Предупреждение**, если вы хотите найти хосты, от которых последние данные были получены давно.
   - **Критическое бездействие**, если вы хотите найти хосты, от которых последние данные были получены очень давно.

4. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Быстрое создание фильтра хостов с Kaspersky Endpoint Agent

Чтобы быстро создать фильтр хостов с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выполните следующие действия по быстрому добавлению условий фильтрации в создаваемый фильтр:

   a. Наведите курсор мыши на ссылку с тем значением столбца таблицы, которое вы хотите добавить в качестве условия фильтрации.

   b. Нажмите на левую клавишу мыши.

   Откроется список действий над значением.

   c. В открывшемся списке выберите одно из следующих действий:

   - **Добавить в фильтр**, если вы хотите включить это значение в условие фильтрации.
   - **Исключить из фильтра**, если вы хотите исключить это значение из условия фильтрации.

3. Если вы хотите добавить несколько условий фильтрации в создаваемый фильтр, выполните действия по быстрому добавлению каждого из условий фильтрации в создаваемый фильтр.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Сброс фильтра хостов с Kaspersky Endpoint Agent

Чтобы сбросить фильтр хостов с программой Kaspersky Endpoint Agent по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

2. Нажмите на кнопку справа от того заголовка столбца таблицы, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только хосты, соответствующие заданным вами условиям.

Настройка показателей активности Kaspersky Endpoint Agent

Пользователи с ролью **Локальный администратор** и **Администратор** могут определить, какой период бездействия программы Kaspersky Endpoint Agent считать нормальной, низкой и очень низкой активностью, а также настроить показатели активности программы Kaspersky Endpoint Agent. Пользователям с ролью **Аудитор** доступен только просмотр параметров показателей активности программы Kaspersky Endpoint Agent. Пользователи с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** могут просмотреть показатели активности программы Kaspersky Endpoint Agent в столбце **Активность** таблицы хостов с Kaspersky Endpoint Agent в разделе **Endpoint Agents** окна веб-интерфейса программы.

Чтобы настроить показатели активности программы Kaspersky Endpoint Agent, выполните следующие действия:

1. Войдите в веб-интерфейс программы под учетной записью **Локальный администратор**, **Администратор** или **Старший сотрудник службы безопасности**.
2. В окне веб интерфейса программы выберите раздел **Параметры**, подраздел **Endpoint Agents**.
3. В полях под названием раздела введите количество дней бездействия хостов с программой Kaspersky Endpoint Agent, которое вы хотите отображать как **Предупреждение** и **Критическое бездействие**.
4. Нажмите на кнопку **Применить**.

Показатели активности программы Kaspersky Endpoint Agent будут настроены.

Поддерживаемые интерпретаторы и процессы

Программа Kaspersky Endpoint Agent 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 программой Kaspersky Endpoint Agent, представлена в таблице ниже.

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

Процесс	Расширения файлов
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 Kaspersky Endpoint Agent

В рамках действия по реагированию на угрозы пользователи с ролью **Старший сотрудник службы безопасности** могут на время расследования инцидента изолировать хосты, на которых обнаружены объекты, требующие вашего внимания.

Сетевая изоляция не является самостоятельным действием по реагированию на угрозу. Сотруднику службы безопасности требуется расследовать инцидент самостоятельно за период действия сетевой изоляции хоста. Вы можете настроить период действия сетевой изоляции хоста при создании правила сетевой изоляции.

Сетевая изоляция доступна для хостов с программой Kaspersky Endpoint Agent версии 3.8 и следующих версий.

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.

Если программа Kaspersky Endpoint Agent на хосте отключена, а также в течение некоторого времени после включения программы Kaspersky Endpoint Agent или после перезагрузки компьютера с программой Kaspersky Endpoint Agent, сетевая изоляция этого хоста может не действовать.

При применении сетевой изоляции действует ряд ограничений.

Создание правила сетевой изоляции

Чтобы создать правило сетевой изоляции:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выберите хост, для которого вы хотите включить или отключить правило сетевой изоляции.

   Откроется окно с информацией о хосте.

3. Нажмите на кнопку **Изолировать**.

4. В поле **Отключить изоляцию через** введите количество часов от 1 до 9999, в течение которых будет действовать сетевая изоляция хоста.

5. В блоке параметров **Исключения для правила изоляции хоста** в списке **Направление трафика** выберите направление сетевого трафика, которое не должно быть заблокировано:

   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.

6. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

   Вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

7. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.

8. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**.

9. Нажмите на кнопку **Сохранить**.

   Хост будет изолирован от сети.

Вы также можете создать правило сетевой изоляции по ссылке **Изолировать <имя хоста>** в информации о событии и в информации об обнаружении.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила сетевой изоляции недоступна.

Для хостов с программой Kaspersky Endpoint Agent для Linux функция сетевой изоляции не предусмотрена.

Добавление исключения из правила сетевой изоляции

Чтобы добавить исключение в ранее созданное правило сетевой изоляции:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Выберите хост, изолированный от сети, для которого вы хотите создать исключение из правила сетевой изоляции.

   Откроется окно с информацией о хосте.

3. По ссылке **Добавить в исключения** раскройте блок параметров **Исключения для правила изоляции хоста**.

4. Выберите направление сетевого трафика, которое не должно быть заблокировано:

   - **Входящее/Исходящее**.
   - **Входящее**.
   - **Исходящее**.

5. В поле **IP** введите IP-адрес, сетевой трафик которого не должен быть заблокирован.

6. Если вы выбрали **Входящее** или **Исходящее**, в поле **Порты** введите порты подключения.

7. Если вы хотите добавить более одного исключения, нажмите на кнопку **Добавить** и повторите действия по заполнению полей **Направление трафика**, **IP** и **Порты**. Нажмите на кнопку **Сохранить**.

Исключение из правила сетевой изоляции будет добавлено.

Вы можете использовать прокси-сервер для соединения Kaspersky Endpoint Agent для Windows с Kaspersky Anti Targeted Attack Platform. При добавлении этого прокси-сервера в исключения сетевые ресурсы, к которым открыт доступ через прокси-сервер, также добавляются в исключения. Если в исключения добавлены сетевые ресурсы, соединение с которыми происходит через прокси-сервер, но при этом исключение для самого прокси-сервера не настроено, исключение не будет работать.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания исключения из правила сетевой изоляции недоступна.

Удаление правила сетевой изоляции

Чтобы удалить правило сетевой изоляции:

1. В окне веб-интерфейса программы выберите раздел **Endpoint Agents**.

   Откроется таблица хостов.

2. Нажатием левой клавиши мыши по имени хоста, для которого вы хотите удалить правило сетевой изоляции, раскройте меню действий над этим хостом.

3. Выберите действие **Удалить правило изоляции хоста**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило сетевой изоляции хоста будет удалено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления правила сетевой изоляции недоступна.

Ограничения, действующие при сетевой изоляции

При применении сетевой изоляции действует ряд ограничений:

- При включении правила сетевой изоляции на хосте прерываются все текущие соединения, а также становится недоступно VPN-подключение.
- Если администратор программы заменяет сертификат сервера с компонентом Central Node при включенном правиле сетевой изоляции, то отключение правила становится недоступно.
- 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.

Автоматическая отправка файлов с хостов с Kaspersky Endpoint Agent на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского"

Если функция включена, программа может автоматически отправлять файлы с хостов с Kaspersky Endpoint Agent на проверку компоненту Sandbox в соответствии с правилами TAA (IOA) "Лаборатории Касперского". Отправка файлов на проверку осуществляется по следующему принципу:

1. Kaspersky Anti Targeted Attack Platform проверяет базу событий и отмечает события, соответствующие правилам TAA (IOA).
2. При наличии соответствующих условий в правилах TAA (IOA), Kaspersky Anti Targeted Attack Platform отправляет файлы на проверку компоненту Sandbox.

   Запросы на отправку файлов на проверку компоненту Sandbox не отображаются в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

3. По результатам проверки программа может записать обнаружения в базу обнаружений.

   Вы можете просмотреть созданные обнаружения, отфильтровав их по показателю **Сведения** – **Автоотправка в Sandbox**.

При включении автоматической отправки файлов на проверку компоненту Sandbox объем обрабатываемого компонентом трафика может значительно увеличиться. Если сервер с компонентом Sandbox не рассчитан на увеличение нагрузки, часть объектов из очереди запросов на обработку будет заменена запросами на обработку файлов, отправленных на проверку автоматически.

Чтобы избежать потери объектов из очереди запросов на обработку, вы можете выполнить следующие действия:

- Развернуть дополнительные серверы Sandbox.
- Отключить функцию автоматической отправки файлов на проверку компоненту Sandbox.
- Добавить в исключения правила TAA (IOA), по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox.

  Информация о правилах, по которым Kaspersky Anti Targeted Attack Platform наиболее часто отправляет файлы на проверку компоненту Sandbox, отображается на виджете **Отправлено в Sandbox по правилам TAA**. Вы можете добавить этот виджет на текущую схему расположения виджетов.

  > При добавлении правила в исключения прекращается также разметка событий и создание обнаружений по этому правилу.

Список файлов, которые могут быть отправлены автоматически на проверку компоненту Sandbox, приведен в таблице ниже.

Список файлов, которые могут быть отправлены автоматически на проверку компоненту Sandbox

Тип события	Тип файла
Запущен процесс	Файл запущенного процесса и файл родительского процесса.
Загружен модуль	Файл загруженного модуля и файл родительского процесса.
Удаленное соединение	Файл родительского процесса.
Правило запрета	Файл приложения, запуск которого был заблокирован, и файл родительского процесса.
Заблокирован документ	Файл документа, запуск которого был заблокирован, и файл родительского процесса.
Изменен файл	Созданный, удаленный или измененный файл и файл родительского процесса.
Журнал событий ОС	Файл процесса (только для Linux).
Изменение в реестре	Файл родительского процесса.
Прослушан порт	Файл родительского процесса.
Загружен драйвер	Файл загруженного драйвера.
Обнаружение	Обнаруженный файл и файл родительского процесса (если есть).
Результат обработки обнаружения	Обнаруженный файл и файл родительского процесса (если есть).
AMSI-проверка	Файл процесса.
Интерпретированный запуск файла	Файла, который был запущен, и файл родительского процесса.
Интерактивный ввод команд в консоли	Файл родительского процесса.

> Информация о файлах, отправленных на проверку компоненту Sandbox, не отображаются в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Включение и отключение автоматической отправки файлов с хостов с Kaspersky Endpoint Agent на проверку компоненту Sandbox

Чтобы включить или отключить автоматическую отправку файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского":

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Endpoint Agents**.
2. В блоке параметров **Автоматическая отправка файлов в Sandbox** выполните следующие действия:
   - Установите флажок **Отправлять файлы**,если хотите включить автоматическую отправку файлов.

     По умолчанию функция включена.
   - Снимите флажок **Отправлять файлы**, если хотите отключить автоматическую отправку файлов.

     Отключение функции не влияет на работу правил TAA (IOA): будет отключена только автоматическая отправка файлов.
3. Нажмите на кнопку **Применить**.

Автоматическая отправка файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского" будет включена или отключена.

В режиме распределенного решения и мультитенантности параметры автоматической отправки файлов на проверку компоненту Sandbox по правилам TAA (IOA) "Лаборатории Касперского", заданные на сервере PCN, распространяются на подключенные к этому серверу PCN серверы SCN. При необходимости вы можете включить или отключить автоматическую отправку файлов на каждом выбранном сервере SCN отдельно.

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.

В режиме распределенного решения и мультитенантности задачи **Завершить процесс**, **Собрать форензику**, **Получить ключ реестра**, **Запустить YARA-проверку**, **Управление службами**, **Выполнить программу**, **Удалить файл**, **Восстановить файл из карантина**, **Поместить файл на карантин** 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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Задачи **Получить файл**, **Получить дамп памяти процесса**, **Получить метафайлы NTFS**, **Получить образ диска**, **Получить дамп памяти** выполняются только на указанном хосте, независимо от режима работы с программой.

Максимальное время выполнение задачи составляет 24 часа. Если за это время задача не успела завершиться, ее выполнение останавливается.

Пользователи с ролью **Старший сотрудник службы безопасности** могут работать со всеми задачами в рамках тех тенантов, к данным которых у них есть доступ.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Пользователи с ролью **Аудитор** могут просматривать таблицу задач и информацию о выбранной задаче.

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).

Вы можете включить или отключить отображение задач, созданных вами с помощью переключателя **Только мои** в правом верхнем углу окна. По умолчанию отображение задач, созданных текущим пользователем, включено.

В таблице задач содержится следующая информация:

- **Время** – дата и время создания задачи.
- **Тип** – тип задачи в зависимости от режима работы программы и сервера, на котором была создана задача.

  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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. Действие этих задач распространяется только на хосты, подключенные к этому серверу SCN. Задачи относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Имя** – название задачи.

  Задача может иметь одно из следующих названий:

  - **Завершить процесс**.
  - **Собрать форензику**.
  - **Запустить YARA-проверку**.
  - **Управление службами**.
  - **Получить метафайлы NTFS**.

- **Получить ключ реестра**.
- **Получить дамп памяти процесса**.
- **Выполнить программу**.
- **Получить файл**.
- **Удалить файл**.
- **Поместить файл на карантин**.
- **Восстановить файл из карантина**.
- **Получить образ диска**.
- **Получить дамп памяти**.

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**.

- **Сведения** – полный путь к файлу или потоку данных, для которого создана задача, или путь к общему сетевому ресурсу.

  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**.

- **Серверы** – имя сервера с ролью PCN или SCN, на котором выполняется задача.

  Поле отображается, только если вы используете режим распределенного решения и мультитенантности.

- **Хосты** – имя хоста, на котором выполняется задача.

  Поле отображается, только если вы используете отдельный сервер Central Node.

- **Автор** – имя пользователя, создавшего задачу.

  > Если вы включили отображение задач, созданных только текущим пользователем, столбец не отображается.

- **Состояние** – статус выполнения задачи.

Задача может иметь один из следующих статусов:

- **Ожидает**.
- **В обработке**.
- **Завершено**.

Просмотр информации о задаче

Чтобы просмотреть информацию о задаче:

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.
- **Тип информации** – тип собранных данных.
- **Путь к ключу реестра** – путь к ключу реестра, который требуется получить.
- **ID процесса** – идентификатор процесса.
- **Маска файла** – маска файлов, которые включены в список данных.
- **Метафайлы** – метафайлы NTFS, которые требуется получить.
- **Том** – имя диска, с которого требуется получить метафайлы, образ диска или дамп памяти.
- **Путь к общему ресурсу** – путь к общему сетевому ресурсу.
- **Сохраненный файл** – ссылка на файл, полученный в результате выполнения задачи.
- **Максимальный уровень вложенности** – максимальный уровень вложенности папок, в которых программа ищет файлы.
- **Исключения** – папки, в которых запрещены поиск или проверка файлов.
- **Область проверки** – папки, в которых проводится проверка по правилам YARA.
- **Действие** – действие, которое было выполнено над службой.

В программе доступны следующие операции со службами:

- **Запустить**.
- **Остановить**.
- **Приостановить**.
- **Продолжить**.
- **Удалить**.
- **Изменить тип запуска**.

- **Максимальное время проверки** – максимальное время выполнения задачи, по истечении которого проверка завершается.
- **SHA256** – SHA256-хеш файла, который вы хотите получить.
- **Запущено от имени** – параметр запуска программы от имени локальной системы.
- **Автор** – имя пользователя, создавшего задачу.
- **Тенант** – название тенанта. Отображается, только когда вы используете режим распределенного решения и мультитенантности.
- **Время создания** – время создания задачи.
- **Время завершения** – время завершения задачи.
- **Отчет** – результат выполнения задачи на выбранных хостах.

Создание задачи получения файла

Вы можете получить файл с выбранных хостов Kaspersky Endpoint Agent для Windows. Для этого вам нужно создать задачу получения файла.

Размер файла, который требуется получить, не должен превышать 100 МБ. Если размер файла превышает 100 МБ, задача завершается ошибкой.

Чтобы создать задачу получения файла:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Файл**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите получить.

Если запрашиваемый файл связан с дополнительными потоками данных NTFS, в результате выполнения задачи вы получите все файлы потоков данных NTFS, с которыми связан запрашиваемый файл.

Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае вы получите только файлы указанного потока.

> При создании задачи программа не проверяет на корректность указанный путь к файлу, который вы хотите получить.

b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите получить. 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. **Хост** – имя или IP-адрес хоста.

Вы можете указать только один хост.

4. Нажмите на кнопку **Добавить**.

Будет создана задача получения файла. Задача запускается автоматически после создания.

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.

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

Вы также можете скачать полученный файл из окна с отчетом о выполнении задачи.

Чтобы скачать полученный файл из окна с отчетом о выполнении задачи:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

Откроется таблица задач.

2. Откройте задачу получения файла, который вы хотите скачать.

3. В разделе **Отчет** нажмите на имя или IP-адрес хоста.

Откроется окно с информацией о файле.

4. Нажмите на кнопку **Скачать**.

Файл будет сохранен на ваш локальный компьютер в папку загрузки браузера.

> Для пользователей с ролью **Аудитор** функция создания задачи получения файла недоступна.

> У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи сбора форензики

Вы можете получить списки файлов, процессов и точек автозапуска с выбранных хостов Kaspersky Endpoint Agent для Windows. Для этого нужно создать задачу сбора форензики.

Чтобы создать задачу сбора форензики:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Форензика**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Тип информации** – тип собираемых данных. Установите флажок напротив одного, нескольких или всех параметров:

   - **Список процессов**, если хотите получить список процессов, запущенных на хосте в момент выполнения задачи.

   - **Список точек автозапуска**, если хотите получить список точек автозапуска.

     В список точек автозапуска включаются данные о программах, добавленных в папку автозагрузки или зарегистрированных в разделах реестра Run, а также о программах, которые запускаются автоматически при загрузке хоста с Kaspersky Endpoint Agent и при входе пользователя в систему на указанных хостах.

     Список поддерживаемых точек автозапуска

     Kaspersky Endpoint Agent поддерживает сбор следующих точек автозапуска:

     - Logon.
     - Run.
     - Explorer.
     - Shell.
     - Office.
     - Internet Explorer®.
     - Tasks.
     - Services.
     - Drivers.
     - Telephony.
     - Cryptography.

- Debuggers.
- COM.
- Session Manager.
- Network.
- LSA.
- Applications.
- Codecs.
- Shellex.
- WMI.
- Unspecified.

- **Список файлов**, если хотите получить список файлов, хранящихся в выбранной папке или во всех папках хоста в момент выполнения задачи.

b. Если вы установили флажок **Список файлов**, в блоке параметров **Тип источника** выберите один из вариантов:

- **Все локальные диски**, если вы хотите, чтобы в список файлов были включены файлы, хранящиеся во всех папках локальных дисков на момент выполнения задачи.
- **Директория**, если вы хотите, чтобы в список файлов были включены файлы, хранящиеся в указанной папке и следующих по пути папках диска на момент выполнения задачи.

c. Если вы выбрали **Директория**, в поле **Начальная директория** укажите путь к папке, с которой начнется поиск файлов.

Вы можете использовать следующие префиксы:

- Системные переменные окружения.
- Пользовательские переменные окружения.

  При использовании пользовательских переменных окружения в список файлов будет включена информация о файлах в папках всех пользователей, определивших указанные переменные окружения. Если пользовательские переменные окружения переопределяет системные, в список файлов будет включена информация о файлах в папках по значению системных переменных окружения.

d. **Хосты** – IP-адрес или имя хоста, на который хотите назначить задачу.

Вы можете указать несколько хостов.

Задача получения сбора данных может быть назначена только на хосты с программой Kaspersky Endpoint Agent для Windows версии 3.10 и выше. Получение списка точек автозапуска доступно только на хостах с Kaspersky Endpoint Agent для Windows версии 3.12 и выше.

При необходимости вы можете указать следующие параметры поиска файлов в папках:

- **Маска файла** – маска файлов, которые должны быть включены в список файлов.
- **Альтернативные потоки данных** – флажок, включающий запись информации об альтернативных потоках данных в список файлов.

  Если запрашиваемый файл связан с дополнительными потоками данных NTFS, в результате выполнения задачи вы получите все файлы потоков данных NTFS, с которыми связан запрашиваемый файл.

  По умолчанию флажок установлен.
- **Максимальный уровень вложенности** – максимальный уровень вложенности папок, в которых программа будет искать файлы.
- **Исключения** – путь к папкам, в которых вы хотите запретить поиск информации о файлах.
- **Описание** – описание задачи.

4. Нажмите на кнопку **Добавить**.

Задача сбора форензики будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи программа помещает в Хранилище ZIP-архив, который содержит файл с выбранными данными. Если задача завершилась успешно, вы можете скачать архив на ваш локальный компьютер.

Для пользователей с ролью **Аудитор** функция создания задачи сбора форензики недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения ключа реестра

Вы можете получить ключ реестра с выбранных хостов Kaspersky Endpoint Agent для Windows. Для этого нужно создать задачу получения ключа реестра.

Чтобы создать задачу получения ключа реестра:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Ключ реестра**.

   Откроется окно создания задачи.
3. Задайте значения следующих параметров:

   a. **Путь к ключу реестра** – путь к ключу реестра, который вы хотите получить.

Вы можете указать путь к ключу реестра в одном из следующих форматов:

- Корневой относительный путь.

  Например, \REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

- Относительный путь с указанием полного имени раздела.

  Например, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

- Относительный путь с аббревиатурой вместо полного имени раздела.

  Например, HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

Если вы хотите получить данные из ветки HKEY_CURRENT_USER, вам требуется указать ветку HKEY_USERS и SID пользователя: HKEY_USERS\<SID пользователя>.

b. **Описание** – описание задачи. Поле не является обязательным.

c. **Хосты** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

Вы можете указать несколько хостов.

Задача получения ключа реестра может быть назначена только на хосты с программой Kaspersky Endpoint Agent для Windows версии 3.13 и выше.

4. Нажмите на кнопку **Добавить**.

Задача получения ключа реестра будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи программа помещает в Хранилище ZIP-архив, который содержит файл в формате .reg, содержащий список всех ключей реестра и их значений, расположенных по указанному при создании задачи пути. Вы можете скачать архив на ваш локальный компьютер.

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения метафайлов NTFS

Вы можете получить метафайлы NTFS с выбранных хостов Kaspersky Endpoint Agent для Windows. Для этого нужно создать задачу получения метафайлов NTFS.

Чтобы создать задачу получения метафайлов NTFS:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Метафайлы NTFS**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Метафайлы** – список метафайлов, которые вы можете получить с помощью задачи. Выберите требуемый метафайл, установив напротив него флажок.

      Вы можете выбрать несколько метафайлов.

   b. **Том** – имя диска, с которого вы хотите получить метафайлы.

      По умолчанию в поле указан системный диск. Вы можете указать путь к другому диску в формате `<буква диска>:`.

   c. **Описание** – описание задачи. Поле не является обязательным.

   d. **Хост** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

      Вы можете указать только один хост.

      Задача получения метафайлов NTFS может быть назначена только на хосты с программой Kaspersky Endpoint Agent для Windows версии 3.13 и выше.

4. Нажмите на кнопку **Добавить**.

   Задача получения метафайлов NTFS будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи программа помещает в Хранилище ZIP-архив, который содержит выбранные метафайлы. Вы можете скачать архив на ваш локальный компьютер.

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

Загрузка выбранных метафайлов может привести к заполнению Хранилища и ротации объектов в нем. Если размер метафайла превышает размер Хранилища, метафайл не загружается

Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна. У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения дампа памяти процесса

Вы можете получить дамп памяти процесса с выбранных хостов Kaspersky Endpoint Agent для Windows. Для этого нужно создать задачу получения дампа памяти процесса.

Чтобы создать задачу получения дампа памяти процесса:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Дамп памяти процесса**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **ID процесса** – идентификатор процесса, для которого вы хотите получить дамп памяти.

   b. **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, для которого вы хотите получить дамп памяти. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

   d. **Хост** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

      Вы можете указать только один хост

      > Задача получения дампа памяти процесса может быть назначена только на хосты с программой Kaspersky Endpoint Agent для Windows версии 3.13 и выше.

4. Нажмите на кнопку **Добавить**.

   Задача получения дампа памяти процесса будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи программа помещает в Хранилище ZIP-архив, который содержит файл с информацией о процессе и файл дампа памяти процесса. Вы можете скачать архив на ваш локальный компьютер.

Если при выполнении задачи произошел сбой, в файл архива записывается описание ошибки.

Если вы используете режим распределенного решения и мультитенантности, архив помещается в Хранилище того сервера Central Node, к которому подключен хост, указанный в поле **Хост**.

> Для пользователей с ролью **Аудитор** функция создания этой задачи недоступна.

> У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения образа диска

Вы можете получить образ диска с выбранного хоста Kaspersky Endpoint Agent для Windows. Для этого нужно создать задачу получения образа диска.

Файл, полученный в результате выполнения задачи, можно сохранить только в общем сетевом ресурсе.

Чтобы создать задачу получения образа диска:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Образ диска**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к общему ресурсу** – путь к общему сетевому ресурсу.

      Вам нужно указать путь в формате Universal Naming Convention (UNC): `\\server\share\path`.

      Если последняя в пути папка с указанным именем отсутствует, Kaspersky Endpoint Agent создает ее. В случае неуспешного создания в веб-интерфейсе Kaspersky Anti Targeted Attack Platform отобразится ошибка.

   b. **Имя пользователя** – имя пользователя учетной записи для доступа к общему сетевому ресурсу.

   c. **Пароль** – пароль учетной записи для доступа к общему сетевому ресурсу.

   d. В блоке параметров **Тип диска** выберите один из вариантов:

      - **Логический**.
      - **Физический**.

   e. Если вы выбрали **Логический**, в поле **Том** введите букву диска без двоеточия и слеша или переменную `%SystemDrive%`.

   f. Если вы выбрали **Физический**, в поле **Физический диск** введите номер диска.

   g. Установите флажок **Разбить файл на части**, если вы хотите, чтобы при сохранении файл был разделен на несколько частей.

   h. Если вы установили флажок, в поле **Размер части, ГБ** укажите минимальный размер части сохраняемого файла.

      Минимальный размер части должен быть более одного гигабайта.

   i. **Описание** – описание задачи. Поле не является обязательным.

   j. **Хост** – IP-адрес или имя хоста, на который хотите назначить задачу.

4. Нажмите на кнопку **Добавить**.

Задача получения образа диска будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи программа помещает в общий сетевой ресурс архив, который содержит файл или файлы в формате EWF.

Вы можете назначить задачу только на хосты с Kaspersky Endpoint Agent для Windows версии 3.14 и выше.

Для пользователей с ролью **Аудитор** функция создания задач недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи получения дампа оперативной памяти

Вы можете получить дамп оперативной памяти с выбранного хоста Kaspersky Endpoint Agent для Windows. Для этого нужно создать задачу получения дампа памяти.

Файл, полученный в результате выполнения задачи, можно сохранить только в общем сетевом ресурсе.

Чтобы создать задачу получения дампа памяти:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке **Собрать данные** выберите **Дамп памяти**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к общему ресурсу** – путь к общему сетевому ресурсу.

      Вам нужно указать путь в формате Universal Naming Convention (UNC): `\\server\share\path`.

      Если последняя в пути папка с указанным именем отсутствует, Kaspersky Endpoint Agent создает ее. В случае неуспешного создания в веб-интерфейсе Kaspersky Anti Targeted Attack Platform отобразится ошибка.

   b. **Имя пользователя** – имя пользователя учетной записи для доступа к общему сетевому ресурсу.

   c. **Пароль** – пароль учетной записи для доступа к общему сетевому ресурсу.

   d. **Описание** – описание задачи. Поле не является обязательным.

   e. **Хост** – IP-адрес или имя хоста, на который хотите назначить задачу.

4. Нажмите на кнопку **Добавить**.

Задача получения дампа оперативной памяти будет создана. Задача запускается автоматически после создания.

В результате выполнения задачи приложение помещает в общий сетевой ресурс файл в формате RAW или архив, который содержит файл в формате RAW.

Вы можете назначить задачу только на хосты с Kaspersky Endpoint Agent для Windows версии 3.14 и выше.

Для пользователей с ролью **Аудитор** функция создания задач недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

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:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Завершить процесс**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу процесса, который вы хотите завершить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будут завершены только процессы указанного потока данных. Процессы остальных потоков этого файла будут выполняться.

   b. **MD5/SHA256** – MD5-, SHA256-хеш файла процесса, который вы хотите завершить. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

d. **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 мультитенантности.
- 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. Задача запускается автоматически после создания.

Для пользователей с ролью **Аудитор** функция создания задачи завершения процесса недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи проверки хостов с помощью правил YARA

Вы можете проверять хосты с Kaspersky Endpoint Agent для Windows с помощью правил YARA. Для этого требуется создать задачу **Запустить YARA-проверку**. Вы можете создать задачу следующими способами:

- В разделе **Задачи**.

  В этом случае при создании задачи вам потребуется выбрать правила YARA, с помощью которых вы хотите проверить хосты.
- В разделе **Пользовательские правила**, подразделе **YARA**.

  В этом случае создается задача для проверки хостов по выбранным правилам YARA.

*Чтобы создать задачу проверки хостов с Kaspersky Endpoint Agent для Windows с помощью правил YARA в разделе **Задачи**:*

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Запустить YARA-проверку**.

   Откроется окно создания задачи.
3. Задайте значения следующих параметров:

   a. **Выбрать правила** – имя правила. Вы можете ввести название правила или несколько знаков из названия правила и выбрать правило в списке.

   Вы можете добавить несколько правил.

b. **Проверить** – область проверки. Выберите один из следующих вариантов:

- **ОЗУ**, если вы хотите проверить процессы, запущенные на момент выполнения задачи.

  Программа не проверяет процессы с низким уровнем приоритета.

- **Точки автозапуска**, если вы хотите проверить точки автозапуска, полученные в результате выполнения задачи **Собрать форензику**.

  Доступно только при интеграции с Kaspersky Endpoint Agent 3.13 и выше.

  Для проверки точек автозапуска вам требуется указать хосты, для которых ранее была выполнена задача **Собрать форензику**.

- **Указанные директории**, если вы хотите проверить файлы, хранящиеся в указанной папке и во всех вложенных папках на момент выполнения задачи.

- **Все локальные диски**, если вы хотите проверить файлы, хранящиеся во всех папках локальных дисков на момент выполнения задачи.

  Проверка всех локальных дисков может создать повышенную нагрузку на хост.

c. Если вы выбрали **ОЗУ**, при необходимости выполните следующие действия:

- В поле **Процессы** укажите короткие имена процессов или маску файлов, которые хотите проверить.

  Программа проверяет все запущенные на хосте процессы с одинаковыми именами.

  Если поле **Процессы** не заполнено, программа проверяет все процессы, запущенные на момент выполнения задачи, кроме процессов с PID ниже 10 и процессов, указанных в поле **Исключения**.

- В поле **Исключения** укажите полные имена процессов или маску файлов, которые хотите исключить из проверки.

  Если на хосте запущено несколько процессов с одинаковыми именами, программа исключит из проверки все эти процессы.

d. Если вы выбрали **Точки автозапуска**, в поле **Тип проверки** выберите тип проверки:

- **Быстрая**.

  В этом случае проверяются все точки автозапуска, кроме COM-объектов.

- **Полная**.

  В этом случае проверяются все точки автозапуска и связанные с ними файлы.

e. Если вы выбрали **Указанные директории**, выполните следующие действия:

- В поле **Указанные директории** укажите полный путь к папкам, имя или маску файлов, которые хотите проверить (например, C:\Users\User1\Documents* или C:\Program files*.exe).
- В поле **Исключения** укажите полный путь к папкам, имя или маску файлов, которые хотите исключить из проверки.

f. **Максимальное время проверки** – максимальное время проверки.

По истечении указанного времени проверка завершится, даже если хосты были проверены не по всем правилам. В отчете о выполнении задачи указываются результаты, актуальные на момент завершения проверки.

g. **Описание** – описание задачи. Поле необязательно для заполнения.

h. **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 мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

> Задача проверки хостов с Kaspersky Endpoint Agent по правилам YARA может быть назначена только на хосты с программой Kaspersky Endpoint Agent для Windows версии 3.12 и выше. При одновременном назначении задачи на хосты с Kaspersky Endpoint Agent 3.12 и более ранними версиями программы задача выполняется только на хостах с Kaspersky Endpoint Agent 3.12.

*Чтобы создать задачу проверки хостов с Kaspersky Endpoint Agent для Windows с помощью правил YARA в разделе **Пользовательские правила**, подразделе **YARA**:*

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.
2. Установите флажки слева от правил, с помощью которых вы хотите проверить хосты.

   В нижней части окна отобразится панель управления.
3. Нажмите на кнопку **Запустить YARA-проверку**.
4. Выполните шаг 3 инструкции, приведенной выше.

Создание задачи будет завершено. Задача запускается автоматически после создания.

Если по результатам проверки будут обнаружены угрозы, Kaspersky Anti Targeted Attack Platform создаст соответствующие обнаружения.

Для пользователей с ролью **Аудитор** создание задачи проверки хостов с Kaspersky Endpoint Agent для Windows по правилам YARA недоступно.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи управления службами

Вы можете удаленно запускать, останавливать, приостанавливать и продолжать работу службы, а также удалить службу или изменить ее тип запуска на выбранных хостах с Kaspersky Endpoint Agent для Windows. Для этого нужно создать задачу управления службами.

Чтобы создать задачу управления службами:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Управление службами**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Имя службы** – укажите имя службы.

   b. **MD5/SHA256** – MD5- или SHA256-хеш службы. Поле необязательно для заполнения.

      Если вы указали хеш службы, которая загружается из DLL, Kaspersky Anti Targeted Attack Platform сравнивает указанный хеш одновременно с хешем библиотеки службы DLL и хешем процесса svchost.

   c. **Действие** – выберите операцию, которую вы хотите произвести со службой.

      В программе доступны следующие операции со службами:

      - **Запустить**.
      - **Остановить**.
      - **Приостановить**.
      - **Продолжить**.
      - **Удалить**.
      - **Изменить тип запуска**.

      При удалении службы процессы, которые были запущены этой службой, продолжают работать до перезагрузки системы или завершении работы процесса.

d. Если вы выбрали **Изменить тип запуска**, в поле **Тип запуска** выберите тип запуска службы.

e. **Описание** – описание задачи. Поле необязательно для заполнения.

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 мультитенантности.
- Если вы хотите выполнить задачу на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

Вы можете назначить задачу только на хосты с Kaspersky Endpoint Agent для Windows версии 3.12 и выше. Хосты с Kaspersky Endpoint Agent для Windows более ранних версий, а также хосты с Kaspersky Endpoint Agent для Linux отображаются в списке хостов, но недоступны для выбора.

4. Нажмите на кнопку **Добавить**.

Задача управления службами будет создана. Задача запускается автоматически после создания.

Настоятельно не рекомендуется останавливать, приостанавливать, а также удалять или изменять тип запуска служб, влияющих на работоспособность хоста.

Список служб, с которыми не рекомендуется проводить операции

- AVP*.
- BFE.
- CertPropSvc.
- CoreMessagingRegistrar.
- CryptSvc.
- DcomLaunch.
- Dhcp.
- DispBrokerDesktopSvc.
- EventLog.
- EventSystem.
- LanmanServer.
- LanmanWorkstation.
- LSM.
- mpssvc.
- Netlogon.
- Netman.
- PlugPlay.
- PolicyAgent.
- Power.
- ProfSvc.
- RasMan.
- RpcEptMapper.
- RpcSs.
- SamSs.
- SCardSvr.
- SecurityHealthService.
- SessionEnv.
- Spooler.
- SstpSvc.
- TermService.
- UmRdpService.
- UserManager.
- UsoSvc.
- VaultSvc.
- W32Time.
- WebClient.
- Winmgmt.

- WlanSvc.
- wscsvc.

Для пользователей с ролью **Аудитор** создание задачи управления службами недоступно.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи выполнения программы

Вы можете создать 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:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Выполнить программу**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. В полях **Путь к файлу** и **Рабочий каталог** ниже введите значения одним из следующих способов:

   - В поле **Путь к файлу** введите полный путь к исполняемому файлу (например, `C:\Windows\System32\ipconfig.exe`). Поле **Рабочий каталог** оставьте пустым.

     При создании задачи программа не проверяет на корректность указанный путь к исполняемому файлу.

   - В поле **Путь к файлу** введите имя и расширение исполняемого файла (например, `ipconfig.exe`). В поле **Рабочий каталог** укажите рабочую директорию (например, `C:\Windows\System32\`).

   b. В поле **Аргументы** введите дополнительные параметры запуска файла или выполнения команды (например, аргумент `/all`).

   c. В поле **Описание** введите описание задачи. Поле не является обязательным.

d. Настройте параметр **Задача для** – область применения задачи:

- Если вы хотите выполнить задачу на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите выполнить задачу на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите выполнить задачу.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- 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. Задача запускается автоматически после создания.

Пример:
Чтобы выполнить команду `ipconfig /all` на хосте с IP-адресом `10.10.10.1`, выполните следующие действия::

1. В окне веб-интерфейса программы выберите раздел **Задачи**.
   Откроется таблица задач.
2. Нажмите на кнопку **Добавить** и выберите **Выполнить программу**.
   Откроется окно создания задачи.
3. Задайте значения следующих параметров:
   a. В полях **Путь к файлу** и **Рабочий каталог** ниже введите значения одним из следующих способов:
      - В поле **Путь к файлу** введите `C:\Windows\System32\ipconfig.exe`. Поле **Рабочий каталог** оставьте пустым.
      - В поле **Путь к файлу** введите `ipconfig.exe`. В поле **Рабочий каталог** введите `C:\Windows\System32\`.

   b. В поле **Аргументы** введите `/all`.

   c. В поле **Описание** введите описание задачи.

   d. Выберите область применения задачи **Выбранных хостов**.

   e. В поле **Хосты** введите несколько символов IP-адреса `10.10.10.1`, и когда этот IP-адрес появится в раскрывающемся списке результатов поиска ниже, выберите его.
4. Нажмите на кнопку **Добавить**.

Для пользователей с ролью **Аудитор** функция создания задачи запуска программы или выполнения команды недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи удаления файла

Чтобы создать задачу удаления файла:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Удалить файл**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите удалить.

      Вы также можете указать путь к альтернативному потоку данных этого файла. В этом случае будет удален только указанный поток данных. Остальные потоки данных этого файла останутся без изменений.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите удалить. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

d. **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 мультитенантности.
- 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. Задача запускается автоматически после создания.

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.

Для пользователей с ролью **Аудитор** создание задачи удаления файла недоступно.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание задачи помещения файла на карантин

Если вы считаете, что на компьютере с программой Kaspersky Endpoint Agent находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив на карантин. Файл будет удален из папки компьютера, в которой он находится, и перемещен на карантин Kaspersky Endpoint Agent в директорию карантина на этом компьютере, указанную при настройке Kaspersky Endpoint Agent.

Чтобы создать задачу помещения файла на карантин:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Поместить файл на карантин**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Путь к файлу** – путь к файлу, который вы хотите поместить на карантин.

   b. **MD5/SHA256** – MD5- или SHA256-хеш файла, который вы хотите поместить на карантин. Поле не является обязательным.

   c. **Описание** – описание задачи. Поле не является обязательным.

   d. **Хосты** – имя или IP-адрес хоста, на который вы хотите назначить задачу.

      Вы можете указать несколько хостов.

   e. Нажмите на кнопку **Добавить**.

Будет создана задача помещения файла на карантин. Задача запускается автоматически после создания.

В результате выполнения задачи:

- Файл будет удален из папки компьютера с программой Kaspersky Endpoint Agent, в которой он находился, и перемещен на карантин Kaspersky Endpoint Agent в директорию карантина на этом компьютере, указанную при настройке Kaspersky Endpoint Agent.
- В списке задач раздела **Задачи** веб-интерфейса программы появится информация о выполнении этой задачи.
- В списке файлов раздела **Хранилище** подраздела **Карантин** появится информация о помещении файла на карантин.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки хоста. Рекомендуется проверить успешность выполнения задачи после перезагрузки хоста.

Задача помещения файла на карантин может завершиться с ошибкой **Доступ запрещен**, если вы пытаетесь поместить на карантин исполняемый файл и он запущен в настоящий момент.

Чтобы решить проблему, создайте задачу завершения процесса для этого файла, а затем повторите попытку создания задачи помещения файла на карантин.

Для пользователей с ролью **Аудитор** функция создания задачи помещения файла на карантин недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

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:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку **Добавить** и выберите **Восстановить файл из карантина**.

   Откроется окно создания задачи.

3. Задайте значения следующих параметров:

   a. **Описание** – описание задачи. Поле не является обязательным.

   b. **Поиск файлов** – имя файла, находящегося в карантине.

4. Нажмите на кнопку **Добавить**.

Будет создана задача восстановления файла из карантина. Задача запускается автоматически после создания.

После восстановления файла из карантина на хост метаданные о файле останутся в таблице объектов, помещенных в Хранилище.

Для пользователей с ролью **Аудитор** функция создания задачи восстановления файла из карантина недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Создание копии задачи

Чтобы скопировать задачу:

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. Если вы хотите изменить параметры задачи, внесите изменения для одного или нескольких параметров в зависимости от типа копируемой задачи.

5. Нажмите на кнопку **Добавить**.

Будет создана копия выбранной задачи.

Для пользователей с ролью **Аудитор** функция создания копии задачи недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Удаление задач

Если вы удалите задачу в процессе ее выполнения, результат выполнения задачи может не сохраниться.

Если вы удалите успешно выполненную задачу загрузки файла, файл будет удален.

Чтобы удалить задачу:

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.

Чтобы удалить все или несколько задач:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Установите флажки напротив задач, которые вы хотите удалить.

   Вы можете выбрать все задачи, установив флажок в строке с заголовками столбцов.

3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены.

Для пользователей с ролью **Аудитор** функция удаления задачи недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к задачам.

Фильтрация задач по времени создания

Чтобы отфильтровать задачи по времени их создания:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. По ссылке **Время** 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 мультитенантности, вы можете отфильтровать задачи по их типу.

Чтобы отфильтровать задачи по их типу:

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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
   - **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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

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:

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:

   - **Завершить процесс**.
   - **Выполнить программу**.
   - **Собрать форензику**.
   - **Запустить YARA-проверку**.

- **Управление службами**.
- **Получить файл**.
- **Удалить файл**.
- **Поместить файл на карантин**.
- **Восстановить файл**.
- **Получить образ диска**.
- **Получить дамп памяти**.

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:

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:

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 режим распределенного решения и мультитенантности, вы можете отфильтровать задачи по серверам, на которые распространяется действие задач.

Чтобы отфильтровать задачи по серверам, на которые распространяется действие задач:

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:

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:

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:

1. В окне веб-интерфейса программы выберите раздел **Задачи**.

   Откроется таблица задач.

2. Нажмите на кнопку справа от того заголовка столбца 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 Kaspersky Endpoint Agent. Программа идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Вы можете создавать, включать и отключать, удалять и изменять правила запрета. Кроме того, по ссылке с названием алгоритма хеширования в таблице правил запрета вы можете выполнять такие действия по поиску объектов, событий или обнаружений, по которым сработали правила запрета, как **Найти события**, **Найти обнаружения**, **Найти на TIP** или **Найти на virustotal.com**.

В режиме распределенного решения и мультитенантности 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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

- **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, редактировать, удалять, включать и отключать, а также импортировать правила запрета в рамках тех тенантов, к данным которых у них есть доступ.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к политикам.

Пользователи с ролью **Аудитор** могут просматривать таблицу правил запрета запуска файлов и процессов, а также информацию о выбранном правиле запрета без возможности редактирования.

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.

Правила запрета могут быть созданы автоматически на основе предустановленных политик (далее также "предустановок"), добавленных по умолчанию. При включенных предустановках программа создает правило запрета на основе обнаружения компонента Sandbox со средним или высоким уровнем важности. Созданное правило запрета блокирует запуск файла по его MD5-хешу. Пользователи с ролью **Старший сотрудник службы безопасности** могут включать и отключать предустановки.

Предустановки не поддерживаются в режиме распределенного решения и мультитенантности.

Для правил запрета, которые были созданы автоматически или импортированы, доступны такие же операции, что и для правил, созданных вручную.

На каждый хеш файла можно создать только одно правило запрета.

Максимальное поддерживаемое количество правил запрета в системе составляет 50 000.

Правила запрета действуют, только когда программа Kaspersky Endpoint Agent запущена на хосте. Если попытка запуска файла будет совершена до запуска программы Kaspersky Endpoint Agent или после завершения работы программы Kaspersky Endpoint Agent на хосте, то запуск файла не будет заблокирован.

Управление правилами запрета запуска файлов и процессов на выбранных хостах с помощью политик доступно при интеграции Kaspersky Endpoint Agent с сервером Central Node и осуществляется только через веб-интерфейс Kaspersky Anti Targeted Attack Platform.

Просмотр таблицы правил запрета

Таблица правил запрета находится в разделе **Политики** окна веб-интерфейса программы.

В таблице содержится следующая информация:

1. **Тип** – тип правила в зависимости от режима работы программы и роли сервера, на котором оно создано:

   - **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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

   - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

2. **Имя** – имя правила запрета.

3. **Серверы** – имена серверов с ролью PCN или SCN, на которые распространяется правило запрета.

   Поле отображается, только когда вы используете режим распределенного решения и мультитенантности.

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 TIP**.
   - **Найти на virustotal.com** (для SHA256).
   - **Найти события**.

     В результате выполнения этого действия откроется раздел **Поиск угроз** с событиями, уже отфильтрованными по выбранному вами хешу.

   - **Найти обнаружения**.

     В результате выполнения этого действия откроется раздел **Обнаружения** с обнаружениями, уже отфильтрованными по выбранному вами хешу.

   - **Включить правило запрета**.
   - **Отключить правило запрета**.
   - **Удалить правило запрета**.
   - **Скопировать значение в буфер**.

6. **Состояние** – текущее состояние правила запрета.

   Правило запрета может находиться в одном из следующих состояний:

   - **Включено**.
   - **Отключено**.

Настройка отображения таблицы правил запрета

Вы можете настроить отображение столбцов, а также порядок их следования в таблице правил запрета.

Чтобы настроить отображение таблицы правил запрета:

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.

5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.

6. Нажмите на кнопку **Применить**.

Отображение таблицы правил запрета будет настроено.

Просмотр правила запрета

Чтобы просмотреть правило запрета:

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.

По ссылке **MD5/SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

- **Имя** – имя правила запрета или файла, запрещенного к запуску.
- **Тип** – тип правила в зависимости от режима работы программы и роли сервера, на котором оно создано:
  - **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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. Действие этих правил запрета распространяется только на хосты, подключенные к этому серверу SCN. Правила запрета относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Уведомление** – состояние параметра **Показывать пользователю уведомление о блокировке запуска файла**.
- **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:

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку **Добавить**.
3. Выберите **Создать правило**.

   Откроется окно создания правила запрета.

4. Задайте значения следующих параметров:

   a. **Состояние** – состояние правила запрета:

   - Если вы хотите включить правило запрета, переведите переключатель в положение **Вкл**.
   - Если вы хотите отключить правило запрета, переведите переключатель в положение **Откл**.

b. **MD5/SHA256** – MD5- или SHA256-хеш файла или потока данных, запуск которого вы хотите запретить.

c. **Имя** – имя правила запрета.

d. Если вы хотите, чтобы программа выводила уведомление о срабатывании правила запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

> Если вы установили флажок **Показывать пользователю уведомление о блокировке запуска файла**, при попытке запуска запрещенного файла пользователю будет показано уведомление о том, что сработало правило запрета запуска этого файла.

e. **Запрет для** – область применения правила запрета:

- Если вы хотите применить правило запрета на всех хостах всех серверов, выберите вариант **Всех хостов**.
- Если вы хотите применить правило запрета на выбранных серверах, выберите вариант **Выбранных серверов** и справа от названия параметра **Серверы** установите флажки рядом с теми именами серверов, на которых вы хотите применить правило запрета.

  Этот вариант доступен только при включенном режиме распределенного решения и мультитенантности.
- Если вы хотите применить правило запрета на выбранных хостах, выберите вариант **Выбранных хостов** и перечислите эти хосты в поле **Хосты**.

> Для хостов с программой Kaspersky Endpoint Agent для Linux функция создания правила запрета не предусмотрена. Если при создании правила запрета в качестве области применения правила вы выберете хост с программой Kaspersky Endpoint Agent для Linux или все хосты, правило запрета не будет применено или будет применено только к хостам с программой Kaspersky Endpoint Agent для Windows.

5. Нажмите на кнопку **Добавить**.

Будет создан запрет на запуск файла.

Вы также можете импортировать правила запрета.

> Для пользователей с ролью **Аудитор** функция создания правила запрета на запуск файла недоступна.

> У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета.

Импорт правил запрета

Вы можете импортировать файл с MD5- и SHA256-хешами файлов, запуск которых хотите запретить. Для каждого хеша Kaspersky Anti Targeted Attack Platform создаст отдельное правило запрета.

Максимальный размер импортируемого файла - 10 МБ. На одной строке должен располагаться только один хеш.

Чтобы импортировать правила запрета:

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку **Добавить**.

3. Выберите **Импортировать правила**.

   Откроется окно импорта правил запрета.

4. Задайте значения следующих параметров:

   a. **Состояние** – состояние правила запрета:

   - Если вы хотите включить все импортированные правила запрета, переведите переключатель в положение **Вкл**.
   - Если вы хотите отключить все импортированные правила запрета, переведите переключатель в положение **Откл**.

   b. Если вы хотите, чтобы программа выводила уведомление о срабатывании правил запрета пользователю компьютера, на который распространяется запрет, установите флажок **Показывать пользователю уведомление о блокировке запуска файла**.

   Поле **Запрет для** недоступно для редактирования. По умолчанию правила запрета, созданные на сервере PCN, распространяются на все хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN (если вы используете режим распределенного решения и мультитенантности).

5. Загрузите файл с хешами файлов, для которых вы хотите создать правила запрета, с помощью кнопки **Обзор**.

   Откроется окно выбора файлов.

6. Выберите файл, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

7. Нажмите на кнопку **Добавить**.

Правила будут импортированы.

Для пользователей с ролью **Аудитор** функция импорта правил запрета на запуск файла недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета.

Включение и отключение правила запрета

Чтобы включить или отключить правило запрета:

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 столбце **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.

Для пользователей с ролью **Аудитор** функция включения и отключения правил запрета недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета запуска файлов и процессов на выбранных хостах с помощью политик.

Включение и отключение предустановок

Чтобы включить или отключить предустановки:

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Выберите закладку **Предустановки**.

3. В строке с предустановкой, которую вы хотите включить или отключить, в столбце **Состояние** переведите переключатель в положение **Включено** или **Отключено**.

Предустановка будет включена или отключена. При отключении предустановки все ранее автоматически созданные правила запрета сохранятся.

Удаление правил запрета

Вы можете удалить одно или несколько правил запрета, а также все правила запрета сразу.

Чтобы удалить одно правило запрета:

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.

Чтобы удалить все или несколько правил запрета:

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Установите флажки напротив правил запрета, которые вы хотите удалить.

   Вы можете выбрать все правила запрета, установив флажок в строке с заголовками столбцов.

3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные правила запрета будут удалены.

Для пользователей с ролью **Аудитор** функция удаления правил запрета недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к правилам запрета запуска файлов и процессов на выбранных хостах с помощью политик.

Фильтрация правил запрета по имени

Чтобы отфильтровать правила запрета по имени:

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. По ссылке **Имя** откройте меню фильтрации запретов.

3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов имени правила запрета.

5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.

6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по типу

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать правила запрета по их типу.

Чтобы отфильтровать правила запрета по типу:

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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
   - **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 тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по хешу файла

Чтобы отфильтровать правила запрета по хешу файла:

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. По ссылке **Хеш файла** откройте меню фильтрации правил запрета.
3. В раскрывающемся списке выберите один из следующих операторов фильтрации запретов:

   - **Содержит**.
   - **Не содержит**.

4. В поле ввода укажите один или несколько символов хеша файла.
5. Если вы хотите добавить условие фильтрации по другому критерию, нажмите на кнопку + и выполните действия по указанию условия фильтрации.
6. Нажмите на кнопку **Применить**.

В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация правил запрета по имени сервера

Если вы используете режим распределенного решения и мультитенантности, вы можете отфильтровать правила запрета по серверам, на которые распространяется действие правил запрета.

Чтобы отфильтровать правила запрета по имени сервера:

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:

1. В окне веб-интерфейса программы выберите раздел **Политики**.

   Откроется таблица правил запрета.

2. Нажмите на кнопку справа от того заголовка столбца таблицы правил запрета, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

   Выбранные фильтры будут сброшены.

   В таблице правил запрета отобразятся только правила запрета, соответствующие заданным вами условиям.

Работа с пользовательскими правилами

Вы можете настроить дополнительную защиту IT-инфраструктуры организации с помощью пользовательских правил **TAA**, **IDS**, **IOC** и **YARA**.

Пользователи с ролью **Старший сотрудник службы безопасности** могут работать с пользовательскими правилами **TAA**, **IDS**, **IOC** и **YARA**: загружать и удалять файлы правил, просматривать списки правил, редактировать выбранные правила.

Пользователи с ролью **Аудитор** могут просматривать списки пользовательских правил **TAA**, **IDS**, **IOC** и **YARA** и свойства выбранных правил без возможности редактирования.

Пользователи с ролью **Сотрудник службы безопасности** могут просматривать списки пользовательских правил **TAA**, **IOC** и **YARA** и свойства выбранных правил без возможности редактирования.

Об использовании индикаторов компрометации (IOC) и атаки (IOA) для поиска угроз

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 "правило TAA (IOA)"), содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Kaspersky Anti Targeted Attack Platform проверяет базу событий программы и отмечает события, которые совпадают с поведением, описанным в правилах TAA (IOA). При проверке используется технология *потоковой проверки*, при которой объекты, загружаемые из сети, проверяются непрерывно в режиме реального времени.

Правила TAA (IOA), сформированные специалистами "Лаборатории Касперского", используются в работе технологии TAA (Targeted Attack Analyzer) и обновляются вместе с базами программы. Они не отображаются в интерфейсе программы и не могут быть отредактированы.

Вы можете добавлять пользовательские правила IOC и TAA (IOA), используя IOC-файлы открытого стандарта описания OpenIOC, а также создавать правила TAA (IOA) на основе условий поиска по базе событий.

Сравнительные характеристики индикаторов компрометации (IOC) и атаки (IOA) приведены в таблице ниже.

Сравнительные характеристики индикаторов IOC и IOA

Сравнительная характеристика	Индикаторы IOC в пользовательских правилах IOC	Индикаторы IOA в пользовательских правилах TAA (IOA)	Индикаторы IOA в правилах TAA (IOA), сформированных специалистами "Лаборатории Касперского"
Область проверки	Компьютеры с программой Kaspersky Endpoint Agent	База событий программы	База событий программы
Механизм проверки	Периодическая проверка	Потоковая проверка	Потоковая проверка
Возможность добавить в исключения из проверки	Нет.	Не требуется. Пользователи с ролью **Старший сотрудник службы безопасности** могут изменить текст индикатора в пользовательских правилах TAA (IOA) согласно требуемым условиям.	Есть.

Если вы используете режим распределенного решения и мультитенантности, в разделе отображаются данные по выбранному вами тенанту.

Работа с пользовательскими правилами IOC

Вы можете использовать IOC-файлы для поиска индикаторов компрометации по базе событий и на компьютерах с установленной программой Kaspersky Endpoint Agent. Например, если вы получили из внешних источников информацию о распространении вредоносной программы, вы можете выполнить следующие действия:

1. Загрузить в веб-интерфейс Kaspersky Anti Targeted Attack Platform IOC-файл с индикаторами компрометации для вредоносной программы.

2. Найти события, соответствующие условиям выбранного IOC-файла.

   Вы можете просмотреть эти события и, если вы хотите, чтобы программа Kaspersky Anti Targeted Attack Platform формировала обнаружения по выбранным событиям, вы можете создать правило TAA (IOA).

3. Включить автоматическое использование выбранного IOC-файла для поиска индикаторов компрометации на компьютерах с программой Kaspersky Endpoint Agent.

   Если в результате проверки компьютеров программа Kaspersky Anti Targeted Attack Platform обнаружит индикаторы компрометации, программа Kaspersky Anti Targeted Attack Platform сформирует обнаружение.

4. Настроить расписание поиска индикаторов компрометации с помощью IOC-файлов на компьютерах с программой Kaspersky Endpoint Agent.

В режиме распределенного решения и мультитенантности IOC-файлы могут быть следующих типов:

- **Локальный** – IOC-файлы, загруженные на сервер SCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent, подключенных к этому серверу SCN.

- **Глобальный** – IOC-файлы, загруженные на сервер PCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent, подключенных к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN.

Вы можете ознакомиться со списком поддерживаемых индикаторов компрометации открытого стандарта OpenIOC, скачав файл.

Пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать, удалять, скачивать IOC-файлы на компьютер, включать и отключать поиск индикаторов компрометации по IOC-файлам, а также настраивать расписание поиска индикаторов компрометации на компьютерах с установленной программой Kaspersky Endpoint Agent.

Пользователи с ролью **Сотрудник службы безопасности** и **Аудитор** могут просматривать список IOC-файлов и информацию о выбранном файле, а также экспортировать IOC-файлы на компьютер.

Просмотр таблицы IOC-файлов

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Таблица IOC-файлов содержит информацию об IOC-файлах, используемых для проверки на компьютерах с программой Kaspersky Endpoint Agent, и находится в разделе **Пользовательские правила**, подразделе **IOC** окна веб-интерфейса программы.

В таблице IOC-файлов содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого IOC-файла.

   Степень важности может иметь одно из следующих значений:

   - – низкая важность.
   - – средняя важность.
   - – высокая важность.

2. **Тип** – тип IOC-файла в зависимости от режима работы программы и сервера, на который загружен IOC-файл:

   - **Локальный** – IOC-файлы, загруженные на сервер SCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent, подключенных к этому серверу SCN.
   - **Глобальный** – IOC-файлы, загруженные на сервер PCN. По этим IOC-файлам производится поиск индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent, подключенных к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN.

3. **Имя** – имя IOC-файла.

4. **Серверы** – имя сервера с компонентом Central Node.

5. **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с программой Kaspersky Endpoint Agent.

   Проверка хостов 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:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, информацию о котором вы хотите просмотреть.

Откроется окно с информацией об IOC-файле.

Окно содержит следующую информацию:

- **Найти обнаружения** – по ссылке открывается раздел **Обнаружения** с условием фильтрации, содержащим имя выбранного вами IOC-файла.
- **Найти события** – по ссылке открывается раздел **Поиск угроз** с условием поиска, содержащим индикаторы компрометации выбранного вами IOC-файла.
- **Скачать** – по ссылке открывается окно скачивания IOC-файла.
- **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с программой Kaspersky Endpoint Agent.
- **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 тенанта и имена серверов, к которым относятся события, проверяемые по этому IOC-файлу (в режиме распределенного решения и мультитенантности).
- **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:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файла на вашем локальном компьютере.

3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

4. Укажите следующие параметры:

   a. **Автоматическая проверка** – использование IOC-файла при автоматической проверке хостов с программой Kaspersky Endpoint Agent:

      - **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 тенанта и имена серверов, которые вы хотите проверять с помощью этого IOC-файла (в режиме распределенного решения и мультитенантности).

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:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

2. Откроется таблица IOC-файлов.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 хостов

Вы можете включить или отключить автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent.

Чтобы включить или отключить автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. В строке с IOC-файлом, использование которого вы хотите включить или отключить, в столбце **Состояние** переведите переключатель в одно из следующих положений:

   - **Включено**.
   - **Отключено**.

Автоматическое использование IOC-файла для поиска индикаторов компрометации на хостах с программой Kaspersky Endpoint Agent будет включено или отключено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция включения или отключения автоматического использования IOC-файла при проверке событий недоступна.

Удаление IOC-файла

Чтобы удалить IOC-файл:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.
2. Откроется таблица IOC-файлов.Выберите IOC-файл, который вы хотите удалить.

   Откроется окно с информацией об IOC-файле.

3. Нажмите на кнопку **Удалить**.

IOC-файл будет удален.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления IOC-файла недоступна.

Поиск обнаружений по результатам IOC-проверки

Чтобы найти и просмотреть результаты проверки по выбранному IOC-файлу:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, для которого вы хотите просмотреть результаты проверки.

   Откроется окно с информацией об IOC-файле.

3. Перейдите в базу обнаружений по ссылке **Найти обнаружения**.

   Откроется новая вкладка браузера с таблицей найденных обнаружений.

Вы также можете просмотреть результаты проверки по всем IOC-файлам, отфильтровав обнаружения по названию технологии.

Поиск событий по IOC-файлу

Чтобы просмотреть события, найденные с помощью IOC-файла:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.

   Откроется таблица IOC-файлов.

2. Выберите IOC-файл, который вы хотите использовать для поиска событий по базе событий.

   Откроется окно с информацией об IOC-файле.

3. Перейдите в базу событий по ссылке **Найти события**.

   Откроется новая вкладка браузера с таблицей найденных событий.

Фильтрация и поиск IOC-файлов

Чтобы отфильтровать или найти IOC-файлы по требуемым критериям:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.
2. Откроется таблица IOC-файлов.Выполните следующие действия в зависимости от критерия фильтрации:

- **По степени важности**

  a. По значку ▤ откройте окно настройки фильтрации IOC-файлов.

  b. Выберите одну или несколько из следующих степеней важности:

  - **Низкая**.
  - **Средняя**.
  - **Высокая**.

  c. Нажмите на кнопку **Применить**.

- **По имени файла**

  a. По ссылке **Имя** откройте окно настройки фильтрации IOC-файлов.

  b. Введите один или несколько символов имени IOC-файла.

  c. Нажмите на кнопку **Применить**.

- **По состоянию автоматической проверки (включена / выключена)**

  a. По ссылке **Автоматическая проверка** откройте окно настройки фильтрации IOC-файлов.

  b. Выберите один из следующих вариантов:

  - **Включено**.
  - **Отключено**.

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:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IOC**.
2. Откроется таблица IOC-файлов.Нажмите на кнопку справа от того заголовка столбца 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 поиска индикаторов компрометации с помощью IOC-файлов на хостах с программой Kaspersky Endpoint Agent.

Чтобы настроить расписание поиска индикаторов компрометации с помощью IOC-файлов на хостах с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Endpoint Agents**, раздел **Расписание IOC-проверки**.
2. В раскрывающихся списках **Время запуска** выберите время начала поиска индикаторов компрометации.
3. В раскрывающемся списке **Максимальное время проверки** выберите ограничение по времени выполнения поиска индикаторов компрометации.
4. Нажмите на кнопку **Применить**.

Новое расписание поиска индикаторов компрометации с помощью IOC-файлов на хостах с программой Kaspersky Endpoint Agent начнет действовать сразу после сохранения изменений. Результаты поиска индикаторов компрометации отобразятся в таблице обнаружений.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** недоступна функция настройки расписания поиска индикаторов компрометации с помощью IOC-файлов на хостах с программой Kaspersky Endpoint Agent.

Работа с пользовательскими правилами TAA (IOA)

Пользовательские правила TAA (IOA) создаются на основе условий поиска по базе событий. Например, если вы хотите, чтобы программа Kaspersky Anti Targeted Attack Platform сформировала обнаружения по событиям запуска программы, которую вы считаете небезопасной, на компьютерах с программой Kaspersky Endpoint Agent, вы можете выполнить следующие действия:

1. Сформировать поисковый запрос по базе событий.

2. Создать правило TAA (IOA) на основе условий поиска событий.

   При поступлении на сервер Central Node событий, соответствующих созданному правилу TAA (IOA), программа Kaspersky Anti Targeted Attack Platform сформирует обнаружения.

Вы также можете создать правило TAA (IOA) на основе одного или нескольких условий поиска событий из выбранного IOC-файла. Для этого вам требуется выполнить следующие действия:

1. Загрузить в веб-интерфейс Kaspersky Anti Targeted Attack Platform IOC-файл с индикаторами компрометации для вредоносной программы.

2. Найти события, соответствующие условиям выбранного IOC-файла.

3. Создать на основе одного или нескольких условий поиска событий из выбранного IOC-файла правило TAA (IOA).

В режиме распределенного решения и мультитенантности правила TAA (IOA) могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.

- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Различия между пользовательскими правилами и правилами "Лаборатории Касперского" представлены в таблице ниже.

Сравнительные характеристики правил TAA (IOA)

Сравнительная характеристика	Пользовательские правила TAA (IOA)	Правила TAA (IOA) "Лаборатории Касперского"
Наличие рекомендаций по реагированию на событие	Нет	Есть Вы можете посмотреть рекомендации в информации об обнаружении
Соответствие технике в базе MITRE ATT&CK	Нет	Есть Вы можете посмотреть описание техники по классификации MITRE в информации об обнаружении
Отображение в таблице правил TAA (IOA)	Да	Нет
Способ отключить проверку базы по этому правилу	Отключить правило	Добавить правило в исключения TAA

Сравнительная характеристика	Пользовательские правила ТАА (IOA)	Правила ТАА (IOA) "Лаборатории Касперского"
Возможность удалить или добавить правило	Вы можете удалить или добавить правило в веб-интерфейсе программы	Правила обновляются вместе с базами программы и не могут быть удалены пользователем
Поиск обнаружений и событий, в которых сработали правила ТАА (IOA)	По ссылкам **Обнаружения** и **События** в окне с информацией о правиле ТАА (IOA)	По ссылкам **Обнаружения** и **События** в окне с информацией об обнаружении

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, импортировать, удалять, включать и выключать правила ТАА (IOA), а также добавлять правила ТАА (IOA) "Лаборатории Касперского" в исключения из проверки. Пользователи с ролями **Сотрудник службы безопасности** и **Аудитор** могут использовать правила ТАА (IOA) для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и обнаружений, а также просматривать таблицу правил ТАА (IOA) и информацию о правилах ТАА (IOA).

Просмотр таблицы правил ТАА (IOA)

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

Таблица пользовательских правил ТАА (IOA) содержит информацию о правилах ТАА (IOA), используемых для проверки событий и создания обнаружений, и находится в разделе **Пользовательские правила**, подразделе **ТАА** окна веб-интерфейса программы.

В таблице содержится следующая информация:

1. – степень важности, которая будет присвоена обнаружению, произведенному с использованием этого правила ТАА (IOA).

   Степень важности может иметь одно из следующих значений:

   - – **Низкая**.
   - – **Средняя**.
   - – **Высокая**.

2. **Тип** – тип правила в зависимости от режима работы программы и роли сервера, на котором оно создано:

   - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.
   - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

3. **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:

   - **Высокая**.
   - **Средняя**.
   - **Низкая**.

Чем выше надежность, тем меньше вероятность ложных срабатываний

4. **Имя** – название правила.
5. **Серверы** – имя сервера с компонентом Central Node, на котором применяется правило.
6. **Обнаружения** – требование сохранять информацию об обнаружении на основе совпадения события из базы с критериями правила.
   - **Включено** – для события создается запись в таблице обнаружений с указанием технологии Targeted Attack Analyzer (TAA).
   - **Отключено** – не отображается в таблице обнаружений.
7. **Состояние** – состояние использования правила при проверке событий:
   - **Включено** – правило используется.
   - **Отключено** – правило не используется.

Создание правила TAA (IOA) на основе условий поиска событий

Чтобы создать правило TAA (IOA) на основе условий поиска событий:

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.
2. Выполните поиск событий в режиме конструктора или режиме исходного кода.
3. Нажмите на кнопку **Сохранить как правило TAA (IOA)**.

   Откроется окно **Новое правило TAA (IOA)**.
4. В поле **Имя** введите имя правила.
5. Нажмите на кнопку **Сохранить**.

Условие поиска событий будет сохранено. В таблице правил TAA (IOA) раздела **Пользовательские правила**, в подразделе **TAA** веб-интерфейса отобразится новое правило с заданным именем.

Не рекомендуется в условиях поиска событий, сохраняемых как пользовательское правило TAA (IOA), использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

На момент сохранения пользовательского правила TAA (IOA) в программе может не быть событий, содержащих данные для этих полей. Когда события с этими данными появятся, пользовательское правило TAA (IOA), созданное ранее, не сможет разметить события по этим полям.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания правила TAA (IOA) на основе условий поиска событий недоступна.

Импорт правила TAA (IOA)

Вы можете импортировать файл формата IOC и использовать его для проверки событий и создания обнаружений Targeted Attack Analyzer.

Настоятельно рекомендуется проверить работу пользовательских правил в тестовой среде перед импортом. Пользовательские правила TAA (IOA) могут вызвать проблемы производительности, в случае которых стабильная работа Kaspersky Anti Targeted Attack Platform не гарантируется

Чтобы импортировать правило TAA (IOA):

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файла на вашем локальном компьютере.

3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

   Откроется окно **Новое правило TAA (IOA)**.

4. Переместите переключатель **Состояние** в положение **Включено**, если вы хотите включить использование правила при проверке базы событий.

5. На закладке **Сведения** в поле **Имя** введите имя правила.

6. В поле **Описание** введите любую дополнительную информацию о правиле.

7. В раскрывающемся списке **Важность** выберите степень важности, которая будет присвоена обнаружению, выполненному по этому правилу TAA (IOA):

   - **Низкая**.
   - **Средняя**.
   - **Высокая**.

8. В раскрывающемся списке **Надежность** выберите уровень надежности этого правила, по вашей оценке:

   - **Низкая**.
   - **Средняя**.
   - **Высокая**.

9. В блоке параметров **Область применения** установите флажки напротив тех серверов, на которых вы хотите применить правило.

10. На закладке **Запрос** проверьте заданные условия поиска. Если требуется, внесите изменения.

11. Нажмите на кнопку **Сохранить**.

Пользовательское правило TAA (IOA) будет импортировано в программу.

Вы также можете добавить правило TAA (IOA), сохранив условия поиска по базе событий в разделе **Поиск угроз**.

Просмотр информации о правиле TAA (IOA)

Чтобы просмотреть информацию о правиле TAA (IOA):

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Обнаружения** – по ссылке в новой вкладке браузера откроется таблица обнаружений, отфильтрованных по технологии Targeted Attack Analyzer и имени правила TAA (IOA), с которым вы работаете.
- **События** – по ссылке в новой вкладке браузера откроется таблица событий, отфильтрованных по имени правила.
- **Запрос** – по ссылке в новой вкладке браузера откроется таблица событий, отфильтрованных по имени правила. В условиях поиска событий указаны данные из правила TAA (IOA), с которым вы работаете. Например, `EventType=Запущен процесс AND FileName CONTAINS <имя правила, с которым вы работаете>`. Вы можете отредактировать запрос на поиск событий.
- **IOA ID** – по ссылке открывается идентификатор, присваиваемый программой каждому правилу.

  Изменение идентификатора недоступно. Вы можете скопировать идентификатор по кнопке **Скопировать значение в буфер**.
- **Состояние** – использование правила при проверке базы событий.

На закладке **Сведения** отображается следующая информация:

- **Имя** – имя правила, которое вы указали при добавлении правила.
- **Описание** – любая дополнительная информация о правиле, которую вы указали.
- **Важность** – оценка возможного влияния события на безопасность компьютеров или локальной сети организации, указанная пользователем при добавлении правила.

- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний, заданный пользователем при добавлении правила.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **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 **Запрос** в верхней части окна вы можете перейти в раздел **Поиск угроз** и выполнить запрос на поиск событий.

Поиск обнаружений и событий, в которых сработали правила TAA (IOA)

Чтобы найти и просмотреть обнаружения и события, при создании которых сработало пользовательское правило TAA (IOA):

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, результат срабатывания которого вы хотите просмотреть.

   Откроется окно с информацией о правиле.

3. Выполните одно из следующих действий:

   - Если вы хотите просмотреть обнаружения, при создании которых сработало правило TAA (IOA), по ссылке **Обнаружения** перейдите в базу обнаружений.

     Откроется новая вкладка браузера с таблицей найденных обнаружений.

   - Если вы хотите просмотреть события, при создании которых сработало правило TAA (IOA), по ссылке **События** перейдите в базу событий.

     Откроется новая вкладка браузера с таблицей найденных событий.

Чтобы найти и просмотреть обнаружения и события, при создании которых сработало правило TAA (IOA) "Лаборатории Касперского", выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке слева выберите **Содержит**.

4. В раскрывающемся списке справа выберите технологию **(TAA) Targeted Attack Analyzer**.

5. Нажмите на кнопку **Применить**.

   В таблице отобразятся обнаружения, выполненные технологией TAA на основе правил TAA (IOA).

6. Выберите обнаружение, для которого в столбце **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об обнаружении.

7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.

8. Выполните одно из следующих действий:

   - Если вы хотите просмотреть обнаружения, при создании которых сработало правило TAA (IOA), по ссылке **Обнаружения** перейдите в базу обнаружений.

     Откроется новая вкладка браузера с таблицей найденных обнаружений.

   - Если вы хотите просмотреть события, при создании которых сработало правило TAA (IOA), по ссылке **События** перейдите в базу событий.

     Откроется новая вкладка браузера с таблицей найденных событий.

Фильтрация и поиск правил TAA (IOA)

Чтобы отфильтровать или найти правила TAA (IOA) по требуемым критериям:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выполните следующие действия в зависимости от критерия фильтрации:

   - **По степени важности**

     a. По значку ≣ откройте окно настройки фильтрации IOA-правил.

     b. Установите флажки напротив тех степеней важности, которые вы хотите включить в критерии фильтрации:

        - **Низкая**.
        - **Средняя**.
        - **Высокая**.

     c. Нажмите на кнопку **Применить**.

- **По типу правила**

  a. По ссылке **Тип** откройте окно настройки фильтрации.

  b. Выберите один из следующих элементов:

  - **Все** – все правила.
  - **Глобальный** – правила, созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.
  - **Локальный** – правила, созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

- **По уровню надежности**

  a. По ссылке **Надежность** откройте окно настройки фильтрации.

  b. Установите флажки напротив тех уровней надежности, которые вы хотите включить в критерии фильтрации:

  - **Низкая**.
  - **Средняя**.
  - **Высокая**.

  c. Нажмите на кнопку **Применить**.

- **По имени правила**

  a. По ссылке **Тег IOA** откройте окно настройки фильтрации.

  b. Введите один или несколько символов названия IOA-правила.

  c. Нажмите на кнопку **Применить**.

- По имени сервера

- **По созданию обнаружений на основе правила**

  a. По ссылке **Обнаружения** раскройте список настройки фильтрации.

  b. Выберите один из следующих вариантов:

  - **Все**.
  - **Включено**.
  - **Отключено**.

- **По состоянию правила**

  a. По ссылке **Состояние** раскройте список настройки фильтрации.

  b. Выберите один из следующих вариантов:

  - **Все**.
  - **Включено**.
  - **Отключено**.

В таблице отобразятся только правила, соответствующие заданным условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил TAA (IOA)

Чтобы сбросить фильтр правил TAA (IOA) по одному или нескольким условиям фильтрации, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Нажмите на кнопку справа от того заголовка столбца таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу каждого из условий фильтрации.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным условиям.

Включение и отключение использования правил TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут включить или отключить использование одного или нескольких правил, а также всех правил сразу.

Чтобы включить или отключить использование правила TAA (IOA) при проверке событий:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. В строке с нужным правилом в столбце **Состояние** включите или выключите переключатель.

Использование правила при проверке событий будет включено или отключено.

Чтобы включить или отключить использование всех или нескольких правил TAA (IOA) при проверке событий:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование всех правил.

Использование выбранных правил при проверке событий будет включено или отключено.

В режиме распределенного решения и мультитенантности на сервере PCN доступно управление только глобальными правилами TAA (IOA). Управление локальными правилами TAA (IOA) доступно на серверах SCN тех тенантов, к которым у вас есть доступ.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** включение и отключение правил TAA (IOA) недоступно.

Изменение правила TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут изменять пользовательские правила TAA (IOA). Изменение правил "Лаборатории Касперского" недоступно.

При работе в режиме распределенного решения и мультитенантности вы можете изменять только те правила TAA (IOA), которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно изменение только правил, созданных на PCN. В веб-интерфейсе SCN доступно изменение только правил, созданных на SCN.

Чтобы изменить правило TAA (IOA):

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, которое вы хотите изменить.

   Откроется окно с информацией об этом правиле.

3. Внесите необходимые изменения.

4. Нажмите на кнопку **Сохранить**.

Параметры правила будут изменены.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила TAA (IOA) на основе условий поиска событий недоступна.

Удаление правил TAA (IOA)

Пользователи с ролью **Старший сотрудник службы безопасности** могут удалить одно или несколько пользовательских правил TAA (IOA), а также все правила сразу.

При работе в режиме распределенного решения и мультитенантности вы можете удалять только те правила TAA (IOA), которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно удаление только правил, созданных на PCN. В веб-интерфейсе SCN доступно удаление только правил, созданных на SCN.

Чтобы удалить пользовательское правило TAA (IOA):

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией об этом правиле.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило будет удалено.

Чтобы удалить все или несколько пользовательских правил TAA (IOA):

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **TAA**.

   Откроется таблица правил TAA (IOA).

2. Установите флажки слева от правил, которые вы хотите удалить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Вы не можете удалять правила TAA (IOA) "Лаборатории Касперского". Если вы не хотите использовать при проверке правило TAA (IOA) "Лаборатории Касперского", вам требуется добавить его в исключения.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила TAA (IOA) на основе условий поиска событий недоступна.

Работа с пользовательскими правилами IDS

В режиме распределенного решения и мультитенантности пользовательские правила IDS могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка событий на этом сервере PCN и на всех серверах SCN, подключенных к этому серверу PCN. Проверяемые события относятся к тенантам, в рамках которых пользователь работает в веб-интерфейсе программы.
- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка событий на этом сервере SCN. Проверяемые события относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

Пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать, настраивать, заменять и удалять пользовательские правила IDS, а также добавлять правила IDS "Лаборатории Касперского" в исключения из проверки. Пользователи с ролями **Старший сотрудник службы безопасности** и **Аудитор** могут использовать правила IDS для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе обнаружений, а также просматривать информацию о правиле IDS.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к к пользовательским правилам IDS.

Импорт пользовательского правила IDS

Вы можете импортировать файл формата Snort® или Suricata и использовать его для проверки событий и создания обнаружений Intrision Detection System.

Настоятельно рекомендуется проверить работу пользовательских правил в тестовой среде перед импортом. Пользовательские правила IDS могут вызвать проблемы производительности, в случае которых стабильная работа Kaspersky Anti Targeted Attack Platform не гарантируется

Например, загрузка пользовательских правил может привести к следующим ошибкам:

- программа может создавать слишком много IDS-обнаружений;
- если программа не будет успевать записывать IDS-обнаружения, некоторые объекты сетевого трафика могут остаться непроверенными;
- регулярные выражения в составе пользовательских правил могут привести к ухудшению производительности или сбоям в работе программы;
- даже формально корректные пользовательские правила могут привести к ухудшению производительности или сбоям в работе программы.

При загрузке идентификаторы и атрибуты пользовательских правил могут быть изменены. Действия правил Reject и Drop будут заменены на Alert, правила с действием Pass будут удалены

Чтобы импортировать пользовательское правило IDS:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS. Нажмите на кнопку **Импортировать**.

   Откроется окно выбора файла на вашем локальном компьютере.
3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

Пользовательское правило IDS будет импортировано в программу.

Просмотр информации о пользовательском правиле IDS

Чтобы просмотреть информацию о пользовательском правиле IDS,

в окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IDS**.

В веб-интерфейсе отображается следующая информация о правиле IDS:

- **Состояние** – состояние использования правила при проверке событий.
- **Размер файла** – размер файла правила.
- **Последнее обновление** – время импорта правила.
- **Автор** – имя пользователя, под учетной записью которого было импортировано правило.
- **Важность** – степень важности, которая будет присвоена обнаружению, выполненному по этому правилу IDS.

Включение и отключение использования правила IDS при проверке событий

Чтобы включить или отключить использование правила IDS при проверке событий:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS.
3. Переведите переключатель **Состояние** в одно из следующих положений:
   - **Включено**.
   - **Отключено**.

Использование правила IDS при проверке событий будет включено или отключено.

Для пользователей с ролью **Аудитор** функция включения и отключения правил IDS недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к пользовательским правилам IDS.

Настройка важности обнаружений, выполненных по пользовательскому правилу IDS

Чтобы настроить степень важности, которая будет присвоена обнаружению, выполненному по правилу IDS:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS. В раскрывающемся списке **Важность** выберите степень важности, которая будет присвоена обнаружению, выполненному по этому правилу IDS:
   - **Низкая**.
   - **Средняя**.
   - **Высокая**.
3. При необходимости с помощью переключателя **Состояние** включите использование этого правила IDS.

Важность обнаружений, выполненных по этому правилу IDS, будет настроена.

Для пользователей с ролью **Аудитор** функция настройки правил IDS недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к к пользовательским правилам IDS.

Замена пользовательского правила IDS

Вы можете заменить ранее импортированный файл формата Snort или Suricata и использовать его для проверки событий и создания обнаружений Intrusion Detection System.

Настоятельно рекомендуется проверить работу пользовательских правил в тестовой среде перед импортом. Пользовательские правила IDS могут вызвать проблемы производительности, в случае которых стабильная работа Kaspersky Anti Targeted Attack Platform не гарантируется

При загрузке идентификаторы и атрибуты пользовательских правил могут быть изменены. Действия правил Reject и Drop будут заменены на Alert, правила с действием Pass будут удалены

Чтобы заменить пользовательское правило IDS:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS. Под информацией о правиле нажмите на кнопку **Заменить**.

   Откроется окно выбора файла на вашем локальном компьютере.
3. Выберите файл, который вы хотите загрузить и нажмите на кнопку **Открыть**.

Пользовательское правило IDS будет импортировано в программу и заменит ранее импортированное правило.

Для пользователей с ролью **Аудитор** функция замены пользовательского правила IDS недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к к пользовательским правилам IDS.

Скачивание файла пользовательского правила IDS на компьютер

Вы можете скачать ранее импортированный файл правила IDS на компьютер.

Чтобы скачать файл пользовательского правила IDS на компьютер:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS. Под информацией о правиле нажмите на кнопку **Скачать**.

Файл будет сохранен на ваш локальный компьютер в папку загрузки браузера.

Удаление пользовательского правила IDS

При работе в режиме распределенного решения пользователи с ролью **Старший сотрудник службы безопасности** могут удалять только то пользовательское правило IDS, которое было импортировано на текущий сервер. Это значит, что в веб-интерфейсе PCN доступно удаление только правила, созданного на PCN. В веб-интерфейсе SCN доступно удаление только правила, созданного на SCN.

Чтобы удалить пользовательское правило IDS:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **IDS**.
2. Откроется окно пользовательского правила IDS. Нажмите на кнопку **Удалить**.

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

Правило будет удалено.

Вы не можете удалять правила IDS "Лаборатории Касперского". Если вы не хотите использовать при проверке правило IDS "Лаборатории Касперского", вам требуется добавить его в исключения.

Для пользователей с ролью **Аудитор** функция удаления пользовательского правила IDS недоступна.

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к пользовательским правилам IDS.

Работа с пользовательскими правилами YARA

Вы можете использовать правила YARA в качестве баз модуля YARA для проверки файлов и объектов, поступающих на Central Node, и для проверки хостов с Kaspersky Endpoint Agent для Windows.

В режиме распределенного решения и мультитенантности пользовательские правила YARA могут быть одного из следующих типов:

- **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** могут импортировать файл правил YARA в Kaspersky Anti Targeted Attack Platform через веб-интерфейс программы.

Пользователи с ролями **Аудитор** и **Сотрудник службы безопасности** могут только просматривать правила YARA.

Просмотр таблицы правил YARA

Таблица пользовательских правил YARA содержит информацию о правилах YARA, используемых для проверки событий и создания обнаружений, и отображается в разделе **Пользовательские правила**, подразделе **YARA** окна веб-интерфейса программы.

В таблице содержится следующая информация:

- **Создано** – время создания правила.
- – 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".

  По умолчанию обнаружениям, выполненным по загруженным правилам YARA, присваивается высокая степень важности.
- **Тип** – тип правила в зависимости от режима работы программы и роли сервера, на котором оно было создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Имя** – название правила.
- **Файл** – название файла, из которого было импортировано правило.
- **Автор** – имя пользователя, под учетной записью которого было импортировано правило.
- **Серверы** – имя сервера с компонентом Central Node, на котором применяется правило.
- **Проверка трафика** – состояние использования правила при потоковой проверке файлов и объектов, поступающих на Central Node:
  - **Включено** – правило используется.
  - **Отключено** – правило не используется.

Импорт правил YARA

Чтобы импортировать правила YARA:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.
2. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.

3. Выберите файл правил YARA, который вы хотите загрузить, и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется, откроется окно **Импорт правил YARA**.

   > Максимальный допустимый размер загружаемого файла – 20 МБ.

   В нижней части окна отображается отчет. В отчете содержится следующая информация:

   - Количество правил, которые могут быть успешно импортированы.
   - Количество правил, которые не будут импортированы (если такие есть).

     Для каждого правила, которое не может быть импортировано, указывается его название.

4. Установите флажок **Проверка трафика**, если вы хотите использовать импортированные правила при потоковой проверке объектов и данных, поступающих на Central Node.

5. При необходимости в поле **Описание** введите любую дополнительную информацию.

   > Поле **Важность** недоступно для редактирования. По умолчанию обнаружениям, выполненным по загруженным правилам YARA, будет присвоена высокая степень важности.

6. В блоке параметров **Область применения** установите флажки напротив тех серверов, на которых вы хотите применить правила.

   Поле отображается только когда вы используете режим распределенного решения и мультитенантности.

7. Нажмите на кнопку **Сохранить**.

Импортированные правила отобразятся в таблице YARA-правил.

Настройка отображения таблицы правил YARA

Вы можете настроить отображение столбцов, а также порядок их следования в таблице.

Чтобы настроить отображение таблицы:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. В заголовочной части таблицы нажмите на кнопку .

   Отобразится окно **Настройка таблицы**.

3. Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.

   Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   > Должен быть установлен хотя бы один флажок.

4. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на строку с нужным параметром, нажмите на кнопку и переместите строку с параметром в нужное место.
5. Если вы хотите восстановить параметры отображения таблицы по умолчанию, нажмите на ссылку **По умолчанию**.
6. Нажмите на кнопку **Применить**.

Отображение таблицы будет настроено.

Просмотр информации о правиле YARA

Чтобы просмотреть информацию о правиле YARA:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.
2. Выберите правило, информацию о котором вы хотите просмотреть.

Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Обнаружения** – по ссылке в новой вкладке браузера откроется таблица обнаружений, отфильтрованных по технологии Targeted Attack Analyzer и имени правила TAA (IOA), с которым вы работаете.
- **Запустить YARA-проверку** – по ссылке открывается окно создания задачи.
- **Скачать** – по ссылке скачивается файл с правилами YARA.
- **Правило** – имя правила, указанное в файле.
- **Проверка трафика** – использование правила при потоковой проверке файлов и объектов, поступающих на Central Node.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Глобальный** – созданные на сервере PCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер PCN и все серверы SCN, подключенные к этому серверу PCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Локальный** – созданные на сервере SCN. По этим правилам производится проверка файлов и объектов, поступивших на сервер SCN. Проверяемые файлы и объекты относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
- **Важность** – степень важности, которая присваивается обнаружению, выполненному по этому правилу.

  По умолчанию обнаружениям, выполненным по загруженным правилам YARA, присваивается высокая степень важности.
- **Описание** – любая дополнительная информация о правиле, которую вы указали.
- **Область применения** – имена серверов с компонентом Central Node, на которых применяется правило.

Фильтрация и поиск правил YARA

Чтобы отфильтровать или найти правила YARA по требуемым критериям:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Выполните следующие действия в зависимости от критерия фильтрации:

   - **По времени создания**

     a. По ссылке **Создано** откройте окно настройки фильтрации.

     b. Выберите один из следующих вариантов:

     - **За все время**, если вы хотите, чтобы программа отображала в таблице правила, созданные за все время.
     - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице правила, созданные за предыдущий час.
     - **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице правила, созданные за предыдущий день.
     - **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице правила, созданные за указанный вами период.

   - **По имени правила**

     a. По ссылке **Правило** откройте меню фильтрации.

     b. В раскрывающемся списке выберите один из следующих операторов фильтрации:

     - **Содержит**.
     - **Не содержит**.

     c. В поле ввода введите название правила или несколько символов из названия правила.

     d. Нажмите на кнопку **Применить**.

   - **По имени файла**

     a. По ссылке **Файл** откройте меню фильтрации.

     b. В раскрывающемся списке выберите один из следующих операторов фильтрации:

     - **Содержит**.
     - **Не содержит**.

c. В поле ввода введите название файла или несколько символов из названия файла.

d. Нажмите на кнопку **Применить**.

- **По имени пользователя, загрузившего файл с правилами**

  a. По ссылке **Автор** откройте меню фильтрации.

  b. В раскрывающемся списке выберите один из следующих операторов фильтрации:

  - **Содержит**.
  - **Не содержит**.

  c. В поле ввода введите имя пользователя или несколько символов из имени пользователя.

  d. Нажмите на кнопку **Применить**.

- **По состоянию правила**

  a. По ссылке **Проверка трафика** раскройте список настройки фильтрации.

  b. Выберите один из следующих вариантов:

  - **Все**.
  - **Включено**.
  - **Отключено**.

В таблице отобразятся только правила, соответствующие заданным условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил YARA

Чтобы сбросить фильтрацию правил YARA по одному или нескольким условиям:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Нажмите на кнопку справа от того заголовка столбца таблицы правил, условия фильтрации по которому вы хотите сбросить.

   Если вы хотите сбросить несколько условий фильтрации, выполните действия по сбросу для каждого из условий.

Выбранные фильтры будут сброшены.

В таблице отобразятся только правила, соответствующие заданным условиям.

Включение и отключение использования правил YARA

Пользователи с ролью **Старший сотрудник службы безопасности** могут включить или отключить использование одного или нескольких правил, а также всех правил сразу.

При работе в режиме распределенного решения и мультитенантности вы можете включить или отключить использование правил YARA, которые были созданы на текущем сервере. Это значит, что в веб-интерфейсе PCN доступно включение и отключение использования только правил, созданных на сервере PCN. В веб-интерфейсе SCN доступно включение и отключение использования только правил, созданных на сервере SCN.

Если на серверах PCN и SCN включено использование правил YARA с одинаковыми именами, при проверке файлов и объектов, поступающих на SCN, применяется правило, созданное на PCN.

Чтобы включить или отключить использование правила YARA при потоковой проверке файлов и объектов, поступающих на Central Node:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. В строке с нужным правилом в столбце **Проверка трафика** включите или отключите переключатель.

   Использование правила при потоковой проверке файлов и объектов, поступающих на Central Node, будет включено или отключено.

Чтобы включить или отключить использование всех или нескольких правил YARA при потоковой проверке файлов и объектов, поступающих на Central Node:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

2. Установите флажки слева от правил, использование которых вы хотите включить или отключить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Включить** или **Отключить**, чтобы включить или отключить использование всех правил.

   Использование выбранных правил при потоковой проверке файлов и объектов, поступающих на Central Node, будет включено или отключено.

Удаление правил YARA

Чтобы удалить правило YARA:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Выберите правило, которое вы хотите удалить.

   Откроется окно с информацией об этом правиле.

3. Нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Правило будет удалено.

Чтобы удалить все или несколько правил YARA:

1. В окне веб-интерфейса программы выберите раздел **Пользовательские правила**, подраздел **YARA**.

   Откроется таблица правил YARA.

2. Установите флажки слева от правил, которые вы хотите удалить.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

   В нижней части окна отобразится панель управления.

3. Нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения действия нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления правила YARA недоступна.

Работа с объектами в Хранилище и на карантине

В Хранилище помещаются файлы, которые нужно отправить на проверку, а также файлы, полученные в результате выполнения задач **Получить файл**, **Восстановить файл из карантина**, **Собрать форензику**, **Получить метафайлы NTFS**, **Получить ключ реестра**, **Получить дамп памяти процесса**.

Хранилище расположено на сервере Central Node.

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.

Если вы используете режим распределенного решения и мультитенантности, Хранилище расположено на серверах PCN и SCN. В веб-интерфейсе сервера PCN отображается информация о Хранилище всех подключенных SCN в рамках тех тенантов, к данным которых у пользователя есть доступ.

Пользователь с ролью **Старший сотрудник службы безопасности** может поместить копии объектов в Хранилище с помощью задач или загрузив объект в Хранилище через веб-интерфейс Kaspersky Anti Targeted Attack Platform на том сервере PCN или SCN, с которым он работает в рамках тех тенантов, к данным которых у него есть доступ.

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 тенантов, к данным которых у него есть доступ.

Если вы считаете файл опасным, вы можете поместить его на карантин на компьютере с программой Kaspersky Endpoint Agent. Метаданные файла, помещенного на карантин, отобразятся в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса Kaspersky Anti Targeted Attack Platform.

Карантин на хостах с Kaspersky Endpoint Agent – это специальное локальное хранилище на компьютере для файлов, которые вы считаете небезопасными. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности компьютера.

При помещении файла на карантин на хосте с Kaspersky Endpoint Agent выполняется его перемещение, а не копирование: объект удаляется из той директории, в которой он был обнаружен и помещается в директорию карантина, указанную в параметрах Kaspersky Endpoint Agent.

Карантин на сервере Kaspersky Anti Targeted Attack Platform – это область Хранилища серверной части решения Kaspersky Anti Targeted Attack Platform, предназначенная для хранения метаданных объектов, помещенных на карантин на компьютерах с программой Kaspersky Endpoint Agent, в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса Kaspersky Anti Targeted Attack Platform.

Вы можете управлять объектами на карантине: восстанавливать объекты из карантина, а также загружать копии объектов, помещенных на карантин на компьютерах с программой Kaspersky Endpoint Agent, в Хранилище Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform отображает информацию об объектах, помещенных на карантин, в виде таблицы.

По умолчанию максимальный объем Хранилища 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.

Реальный размер объекта может быть больше видимого размера объекта из-за метаданных, необходимых для восстановления объекта из карантина. При помещении на карантин учитывается реальный размер объекта. Зашифрованные файлы могут передаваться в расшифрованном виде (в зависимости от параметров шифрования), сжатые файлы передаются в исходном виде.

Просмотр таблицы объектов, помещенных в Хранилище

Таблица объектов, помещенных в Хранилище, находится в разделе **Хранилище**, подразделе **Файлы** веб-интерфейса программы.

В таблице объектов, помещенных в Хранилище, содержится следующая информация:

1. **Тип** – расположение объекта в Хранилище.

Возможны следующие типы объектов:

- – объект помещен в хранилище одним из следующих способов:
  - выполнена задача **Получить файл**;
  - получена копия объекта, помещенного на карантин на хостах с Kaspersky Endpoint Agent (в разделе **Хранилище**, подразделе **Карантин** в меню, раскрывшемся по ссылке с директорией объекта, выбрано действие **Получить файл из карантина**).
- – объект помещен в хранилище одним из следующих способов:
  - выполнена задача **Собрать форензику**;
  - выполнена задача **Получить дамп памяти процесса**;
  - выполнена задача **Получить ключ реестра**;
  - выполнена задача **Получить метафайлы NTFS**.
- – объект загружен пользователем вручную в разделе **Хранилище**, подразделе **Файлы**.

2. **Объект** – информация об объекте. Например, имя файла или путь к файлу.
3. **Результаты проверки** – результат проверки объекта.

   Результат проверки отображается в виде одного из следующих значений:

   - **Не обнаружено** – в результате проверки программа не обнаружила признаков целевой атаки, возможно зараженных объектов или подозрительной активности.
   - **Ошибка выполнения** – 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 (отображается если вы используете режим распределенного решения и мультитенантности).
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.

В правой части строки с информацией об объекте расположены кнопки:

- Кнопка позволяет удалить объект из Хранилища.
- Кнопка позволяет отправить объект из Хранилища на проверку технологиями Anti-Malware Engine, YARA и Sandbox.
- Кнопка позволяет скачать объект из Хранилища на компьютер.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скачать**.
- **Отправить файл на проверку**.
- Найти события:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- Найти обнаружения:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- Найти события.
- Найти обнаружения.
- **Скопировать значение в буфер**.

Просмотр информации об объекте, загруженном в Хранилище через веб-интерфейс

Чтобы просмотреть информацию об объекте, загруженном в Хранилище вручную, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.

3. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- **Файл** – имя файла.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время загрузки** – время загрузки для объектов, загруженных пользователем вручную.
- **Имя пользователя** – имя учетной записи пользователя, загрузившего объект в Хранилище вручную.
- **Результаты проверки** – результат проверки объекта программой.

Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события**.
- **Найти обнаружения**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти события**.
- **Найти обнаружения**.

- Создать правило запрета.
- **Скопировать значение в буфер**.

Просмотр информации об объекте, помещенном в Хранилище по задаче получения файла

*Чтобы просмотреть информацию об объекте, помещенном в Хранилище по задаче **Получить файл** или **Получить файл из карантина**:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.
3. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- Блок рекомендаций. Могут отображаться следующие рекомендации:
  - Задача – ссылка, по которой открывается раздел **Задачи**, задача, с помощью которой объект был помещен в Хранилище.
  - Обнаружение – ссылка, по которой открывается раздел **Обнаружения**, обнаружение, содержащее объект, помещенный в Хранилище.
  - **Объект на карантине** – ссылка, по которой открывается раздел **Хранилище**, подраздел **Карантин**, метаданные объекта на карантине.
- **Объект** – имя файла или путь к файлу.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время** – время помещения объекта в Хранилище.
- **Тенант** – название тенанта, к которому 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.
- **Результаты проверки** – результат проверки объекта программой.

Нажатием на кнопку Sandbox-обнаружение вы можете открыть окно с подробной информацией о результатах исследования поведения файла.

Кнопка **Найти на TIP** позволяет найти файл на Kaspersky Threat Intelligence Portal.

Кнопка **Создать правило запрета** позволяет запретить запуск файла.

Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события**.
- **Найти обнаружения**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти события**.
- **Найти обнаружения**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

Просмотр информации об объекте, помещенном в Хранилище по задаче получения данных

*Чтобы просмотреть информацию об объекте, помещенном в Хранилище по задачам **Собрать форензику**, **Получить дамп памяти процесса**, **Получить ключ реестра**, **Получить метафайлы NTFS**:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов. В таблице выберите объект со значком , информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- **Объект** – имя файла или путь к файлу.
- **Размер** – размер файла.
- **MD5** – MD5-хеш файла.
- **SHA256** – SHA256-хеш файла.
- **Время** – время помещения объекта в Хранилище.
- **Хост** – имя хоста, с которого получен объект.

Кнопка **Скачать** позволяет загрузить файл на жесткий диск вашего компьютера.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти события**.
- **Найти обнаружения**.
- **Скопировать значение в буфер**.

По ссылке с **MD5** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти события**.
- **Найти обнаружения**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

По ссылке с **SHA256** раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Найти на TIP**.
- **Найти на virustotal.com**.
- **Найти события**.
- **Найти обнаружения**.
- **Создать правило запрета**.
- **Скопировать значение в буфер**.

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:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов. 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.

Чтобы загрузить объект в Хранилище:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов. В правом верхнем углу окна нажмите на кнопу **Загрузить**.

   Откроется окно выбора файла.
3. Выберите объект, который вы хотите загрузить в Хранилище.
4. Если вы хотите загрузить в Хранилище файл с расширением .Lnk, выполните следующие действия:

   a. В поле **File name** введите *.Lnk и нажмите на клавишу **Enter**.

   b. Выберите объект.
5. Нажмите на кнопку **Open**.

Объект будет загружен в Хранилище и отобразится в таблице объектов.

Для пользователей с ролью **Аудитор** функция загрузки объектов в Хранилище недоступна.

Отправка объектов из Хранилища на проверку

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:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.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.

Вы также можете отправить объект из Хранилища на проверку нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных в Хранилище.

Для пользователей с ролью **Аудитор** функция проверки объектов, помещенных в хранилище, недоступна.

Удаление объектов из Хранилища

Чтобы удалить объект из Хранилища:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.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.

Вы также можете удалить объект из Хранилища нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных в Хранилище.

Чтобы удалить все или несколько объектов из Хранилища:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.Установите флажки напротив объектов, которые вы хотите удалить из Хранилища.

   Вы можете выбрать все объекты, установив флажок в строке с заголовками столбцов.
3. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

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

Выбранные объекты будут удалены из Хранилища.

Для пользователей с ролью **Аудитор** функция удаления объектов, помещенных в хранилище, недоступна.

Фильтрация объектов в Хранилище по типу объекта

Чтобы отфильтровать объекты в Хранилище по их типу:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.По ссылке **Тип** откройте меню фильтрации объектов.
3. Установите один или несколько флажков:

   - **Загружен по задаче Получить файл**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище по задачам **Получить файл** и **Восстановить файл из карантина**.
   - **Загружен через веб-интерфейс**, если вы хотите, чтобы программа отображала в таблице объекты, загруженные пользователем через веб-интерфейс Kaspersky Anti Targeted Attack Platform.
   - **Загружен по задаче получения данных**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные в Хранилище по задачам **Собрать форензику**, **Получить метафайлы NTFS**, **Получить ключ реестра**, **Получить дамп памяти процесса**.
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:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.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:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.По ссылке **Результаты проверки** откройте меню фильтрации объектов.

3. Установите один или несколько флажков:
   - **Не обнаружено**.
   - **Ошибка выполнения**.
   - **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:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.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:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.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:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.

2. Откроется таблица объектов.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:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Файлы**.
2. Откроется таблица объектов.Нажмите на кнопку справа от того заголовка столбца 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 таблицы объектов, помещенных на карантин на компьютерах с Kaspersky Endpoint Agent

Таблица объектов, помещенных на карантин на компьютерах с программой Kaspersky Endpoint Agent, находится в разделе **Хранилище**, подразделе **Карантин** веб-интерфейса программы.

На сервере Kaspersky Anti Targeted Attack Platform хранятся метаданные объектов, помещенных на карантин на компьютерах с программой Kaspersky Endpoint Agent. Сами объекты хранятся в специальном хранилище на каждом компьютере, на котором был обнаружен опасный объект.

В таблице объектов, помещенных на карантин на компьютерах с программой Kaspersky Endpoint Agent, содержится следующая информация:

1. **Объект** – информация об объекте. Например, имя файла или путь к файлу.
2. **Адрес источника** – IP-адрес или имя хоста компьютера с программой Kaspersky Endpoint Agent, на карантине которого находится объект.
3. **Время** – дата и время помещения объекта на карантин.
4. **Состояние** – состояние объекта.

В правой части строки с информацией об объекте расположены кнопки:

- Кнопка позволяет удалить метаданные объекта на сервере Kaspersky Anti Targeted Attack Platform.
- Кнопка позволяет восстановить объект из карантина на компьютере с программой Kaspersky Endpoint Agent.
- Кнопка позволяет получить копию объекта из карантина на компьютере с программой Kaspersky Endpoint Agent на сервер Kaspersky Anti Targeted Attack Platform.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- **Скачать**.
- **Отправить файл на проверку**.
- Найти события:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- Найти обнаружения:
  - **Путь к файлу**.
  - **MD5**.
  - **SHA256**.
- **Скопировать значение в буфер**.

По ссылке с именем хоста раскрывается список, в котором вы можете выбрать одно из следующих действий:

- **Добавить в фильтр**.
- **Исключить из фильтра**.
- Найти события.
- Найти обнаружения.
- **Скопировать значение в буфер**.

Просмотр информации об объекте на карантине

Чтобы просмотреть информацию об объекте, помещенном на карантин на компьютере с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.
2. Откроется таблица объектов.В таблице выберите объект, информацию о котором вы хотите посмотреть.

   Откроется окно сведений об объекте.

В окне содержится следующая информация:

- Блок рекомендаций. Может отображаться рекомендация **Задача** – ссылка, по которой открывается раздел **Задачи**, задача, с помощью которой объект был помещен на карантин.
- **Объект** – имя файла или путь к файлу.
- **Размер** – размер файла.
- **Время помещения на карантин** – время помещения объекта на карантин.
- **Тенант** – название тенанта, к которому относится сервер Central Node, PCN или SCN.
- **Хост** – имя компьютера с программой Kaspersky Endpoint Agent, на карантине которого находится объект.
- **Файл** – состояние файла (получена ли копия на сервер Kaspersky Anti Targeted Attack Platform). Если копия файла была получена на сервер Kaspersky Anti Targeted Attack Platform, по ссылке **Найти файл в Хранилище** открывается информация о файле в Хранилище.
- **Состояние** – состояние файла (можно ли восстановить файл из карантина).

Кнопка **Восстановить** позволяет восстановить файл из карантина.

Кнопка **Получить файл** позволяет получить копию файла на сервер Kaspersky Anti Targeted Attack Platform.

По ссылке с именем файла или путем к файлу раскрывается список, в котором вы можете выбрать одно из следующих действий:

- Найти события.
- Найти обнаружения.
- **Скопировать значение в буфер**.

Восстановление объекта из карантина

Чтобы восстановить объект из карантина на компьютере с программой Kaspersky Endpoint Agent:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. В таблице выберите объект, который вы хотите восстановить из карантина на компьютере с программой Kaspersky Endpoint Agent.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Восстановить** в нижней части окна.

   Откроется раздел **Задачи**, задача **Восстановить файл из карантина**.

4. В поле **Описание** введите описание задачи.

5. Нажмите на кнопку **Добавить**.

Файл будет восстановлен из карантина.

Вы также можете запустить задачу восстановления файла из карантина нажатием на кнопку в правой части строки с информацией об объекте таблицы объектов, помещенных на карантин на компьютерах с Kaspersky Endpoint Agent.

Для пользователей с ролью **Аудитор** функция восстановления объекта из карантина недоступна.

Получение копии объекта на карантине на сервер Kaspersky Anti Targeted Attack Platform

Размер объекта, копию которого требуется получить, не должен превышать 100 МБ. Если размер объекта превышает 100 МБ, задача завершается ошибкой.

Чтобы получить копию объекта, помещенного на карантин на компьютере с программой Kaspersky Endpoint Agent, на сервер Kaspersky Anti Targeted Attack Platform:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.

2. В таблице выберите объект, который вы хотите восстановить из карантина на компьютере с программой Kaspersky Endpoint Agent.

   Откроется окно сведений об объекте.

3. Нажмите на кнопку **Получить файл** в нижней части окна.

   Будет создана задача получения копии объекта, помещенного на карантин на компьютере с программой Kaspersky Endpoint Agent. При успешном завершении задачи копия объекта загрузится на сервер Kaspersky Anti Targeted Attack Platform. Объект отобразится в разделе **Хранилище**, подразделе **Файлы** веб-интерфейса программы в таблице объектов, помещенных в Хранилище.

   Информация о задаче отобразится в разделе **Задачи** веб-интерфейса.

Вы также можете получить копию объекта из карантина на компьютере с программой Kaspersky Endpoint Agent на сервер Kaspersky Anti Targeted Attack Platform нажатием на кнопку в правой части строки с информацией об объекте таблицы объектов, помещенных на карантин на компьютерах с Kaspersky Endpoint Agent.

Для пользователей с ролью **Аудитор** получение копии объекта из карантина недоступно.

Удаление информации об объекте, помещенном на карантин, из таблицы

Чтобы удалить информацию об объекте, помещенном на карантин на компьютере с программой Kaspersky Endpoint Agent, из таблицы Kaspersky Anti Targeted Attack Platform:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.
2. Откроется таблица объектов.Нажмите на объект, информацию о котором вы хотите удалить из таблицы.

   Откроется окно сведений об объекте.
3. Нажмите на кнопку **Удалить**.

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

Информация об объекте, помещенном на карантин на компьютере с программой Kaspersky Endpoint Agent, будет удалена из таблицы.

Вы также можете удалить информацию об объекте, помещенном на карантин на компьютере с программой Kaspersky Endpoint Agent, из таблицы нажатием на кнопку в правой части строки с информацией об объекте в таблице объектов, помещенных на карантин.

Для пользователей с ролью **Аудитор** удаление информации об объекте, помещенном на карантин, из таблицы недоступно.

Фильтрация информации об объектах, помещенных на карантин, по типу объекта

Чтобы отфильтровать информацию об объектах, помещенных на карантин, по их типу:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.

   Откроется таблица объектов.
2. По ссылке **Тип** откройте меню фильтрации объектов.

3. Установите один или несколько флажков:

   - **Файл**, если вы хотите, чтобы программа отображала в таблице метаданные объектов, помещенных на карантин.
   - **Дамп памяти процесса**, если вы хотите, чтобы программа отображала в таблице метаданные дампов, помещенных на карантин.

4. Нажмите на кнопку **Применить**.

В таблице объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация информации об объектах, помещенных на карантин, по описанию объекта

Чтобы отфильтровать информацию об объектах, помещенных на карантин, по описанию объекта:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.
2. Откроется таблица объектов.По ссылке **Объект** 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 описания 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 объектов отобразятся только объекты, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация информации об объектах, помещенных на карантин, по имени хоста

Чтобы отфильтровать информацию об объектах, помещенных на карантин, по имени хоста, на котором они были помещены на карантин:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.
2. Откроется таблица объектов.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 имени хоста.
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 информации об объектах, помещенных на карантин, по времени

Чтобы отфильтровать информацию об объектах, помещенных на карантин, по времени помещения на карантин:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.
2. Откроется таблица объектов.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 объекты.
   - **Прошедший час**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные на карантин за предыдущий час.

- **Прошедшие сутки**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные на карантин за предыдущий день.
- **Пользовательский диапазон**, если вы хотите, чтобы программа отображала в таблице объекты, помещенные на карантин 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 информации об объектах на карантине

Чтобы сбросить фильтр по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса программы выберите раздел **Хранилище**, подраздел **Карантин**.
2. Откроется таблица объектов.Нажмите на кнопку справа от того заголовка столбца таблицы объектов на карантине, 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.

Работа с отчетами

При работе в веб-интерфейсе программы пользователи с ролью **Старший сотрудник службы безопасности** могут управлять отчетами об обнаружениях программы: создавать шаблоны отчетов, создавать отчеты по шаблону, просматривать и удалять отчеты и шаблоны отчетов.

Пользователи с ролью **Аудитор** могут просматривать отчеты и шаблоны отчетов и создавать отчеты по шаблону.

Отчет формируется на основе выборки обнаружений за указанный период. Если вы используете режим распределенного решения и мультитенантности, выборка данных осуществляется также по тенанту и серверам этого тенанта.

Управление шаблонами отчетов и отчетами доступно во всех режимах работы программы в соответствии с лицензией.

Выполняйте действия по созданию отчета в следующем порядке:

1. **Создайте шаблон отчета.**
2. **Создайте отчет на основе шаблона.**

У пользователей с ролью **Сотрудник службы безопасности** нет доступа к отчетам.

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 мультитенантности).
- **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.

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 в разделе **Отчеты**, подразделе **Созданные отчеты** интерфейса позволяет только выбрать шаблон для создания отчета и период отображения данных.

Новый шаблон отчета создается для каждой выборки данных.

Чтобы создать шаблон:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

   Откроется таблица шаблонов.

2. Нажмите на кнопку **Добавить**.

   Откроется окно создания шаблона. Окно содержит тело отчета и конструктор отчета в плавающем окне. Вы можете перемещать конструктор отчета по рабочей области окна веб-интерфейса.

3. В поле **Имя шаблона** в правом верхнем углу окна введите имя, которое вы хотите присвоить отчетам, создаваемым по этому шаблону. Например, **Обнаружения по технологии**.

   Это имя отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов на этом шаблоне.

4. Вместо текста **Заголовок отчета** введите имя отчета, которое отобразится в отчете после создания отчета. Если вы не хотите добавлять имя отчета, вы можете удалить 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 удалить 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.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция создания шаблона отчета недоступна.

Создание отчета по шаблону

Чтобы создать отчет по шаблону:

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 мультитенантности, в блоке параметров **Серверы** установите флажки напротив тех тенантов 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 на вашем компьютере.

Для пользователей с ролью **Сотрудник службы безопасности** функция создания шаблона отчета недоступна.

Просмотр отчета

Чтобы просмотреть отчет:

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:

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:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.

2. Откроется таблица шаблонов. Выберите шаблон, который вы хотите изменить.

   Откроется окно изменения шаблона.

3. Вы можете изменить следующие параметры:

- **Имя шаблона** – имя отчета, которое отобразится в таблице в разделе **Отчеты**, подразделе **Созданные отчеты** при создании всех отчетов по этому шаблону.
- **Заголовок отчета** – имя отчета, которое отобразится в отчете после создания отчета.

  Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
- **Описание отчета** – описание отчета, которое отобразится в отчете после создания отчета.

  Вы можете форматировать текст с помощью кнопок в блоке **Text** в конструкторе шаблона.
- **Изображение**. Вы можете загрузить или удалить изображение.
- **Диаграмма**. Вы можете изменить следующие параметры диаграммы:
  - **Имя**.
  - **Источник данных**.
  - **Количество секторов**.

  Нажмите на кнопку **Применить**.
- **Таблица**. Вы можете изменить следующие параметры таблицы:
  - **Выбранные столбцы**. Вы можете перетаскивать имена столбцов между полями **Доступные столбцы** и **Выбранные столбцы**, а также менять порядок столбцов таблицы отчета.
  - **Состояние**.
  - **Технологии**.
  - **Важность**.
  - **Статус VIP**.

4. Выберите один из следующих способов сохранения шаблона:

- Если вы хотите применить изменения к текущему шаблону, нажмите на кнопку **Сохранить**.

  Шаблон будет изменен.
- Если вы хотите создать новый шаблон, введите имя шаблона и нажмите на кнопку **Сохранить как**.

  > Имя нового шаблона не должно совпадать с именем уже существующего шаблона.

  Новый шаблон будет сохранен.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения шаблона недоступна.

Фильтрация шаблонов по имени

Чтобы отфильтровать шаблоны по имени:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. 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:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. 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:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. 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:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. Нажмите на кнопку справа от того заголовка столбца 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:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Шаблоны**.
2. Откроется таблица шаблонов. 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.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления шаблона недоступна.

Фильтрация отчетов по времени создания

Чтобы отфильтровать отчеты по времени их создания:

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:

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:

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:

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:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**, подраздел **Созданные отчеты**.

   Откроется таблица отчетов.

2. Нажмите на кнопку справа от того заголовка столбца 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:

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.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления отчета недоступна.

Работа с правилами присвоения обнаружениям статуса VIP

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, удалять, изменять, импортировать и экспортировать список правил присвоения обнаружениям статуса VIP.

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.

Пользователи с ролью **Аудитор** могут просматривать, импортировать и экспортировать список правил присвоения обнаружениям статуса VIP.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения обнаружениям статуса VIP недоступен.

Просмотр таблицы правил присвоения статуса VIP

Таблица правил присвоения статуса VIP находится в разделе веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.

В таблице содержится следующая информация:

- **Критерий** – критерий добавления записи в список правил.
- **Значение** – значение критерия.
- **Описание** – дополнительная информация, указанная при создании правила.

Создание правила присвоения статуса VIP

Чтобы добавить правило присвоения обнаружениям статуса VIP:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Добавить**.

   Откроется окно добавления правила.
3. В раскрывающемся списке **Критерий** выберите один из следующих типов правила:
   - **IP**, если вы хотите добавить правило для IP-адреса компьютера.
   - **Хост**, если вы хотите добавить правило для имени хоста.
   - **Email**, если вы хотите добавить правило для адреса электронной почты.
4. В поле **Значение** введите нужное значение.

   Например, если в списке **Критерий** вы выбрали **Email**, в поле **Значение** введите адрес электронной почты, для которого вы хотите добавить правило.
5. В поле **Описание** введите дополнительную информацию, если необходимо.
6. Нажмите на кнопку **Добавить**.

Правило будет добавлено. Новым обнаружениям, связанным с добавленным IP-адресом, именем хоста или адресом электронной почты, будет присвоен статус VIP.

Для пользователей с ролью **Аудитор** функция создания правил для присвоения обнаружениям статуса VIP недоступна.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения обнаружениям статуса VIP недоступен.

Удаление правила присвоения статуса VIP

Чтобы удалить правило присвоения обнаружениям статуса VIP:

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.

Для пользователей с ролью **Аудитор** функция удаления правил для присвоения обнаружениям статуса VIP недоступна.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения обнаружениям статуса VIP недоступен.

Изменение правила присвоения статуса VIP

Чтобы изменить правило присвоения обнаружениям статуса VIP:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. Выберите правило, которое вы хотите изменить.

   Откроется окно изменения правила.
3. Внесите необходимые изменения в поля **Критерий**, **Значение**, **Описание**.
4. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Для пользователей с ролью **Аудитор** функция изменения правил для присвоения обнаружениям статуса VIP недоступна.

Пользователям с ролью **Сотрудник службы безопасности** просмотр списка правил присвоения обнаружениям статуса VIP недоступен.

Импорт списка правил присвоения статуса VIP

Чтобы импортировать список правил присвоения обнаружениям статуса VIP:

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:

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:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Статус VIP**.
2. По ссылке **Критерий** откройте окно настройки фильтрации.

3. Установите один или несколько флажков рядом с типами правил:

   - **IP**.
   - **Хост**.
   - **Email**.

4. Нажмите на кнопку **Применить**.

   Окно настройки фильтрации закроется.

   В таблице отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Фильтрация и поиск по значению правила присвоения статуса VIP

Чтобы отфильтровать или найти правила присвоения обнаружениям статуса VIP по значению правила:

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:

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:

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

2. Нажмите на кнопку справа от того заголовка столбца 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 со списком исключений из проверки

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, импортировать и экспортировать список *исключений из проверки* – список данных, которые Kaspersky Anti Targeted Attack Platform будет считать безопасными и не будет отображать в таблице обнаружений. Вы можете создать правила исключений из проверки для следующих данных:

- **MD5**.
- **Формат**.
- **Маска URL**.
- **Email получателя**.
- **Email отправителя**.
- **IP или подсеть источника**.

- **IP или подсеть назначения**.
- **Агент пользователя**.

Пользователи с ролью **Аудитор** и **Сотрудник службы безопасности** могут просматривать список правил исключений из проверки, а также экспортировать его.

Просмотр таблицы данных, исключенных из проверки

Чтобы просмотреть таблицу с данными, исключенными из проверки:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения из проверки**.

   Отобразится таблица со списком данных, которые Kaspersky Anti Targeted Attack Platform будет считать безопасными и не будет создавать для них обнаружения. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- **Критерий** – критерий добавления записи в список разрешенных объектов.
- **Значение** – значение критерия.

Добавление правила исключения из проверки

Чтобы добавить правило исключения из проверки:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения из проверки**.
3. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. В раскрывающемся списке **Критерий** выберите один из следующих критериев добавления правила в список исключений из проверки:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Email получателя**.
   - **Email отправителя**.
   - **IP или подсеть источника**.

- **IP или подсеть назначения**.
- **Агент пользователя**.

5. Если вы выбрали **Формат**, в раскрывающемся списке **Значение** выберите формат файла, который вы хотите добавить.

   Например, вы можете выбрать формат **MSOfficeDoc**.

6. Если вы выбрали **MD5**, **Маска URL**, **Email получателя**, **Email отправителя**, **IP или подсеть источника**, **IP или подсеть назначения** или **Агент пользователя**, в поле **Значение** введите значение соответствующего критерия, которое вы хотите добавить в список исключений из проверки:

   - 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 исключения из проверки, при вводе этих символов нужно использовать `\` – отмена одного из следующих за ним символов `*` или `?`, `\`.

     Пример:
     В качестве доверенного адреса требуется 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 список исключений из проверки, будет выглядеть следующим образом:
     `www.example.com/download_virus/virus.dll\?virus_name=`

   - Если вы выбрали **Email получателя** или **Email отправителя**, в поле **Значение** введите адрес электронной почты.
   - Если вы выбрали **Агент пользователя**, в поле **Значение** введите заголовок **User agent HTTP-запросов**, содержащий информацию о браузере.
   - Если вы выбрали **IP или подсеть источника** или **IP или подсеть назначения**, в поле **Значение** введите адрес или подсеть (например, 255.255.255.0).

   В полях **Маска URL**, **Email получателя**, **Email отправителя** вы можете указывать доменные имена, содержащие символы кириллицы. В этом случае указанный адрес будет преобразован в Punycode и обработан в соответствии с параметрами программы.

7. Нажмите на кнопку **Добавить**.

Правило будет добавлено в список исключений из проверки.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция добавления правила исключения из проверки недоступна.

Удаление правила исключения из проверки

Чтобы удалить одно или несколько правил из списка исключений из проверки:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения из проверки**.
3. Установите флажок слева от каждого правила, которое вы хотите удалить из списка исключений из проверки.

   Если вы хотите удалить все правила, установите флажок над списком.
4. В нижней части окна нажмите на кнопку **Удалить**.

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

Выбранные правила будут удалены из списка исключений из проверки.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления записи в списке исключений из проверки недоступна.

Изменение правила, добавленного в исключения из проверки

Чтобы изменить правило в списке исключений из проверки:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения из проверки**.
3. Выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения в поля **Критерий** и **Значение**.
5. Нажмите на кнопку **Сохранить**.

Правило будет изменено.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция изменения правила в списке исключений из проверки недоступна.

Экспорт списка данных, исключенных из проверки

Чтобы экспортировать список исключений из проверки:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения из проверки**.
3. В правом верхнем углу окна веб-интерфейса программы нажмите на кнопку **Экспортировать**.

Файл в формате JSON с экспортированным списком исключений из проверки будет сохранен в папку загрузки браузера на вашем компьютере.

Фильтрация правил в списке исключений из проверки по критерию

Чтобы отфильтровать записи в списке исключений из проверки по типу правила:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения из проверки**.
3. По ссылке **Критерий** откройте окно настройки фильтрации.
4. Установите один или несколько флажков рядом с критериями, по которым вы хотите отфильтровать правила:
   - **MD5**.
   - **Формат**.
   - **Маска URL**.
   - **Email получателя**.
   - **Email отправителя**.
   - **IP или подсеть источника**.
   - **IP или подсеть назначения**.
   - **Агент пользователя**.
5. Нажмите на кнопку **Применить**.

Окно настройки фильтрации закроется.

В списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Поиск правил в списке исключений из проверки по значению

Чтобы найти правила в списке исключений из проверки по значению:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения из проверки**.
3. По ссылке **Значение** откройте окно настройки фильтрации.
4. Введите символы значения.
5. Нажмите на кнопку **Применить**.

В списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Вы можете использовать несколько фильтров одновременно.

Сброс фильтра правил в списке исключений из проверки

Чтобы сбросить фильтр записей в списке исключений по одному или нескольким условиям фильтрации:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения из проверки**.
3. Нажмите на кнопку справа от того заголовка столбца таблицы записей в списке исключений из проверки, 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 списке исключений из проверки отобразятся только правила, соответствующие заданным вами условиям.

Работа с IDS-исключениями

Пользователи с ролью **Старший сотрудник службы безопасности** могут добавлять правила IDS "Лаборатории Касперского", по которым выполнены обнаружения средней и высокой степени важности, в исключения из проверки. Kaspersky Anti Targeted Attack Platform не будет создавать обнаружения по правилам IDS, добавленным в исключения.

Вы можете добавить в исключения только правила IDS "Лаборатории Касперского". Если вы не хотите применять при проверке пользовательское правило IDS, вы можете отключить это правило или удалить его.

Пользователи с ролью **Аудитор** могут просматривать список правил IDS, добавленных в исключения, и свойства выбранного правила.

Пользователям с ролью **Сотрудник службы безопасности** список правил IDS, добавленных в исключения, недоступен.

Просмотр таблицы правил IDS, добавленных в исключения

Чтобы просмотреть таблицу правил IDS, добавленных в исключения:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите на закладку **Исключения IDS**.

   Отобразится таблица правил IDS, добавленных в исключения. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- **Время создания** – дата и время добавления правила IDS в исключения.
- **Правило** – имя правила IDS.
- **ID правила** – идентификатор правила IDS. sid (signature ID) в формате Suricata.
- **Описание** – описание правила IDS.
- **Автор** – имя пользователя, под учетной записью которого правило IDS было добавлено в исключения.

Добавление правила IDS в исключения

Вы можете добавлять правила IDS "Лаборатории Касперского", по которым выполнены обнаружения средней и высокой степени важности, в исключения из проверки событий.

Вы можете добавить в исключения только правила IDS "Лаборатории Касперского". Если вы не хотите применять при проверке событий пользовательское правило IDS , вы можете отключить это правило или удалить его.

Чтобы добавить правило IDS в исключения:

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке слева выберите **Содержит**.

4. В раскрывающемся списке справа выберите технологию **(IDS) Intrusion Detection System**.

5. Нажмите на кнопку **Применить**.

6. По значку раскройте список параметров фильтрации.

7. Выберите одну или обе степени важности обнаружений:

   - **Средняя** – обнаружение средней степени важности.
   - **Высокая** – обнаружение высокой степени важности.

   В таблице отобразятся обнаружения средней и/или высокой степени важности, выполненные технологией Intrusion Detection System на основе правил IDS "Лаборатории Касперского".

8. Выберите обнаружение, для которого в столбце **Обнаружено** отображается название нужного правила IDS.

   Откроется окно с информацией об обнаружении.

9. В правой части окна в блоке **Рекомендации** в разделе **Оценка** выберите **Добавить в исключения**.

   Откроется окно **Добавить правило IDS в исключения**.

10. В поле **Описание** введите описание правила IDS.

11. Нажмите на кнопку **Добавить**.

    Правило IDS будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса программы, подразделе **Исключения** на закладке **Исключения IDS**. Это правило не будет применяться при создании обнаружений.

Для пользователей с ролью **Аудитор** функция изменения записи в списке разрешенных объектов недоступна.

Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку правил IDS, добавленных в исключения.

Редактирование описания правила IDS, добавленного в исключения

*Чтобы отредактировать описание правила IDS, добавленного в исключения, из раздела **Обнаружения**:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.

2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.

3. В раскрывающемся списке слева выберите **Содержит**.

4. В раскрывающемся списке справа выберите технологию **(IDS) Intrusion Detection System**.

5. Нажмите на кнопку **Применить**.

6. По значку раскройте список параметров фильтрации.

7. Выберите одну или обе степени важности обнаружений:

   - **Средняя** – обнаружение средней степени важности.
   - **Высокая** – обнаружение высокой степени важности.

   В таблице отобразятся обнаружения средней и/или высокой степени важности, выполненные технологией Intrusion Detection System на основе правил IDS "Лаборатории Касперского".

8. Выберите обнаружение, для которого в столбце **Обнаружено** отображается название нужного правила IDS.

   Откроется окно с информацией об обнаружении.

9. В правой части окна в блоке **Рекомендации** в разделе **Оценка** выберите **Изменить исключение IDS**.

   Откроется окно **Изменить исключение IDS**.

   В поле **Описание** измените описание правила.

Нажмите на кнопку **Сохранить**.

Описание правила IDS, добавленного в исключения, будет изменено. Это правило не будет применяться при создании обнаружений.

Для пользователей с ролью **Аудитор** функция редактирования описания правила IDS недоступна.

Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку правил IDS, добавленных в исключения.

Удаление правил IDS из исключений

Вы можете удалить из исключений одно или несколько правил IDS, а также все правила сразу.

Чтобы удалить правило IDS из исключений:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Исключения** и перейдите на закладку **Исключения IDS**.
2. Отобразится список правил IDS, добавленных в исключения.
3. Выберите правило, которое вы хотите удалить из исключений.

   Откроется окно с информацией о правиле.
4. Нажмите на кнопку **Удалить**.

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

Правило будет удалено из исключений. Правило будет применяться при создании обнаружений.

Чтобы удалить все или несколько правил IDS из исключений:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Исключения** и перейдите на закладку **Исключения IDS**.
2. Отобразится список правил IDS, добавленных в исключения.
3. Установите флажки напротив правил, которые вы хотите удалить из исключений.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

4. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из исключений. Правила будут применяться при создании обнаружений.

Для пользователей с ролью **Аудитор** функция удаления правила IDS из исключений недоступна.

Пользователи с ролью **Сотрудник службы безопасности** не имеют доступа к списку IDS-исключений.

Работа с TAA-исключениями

Правила TAA (IOA), сформированные специалистами "Лаборатории Касперского", содержат признаки подозрительного поведения объекта в IT-инфраструктуре организации. Kaspersky Anti Targeted Attack Platform проверяет базу событий программы и создает обнаружения для событий, которые совпадают с поведением, описанным в правилах TAA (IOA). Если вы хотите, чтобы программа не создавала обнаружения для событий, сформированных в результате нормальной для вашей организации активности хоста, вы можете добавить правило TAA (IOA) в исключения.

В программе предусмотрены следующие режимы работы правил TAA (IOA), добавленных в исключения:

- Правило исключается всегда.

  В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу TAA (IOA) и не создает обнаружения по этому правилу.

- Правило дополняется условием.

  В этом случае правило TAA (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу TAA (IOA). Для событий, которые соответствуют правилу TAA (IOA), но не соответствуют условиям примененного исключения, программа отмечает события и создает обнаружения.

Если вы используете режим распределенного решения и мультитенантности, исключения TAA могут быть следующих типов:

- **Локальный** – созданные на сервере SCN. Действие исключений распространяется только на хосты, подключенные к этому серверу SCN. Исключения относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.

- **Глобальный** – созданные на сервере PCN. Действие исключений распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Исключения относятся к тенанту, в рамках которой пользователь работает в веб-интерфейсе программы.

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать, редактировать, удалять исключения в рамках тех тенантов, к данным которых у них есть доступ.

Пользователи с ролью **Аудитор** и **Сотрудник службы безопасности** могут только просматривать список исключений TAA и свойства выбранного исключения.

Для каждого правила TAA (IOA) можно создать только одно локальное или глобальное исключение.

Если для одного правила TAA (IOA) созданы исключения на сервере SCN и PCN, Kaspersky Anti Targeted Attack Platform обрабатывает события в соответствии с параметрами, заданными для исключения на сервере PCN.

Просмотр таблицы правил TAA (IOA), добавленных в исключения

Чтобы просмотреть таблицу правил TAA (IOA), добавленных в исключения:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения**.
2. Перейдите закладку **Исключения TAA (IOA)**.

   Отобразится таблица правил TAA (IOA), добавленных в исключения. Вы можете фильтровать правила по ссылкам в названии столбцов.

В таблице содержится следующая информация:

- – степень важности, присвоенная обнаружению, выполненному по этому правилу TAA (IOA).

  Степень важности может иметь одно из следующих значений:

  - – **Низкая**.
  - – **Средняя**.
  - – **Высокая**.
- **Тип** – тип правила в зависимости от роли сервера, на котором оно создано:
  - **Локальный** – созданные на сервере SCN. Действие исключений распространяется только на хосты, подключенные к этому серверу SCN. Исключения относятся к тенанту, в рамках которого пользователь работает в веб-интерфейсе программы.
  - **Глобальный** – созданные на сервере PCN. Действие исключений распространяется на хосты, подключенные к этому серверу PCN и ко всем серверам SCN, подключенным к этому серверу PCN. Исключения относятся к тенанту, в рамках которой пользователь работает в веб-интерфейсе программы.

- **Надежность** – уровень надежности в зависимости от вероятности ложных срабатываний правила:
  - **Высокая**.
  - **Средняя**.
  - **Низкая**.

  Чем выше уровень надежности, тем меньше вероятность ложных срабатываний.
- **Исключать правило** – режим работы правила, добавленного в исключения.
  - **Всегда** – правило исключается всегда. В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу TAA (IOA) и не создает обнаружения по этому правилу.
  - **При условии** – правило исключается при добавлении условия. В этом случае правило TAA (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу TAA (IOA). Для событий, которые соответствуют правилу TAA (IOA), но не соответствуют условиям примененного исключения, программа отмечает события и создает обнаружения.
- **Имя** – имя правила.

Добавление правила TAA (IOA) в исключения

Вы можете добавить в исключения только правила TAA (IOA) "Лаборатории Касперского". Если вы не хотите применять при проверке событий пользовательское правило TAA (IOA), вы можете отключить это правило или удалить его.

*Чтобы добавить правило TAA (IOA) в исключения из раздела **Обнаружения**:*

1. В окне веб-интерфейса программы выберите раздел **Обнаружения**.

   Откроется таблица обнаружений.
2. По ссылке в столбце **Технологии** откройте окно настройки фильтрации.
3. В раскрывающемся списке слева выберите **Содержит**.
4. В раскрывающемся списке справа выберите технологию **(TAA) Targeted Attack Analyzer**.
5. Нажмите на кнопку **Применить**.

   В таблице отобразятся обнаружения, выполненные технологией TAA на основе правил TAA (IOA).
6. Выберите обнаружение, для которого в столбце **Обнаружено** отображается название нужного правила.

   Откроется окно с информацией об обнаружении.
7. В блоке **Результаты проверки** по ссылке с названием правила откройте окно с информацией о правиле.
8. Справа от названия параметра **Исключения TAA** нажмите на кнопку **Добавить в исключения**.

   Откроется окно добавления правила TAA (IOA) в исключения.

9. В поле **Исключать правило** выберите режим работы исключения:

   - **Всегда**, если вы хотите, чтобы программа не создавала обнаружения для событий, соответствующих выбранному правилу TAA (IOA).

   - **При условии**, если вы хотите, чтобы программа не создавала обнаружения только для событий, подходящих под заданные условия. Для событий, которые соответствуют правилу TAA (IOA) при заданных условиях исключения, программа создаст обнаружения.

     Если вы выбрали **При условии**, выполните следующие действия:

     a. По ссылке **Настройка дополнительных условий** откройте форму поиска событий.

     b. Если вы используете режим распределенного решения и мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.

     c. Выполните поиск событий в режиме конструктора.

        Отобразится таблица событий, соответствующих правилу TAA (IOA) при заданных условиях исключения.

        Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

     d. Нажмите на имя того сервера, события которого вы хотите просмотреть.

        Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

        > При необходимости вы можете изменить условия поиска событий.

     e. Нажмите на кнопку **Добавить исключение**.

10. Если вы используете режим распределенного решения и мультитенантности, в поле **Применить к серверам*** установите флажки напротив тенантов и серверов, к которым будет применяться правило.

11. Нажмите на кнопку **Добавить**.

Правило TAA (IOA) будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса программы, подразделе **Исключения** на закладке **Исключения TAA (IOA)**. Это правило не будет применяться при создании обнаружений.

*Чтобы добавить правило TAA (IOA) в исключения из раздела **Поиск угроз**:*

1. В окне веб-интерфейса программы выберите раздел **Поиск угроз**.

   Откроется форма поиска событий.

2. Задайте условия поиска и нажмите на кнопку **Найти**. Например, вы можете выбрать критерии для поиска событий в группе **Свойства TAA** в режиме конструктора.

   Отобразится таблица событий, удовлетворяющих условиям поиска.

3. Выберите событие.

4. Справа от названия параметра **Теги IOA** нажмите на имя правила.

   Откроется окно с информацией о правиле.

5. Справа от названия параметра **Исключения ТАА** нажмите на кнопку **Добавить в исключения**.

   Откроется окно добавления правила ТАА (IOA) в исключения.

6. В поле **Исключать правило** выберите режим работы исключения:

   - **Всегда**, если вы хотите, чтобы программа не создавала обнаружения для событий, соответствующих выбранному правилу ТАА (IOA).

   - **При условии**, если вы хотите, чтобы программа не создавала обнаружения только для событий, подходящих под заданные условия. Для событий, которые соответствуют правилу ТАА (IOA) при заданных условиях исключения, программа создаст обнаружения.

     Если вы выбрали **При условии**, выполните следующие действия:

     a. По ссылке **Настройка дополнительных условий** откройте форму поиска событий.

     b. Если вы используете режим распределенного решения и мультитенантности и хотите включить отображение событий по всем тенантам, включите переключатель **Искать по всем тенантам**.

     c. Выполните поиск событий в режиме конструктора.

        Отобразится таблица событий, соответствующих правилу ТАА (IOA) при заданных условиях исключения.

        Если вы используете режим распределенного решения и мультитенантности, отобразятся уровни группировки найденных событий: Сервер – Названия тенантов – Имена серверов.

     d. Нажмите на имя того сервера, события которого вы хотите просмотреть.

        Отобразится таблица хостов выбранного сервера. Уровни группировки событий отобразятся над таблицей.

        > При необходимости вы можете изменить условия поиска событий.

     e. Нажмите на кнопку **Добавить исключение**.

7. Нажмите на кнопку **Добавить**.

Правило ТАА (IOA) будет добавлено в исключения и отобразится в списке исключений в разделе **Параметры** веб-интерфейса программы, подразделе **Исключения** на закладке **Исключения ТАА (IOA)**. Это правило не будет применяться при проверке событий.

При создании поискового запроса, сохраняемого как условия исключения, не рекомендуется использовать следующие поля:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

Перечисленные поля отображаются только после того, как Kaspersky Anti Targeted Attack Platform отмечает события как подходящие под правила TAA (IOA).

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция добавления правила TAA (IOA) в исключения недоступна.

Просмотр правила TAA (IOA), добавленного в исключения

Чтобы просмотреть правило TAA (IOA), добавленное в исключения:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **Исключения TAA (IOA)**.

   Отобразится таблица правил TAA (IOA), добавленных в исключения.

2. Выберите правило, которое вы хотите просмотреть.

   Откроется окно с информацией о правиле.

Окно содержит следующую информацию:

- **Правило TAA (IOA)** – по ссылке открывается окно с описанием техники MITRE, соответствующей этому правилу, рекомендациями 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".
- **Исключать правило** – режим работы правила, добавленного в исключения.
  - **Всегда** – правило исключается всегда. В этом случае Kaspersky Anti Targeted Attack Platform не отмечает события как соответствующие правилу TAA (IOA) и не создает обнаружения по этому правилу.
  - **При условии** – правило исключается при добавлении условия. В этом случае правило TAA (IOA) дополняется условиями в виде поискового запроса. Kaspersky Anti Targeted Attack Platform не отмечает события, подходящие под заданные условия, как соответствующие правилу TAA (IOA). Для событий, которые соответствуют правилу TAA (IOA), но не соответствуют условиям примененного исключения, программа отмечает события и создает обнаружения.
- **Настройка дополнительных условий** – по ссылке открывается форма поиска событий с условиями поискового запроса.

  Поле отображается, если при добавлении правила TAA (IOA) в исключения вы выбрали режим работы правила **При условии** и задали условия поискового запроса.

- Условия поискового запроса в формате `<IOA ID> AND NOT <условия поискового запроса>`.

  Условия поискового запроса отображаются, если при добавлении правила TAA (IOA) в исключения вы выбрали режим работы правила **При условии** и задали условия поискового запроса.

- **Применить к серверам*** – хосты, к которым применяется исключение.

  Поле отображается в режиме распределенного решения и мультитенантности.

Удаление правил TAA (IOA) из исключений

Вы можете удалить из исключений одно или несколько правил TAA (IOA), а также все правила сразу.

Чтобы удалить правило TAA (IOA) из исключений, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **Исключения TAA (IOA)**.

   Отобразится таблица правил TAA (IOA), добавленных в исключения.

2. Выберите правило, которое вы хотите удалить из исключений.

   Откроется окно с информацией о правиле.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

4. Нажмите на кнопку **Да**.

Правило будет удалено из исключений. Правило будет применяться при создании обнаружений и при проверке событий.

Чтобы удалить все или несколько правил TAA (IOA) из исключений, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Исключения** и перейдите на закладку **Исключения TAA (IOA)**.

2. Отобразится таблица правил TAA (IOA), добавленных в исключения.

3. Установите флажки напротив правил, которые вы хотите удалить из исключений.

   Вы можете выбрать все правила, установив флажок в строке с заголовками столбцов.

4. В панели управления в нижней части окна нажмите на кнопку **Удалить**.

   Откроется окно подтверждения действия.

5. Нажмите на кнопку **Да**.

Выбранные правила будут удалены из исключений. Правила будут применяться при создании обнаружений и при проверке событий.

Для пользователей с ролью **Аудитор** и **Сотрудник службы безопасности** функция удаления из исключений правил TAA (IOA) недоступна.

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:

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.

Пользователи с ролью **Аудитор** могут просматривать список паролей для архивов без возможности редактирования.

Просмотр параметров сервера

Пользователям с ролью **Аудитор** доступен просмотр настроек сервера Central Node и PCN в режиме распределенного решения и мультитенантности.

Настройки сервера располагаются в разделе **Параметры** окна веб-интерфейса. В этом разделе вы можете просмотреть следующую информацию:

- **Пользователи** – список учетных записей пользователей веб-интерфейса программы.
- **Общие параметры** – общие параметры сервера.
  - **Обновление баз** – обновление баз данных.
  - **Мониторинг** – максимальное допустимое значение заполнения жесткого диска серверов Central Node и Sensor.

- **SNMP** – параметры соединения с протоколом SNMP.
- **Управление сервером** – управление сервером.

- **Сертификаты** – состояние сертификатов сервера и компьютеров с программой Kaspersky Endpoint Agent.
- **Дата и время** – настройки даты и времени сервера.
- **Endpoint Agents** – функции программы, доступные при интеграции с Kaspersky Endpoint Agent.
  - **Расписание IOC-проверки** – настройки расписания IOC-проверки.
  - **Автоматическая отправка файлов в Sandbox** – автоматическая отправка файлов на проверку компоненту Sandbox.
  - **Индикаторы активности** – показатели активности программы Kaspersky Endpoint Agent.
- **KSN/KPSN и MDR** – настройки участия в Kaspersky Security Network и Kaspersky Privat Security Network.
- **Репутационная база KPSN** – настройки использования репутационной базы KPSN.
- **SIEM-система** – настройки интеграции с SIEM-системой.
- **Уведомления** – настройки отправки уведомлений
- **Статус VIP** – список правил присвоения обнаружениям статуса VIP.
- **Исключения** – список разрешенных объектов и списки исключений из правил TAA и IDS.
- **Сетевые параметры** – настройки параметров сетевого интерфейса.
- **Пароли к архивам** – список паролей для архивов.
- **Лицензия** – состояние ключа лицензии.
- **Журнал активности** – настройки журнала активности.

Просмотр таблицы серверов с компонентом Sandbox

Для пользователей с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** просмотр таблицы серверов с компонентом Sandbox недоступен.

Пользователи с ролью **Аудитор** могут просматривать таблицу 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.

Просмотр таблицы серверов с компонентом Sensor

Пользователи с ролью **Аудитор** могут просматривать таблицу серверов с компонентом Sensor.

- 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.

Для пользователей с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** просмотр таблицы серверов с компонентом Sensor недоступен.

Просмотр таблицы внешних систем

Пользователи с ролью **Аудитор** могут просматривать таблицу 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 столбце отображается прочерк.
- **ID** – идентификатор внешней системы.
- **Отпечаток сертификата** – отпечаток TLS-сертификата сервера с внешней системой, с помощью которого устанавливается шифрованное соединение с сервером Central Node.

  Отпечаток сертификата сервера с компонентом Central Node отображается в верхней части окна в поле **Отпечаток сертификата**.
- **Состояние** – состояние запроса на интеграцию.

Для пользователей с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** просмотр таблицы внешних систем недоступен.

Отправка уведомлений

Пользователи с ролью **Администратор**, **Старший сотрудник службы безопасности**, **Сотрудник службы безопасности** могут настроить отправку уведомлений на один или несколько адресов электронной почты.

Вы можете создать уведомления об обнаружениях и о работоспособности системы.

Пользователи с ролью **Аудитор** могут просматривать список правил для отправки уведомлений, свойства выбранного правила и параметры соединения с почтовым сервером без возможности редактирования.

Для корректной отправки уведомлений на адрес электронной почты необходимо предварительно настроить параметры соединения с почтовым сервером. Настройку соединения выполняет **Администратор**.

Просмотр таблицы правил для отправки уведомлений

Правила для отправки уведомлений отображаются в разделе **Параметры**, подразделе **Уведомления** 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:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.

3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.

4. 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.

5. В поле **Тема** введите тему сообщения с уведомлением.

6. Если вы хотите, чтобы программа подставляла важность обнаружения в тему сообщения, добавьте в поле **Тема** макрос `%importance%`.

7. В поле **Тип уведомления** выберите **Обнаружения**.

8. 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.

9. 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.

10. 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.

11. В блоке параметров **Компоненты** установите флажки рядом с названиями одной или нескольких технологий, если вы хотите настроить отправку уведомлений об обнаружениях, выполненных определенными технологиями.

12. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений об обнаружениях будет добавлено в список правил. Чтобы уведомления приходили на указанный адрес электронной почты, требуется включить правило отправки уведомлений. Уведомления отправляются однократно по всем указанным в правиле адресам электронной почты.

Для пользователей с ролью **Администратор** и **Аудитор** функция создания правил для отправки уведомлений об обнаружениях недоступна.

В режиме распределенного решения уведомления требуется создать отдельно для каждого подчиненного сервера (*Secondary Central Node*, *SCN*).

Создание правила для отправки уведомлений о работе компонентов программы

Чтобы создать правило для отправки уведомлений о работе компонентов программы:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
4. 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.
5. В поле **Тема** введите тему сообщения с уведомлением.
6. Если вы хотите, чтобы программа указывала важность обнаружения в теме сообщения, добавьте в поле **Тема** макрос `%importance%`.
7. В поле **Тип уведомления** выберите **Работа программы**.
8. В блоке параметров **Компоненты** установите флажки рядом с названиями тех функциональных областей программы, о которых вы хотите получать уведомления.
9. Нажмите на кнопку **Добавить**.

Правило для отправки уведомлений о работе компонентов программы будет добавлено в список правил. Чтобы уведомления приходили на указанный адрес электронной почты, требуется включить правило отправки уведомлений. Уведомления отправляются однократно по всем указанным в правиле адресам электронной почты.

Для пользователей с ролью **Аудитор** функция создания правил для отправки уведомлений о работе программы недоступна.

В режиме распределенного решения уведомления настраиваются отдельно для каждого подчиненного сервера (*Secondary Central Node*, *SCN*).

Включение и отключение правила для отправки уведомлений

Чтобы включить или отключить правило для отправки уведомлений об обнаружениях:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В столбце **Состояние** включите или отключите правило для отправки уведомлений с помощью переключателя рядом с этим правилом.

Состояние правила для отправки уведомлений об обнаружениях будет изменено.

Для пользователей с ролью **Аудитор** функция включения и отключения правил для отправки уведомлений недоступна.

Изменение правила для отправки уведомлений

Чтобы изменить правило для отправки уведомлений:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В списке правил для отправки уведомлений выберите правило, которое вы хотите изменить.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения.
5. Нажмите на кнопку **Сохранить**.

Правило для отправки уведомлений будет изменено.

Для пользователей с ролью **Аудитор** функция изменения правил для отправки уведомлений недоступна.

Удаление правила для отправки уведомлений

Чтобы удалить правило для отправки уведомлений:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Установите флажок слева от названия каждого правила, которое вы хотите удалить.

   Если вы хотите удалить все правила, установите флажок над списком.
4. Нажмите на кнопку **Удалить** в нижней части окна.
5. В окне подтверждения нажмите на кнопку **Да**.

Выбранные правила будут удалены.

Для пользователей с ролью **Аудитор** функция удаления правил для отправки уведомлений недоступна.

Фильтрация и поиск правил отправки уведомлений по типу правила

Чтобы отфильтровать или найти правила отправки уведомлений по типу правила:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. В таблице правил для отправки уведомлений нажмите на значок ⬚.

   Откроется окно настройки фильтрации.
4. 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:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Тема** откройте окно настройки фильтрации.
4. Введите один или несколько символов темы уведомлений.
5. 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:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Кому** откройте окно настройки фильтрации.
4. Введите один или несколько символов адреса электронной почты.
5. 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:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. По ссылке **Состояние** откройте окно настройки фильтрации.
4. Установите один или несколько флажков рядом со значениями состояний:
   - **Включено**.
   - **Отключено**.
5. 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:

1. В окне веб-интерфейса программы выберите раздел **Параметры**, подраздел **Уведомления**.
2. Перейдите на закладку **Правила уведомлений**.
3. Нажмите на кнопку справа от того заголовка столбца 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.

Управление программой Kaspersky Endpoint Agent для Windows

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

Взаимодействие программы с Kaspersky Anti Targeted Attack Platform выполняется с помощью компонента KATA Central Node. При настроенной интеграции Kaspersky Endpoint Agent с KATA Central Node, программа выполняет задачи и применяет настройки, поступающие от компонента KATA Central Node, а также отправляет на сервер с компонентом KATA Central Node данные телеметрии с защищаемого устройства.

Установка и удаление Kaspersky Endpoint Agent

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Agent на устройство, как обновить предыдущую версию программы и как удалить программу с устройства.

Подготовка к установке Kaspersky Endpoint Agent

Перед установкой Kaspersky Endpoint Agent на устройство или обновлением предыдущей версии программы проверьте следующие условия:

- выполнение аппаратных и программных требований;
- наличие прав на установку программного обеспечения.

Если какое-либо из перечисленных условий не выполнено, на экран выводится соответствующее уведомление.

Установка Kaspersky Endpoint Agent

Установка Kaspersky Endpoint Agent может быть выполнена:

- локально с помощью Мастера установки;
- локально с помощью командной строки;
- удаленно с помощью Kaspersky Security Center;
- удаленно с помощью редактора управления групповыми политиками Microsoft Windows (подробнее см. на сайте Службы технической поддержки Microsoft).

При удаленной установке параметры установки можно передать при помощи конфигурационного файла install_props.json. Для это необходимо предварительно разместить файл install_props.json в одной папке с файлом endpointagent.msi.

Локальная установка и удаление Kaspersky Endpoint Agent

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

Установка Kaspersky Endpoint Agent с помощью Мастера установки

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы.

Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы,

скопируйте файл endpointagent.msi, входящий в комплект поставки, на устройство пользователя и запустите его.

Запустится мастер установки программы.

После установки программы Kaspersky Endpoint Agent на устройство, мастер установки может быть запущен на этом устройстве в одном из следующих режимов:

- **Восстановление** (восстановить поврежденные модули программы).
- **Удаление** (удалить программу с устройства).

Удаление Kaspersky Endpoint Agent с помощью Мастера установки и удаления

Вы можете удалить Kaspersky Endpoint Agent стандартными средствами установки и удаления программ Microsoft Windows. Для удаления программы запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы.

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

Установка, восстановление и удаление программы с помощью командной строки

Kaspersky Endpoint Agent можно установить и удалить при помощи msi-пакета, задавая при этом значения свойств MSI стандартным образом. Подробная информация об использовании стандартных команд и ключей установщика Windows содержится в документации, предоставляемой корпорацией Microsoft.

Установка Kaspersky Endpoint Agent

Ниже приведен пример установки программы в неинтерактивном режиме с параметрами по умолчанию. После запуска установки программы в неинтерактивном режиме ваше участие в процессе установки не требуется.

Установка Kaspersky Endpoint Agent в неинтерактивном режиме требует принятия Лицензионного соглашения и Политики конфиденциальности. Используйте параметры `EULA=1` и `PRIVACYPOLICY=1`, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения и Политики конфиденциальности.

Пример:

```
msiexec /i endpointagent.msi EULA=1 PRIVACYPOLICY=1 USE_AZURE_SUPPORT=1 /qn
```

Параметры команды для установки Kaspersky Endpoint Agent

Параметр	Описание
`EULA`	Обязательный параметр. Параметр передает согласие или отказ от условий Лицензионного соглашения. Значения: • 0 – отказ; • 1 – согласие. Если передано значение 0, то установка программы не выполняется.
`PRIVACYPOLICY`	Обязательный параметр. Параметр передает согласие или отказ от условий Политики конфиденциальности. Значения: • 0 – отказ; • 1 – согласие. Если передано значение 0, то установка программы не выполняется.
`USE_AZURE_SUPPORT`	Параметр устанавливает признак использования идентификатора физического оборудования в виде значения параметра `EnableAzureSupport` HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment для операционных систем на платформе x86 или HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\SOYUZ\4.0\Environment для операционных систем на платформе x64. Значения: • 0 – Kaspersky Endpoint Agent при отправке событий на сервер сбора телеметрии в качестве значения sensor_id в отправляемых запросах серверу передает идентификатор ОС хоста из реестра. Значение по умолчанию. • 1 – Kaspersky Endpoint Agent при отправке событий на сервер сбора телеметрии в качестве значения sensor_id в отправляемых запросах серверу передает идентификатор BIOS хоста.

Восстановление Kaspersky Endpoint Agent

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

Пример:
```
msiexec /i endpointagent.msi REINSTALL=ALL /qn
```

Удаление Kaspersky Endpoint Agent

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

Пример:
```
msiexec /i {BB66A7B5-A5C0-45E6-92B9-D0B848B6F394} REMOVE=ALL /qn
```
Если программа защищена паролем:
```
msiexec /i {BB66A7B5-A5C0-45E6-92B9-D0B848B6F394} REMOVE=ALL UNLOCK_PASSWORD=<пароль> /qn
```

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

Установка Kaspersky Endpoint Agent с помощью Kaspersky Security Center

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

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

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

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

Создание инсталляционного пакета Kaspersky Endpoint Agent

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

Создание инсталляционного пакета в Консоли администрирования.

Чтобы создать инсталляционный пакет, выполните следующие действия:

1. В Консоли администрирования перейдите в папку **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Просмотреть актуальные версии программ "Лаборатории Касперского"**.

   Появится список текущих версий программ "Лаборатории Касперского".

3. Выберите инсталляционный пакет Kaspersky Endpoint Agent.

4. Нажмите на кнопку **Загрузить программу и создать инсталляционный пакет**.

   Инсталляционный пакет отображается в списке инсталляционных пакетов.

5. Чтобы изменить свойства инсталляционного пакета, в контекстном меню инсталляционного пакета выберите пункт **Свойства**.

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

   - папку для установки программы;
   - значение параметра восстановления программы;
   - значение параметра совместимости с Azure WVD;
   - параметры файла ключа для активации программы.

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

Создание инсталляционного пакета в Web Console и Cloud Console.

Чтобы создать инсталляционный пакет, выполните следующие действия:

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

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета.

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

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

4. Выберите инсталляционный пакет Kaspersky Endpoint Agent.

   Откроется окно с информацией об инсталляционном пакете.

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

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

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

      Дождитесь окончания загрузки файла.

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

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

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

   e. Следуйте дальнейшим указаниям мастера.

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

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

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

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

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

   - папку для установки программы;
   - значение параметра восстановления программы;
   - значение параметра совместимости с Azure WVD;
   - параметры файла ключа для активации программы.

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

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

Создание задачи удаленной установки Kaspersky Endpoint Agent

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

Создание задачи удаленной установки в Консоли администрирования.

Чтобы создать задачу удаленной установки, выполните следующие действия:

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

   Откроется список задач.

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

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

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

Шаг 2. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите инсталляционный пакет Kaspersky Endpoint Agent.

Вы можете изменить свойства инсталляционного пакета в Kaspersky Security Center.

Шаг 3. Дополнительно

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

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

Шаг 4. Параметры

Настройте следующие дополнительные параметры программы:

- **Принудительно загрузить инсталляционный пакет**. Выберите средства установки программы:
  - **С помощью Агента администрирования**. Если на компьютере не установлен Агент администрирования, то сначала Агент администрирования устанавливается средствами операционной системы. Далее Kaspersky Endpoint Agent устанавливается средствами Агента администрирования.
  - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в *Справке Kaspersky Security Center*.
  - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.
- **Поведение устройств, управляемых другими Серверами**. Выберите способ установки Kaspersky Endpoint Agent. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одной и той же программы на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.
- **Не устанавливать программу, если она уже установлена**. Снимите этот флажок, если вы хотите, например, установить программу более ранней версии.

Шаг 5. Выбор параметра перезагрузки операционной системы

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

Шаг 6. Выбор устройств, которым будет назначена задача

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

Шаг 7. Выбор учетной записи для запуска задачи

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

Шаг 8. Настройка расписания запуска задачи

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

Шаг 9. Определение названия задачи

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

Шаг 10. Завершение создания задачи

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

Создание задачи удаленной установки в Web Console и Cloud Console.

Чтобы создать задачу удаленной установки, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

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

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

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

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

Шаг 2. Выбор компьютеров для установки

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

Шаг 3. Настройка параметров инсталляционного пакета

На этом шаге настройте параметры инсталляционного пакета:

1. Выберите инсталляционный пакет Kaspersky Endpoint Agent.

2. Выберите инсталляционный пакет Агента администрирования.

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

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

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

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

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

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

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

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

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

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

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

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

Шаг 4. Выбор параметра перезагрузки операционной системы

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

Шаг 5. Выбор учетной записи для запуска задачи

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

Шаг 6. Завершение создания задачи

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

Установка средств администрирования Kaspersky Endpoint Agent

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

Установка и обновление плагина управления Kaspersky Endpoint Agent

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

Чтобы установить плагин управления Kaspersky Endpoint Agent,

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

Запустится мастер установки программы.

Обновление предыдущей установленной версии плагина управления Kaspersky Endpoint Agent

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

При установке плагина на устройство с установленной предыдущей версией плагина:

- Все значения параметров, включая политики, групповые и локальные задачи, переносятся в новую версию плагина, а предыдущая установленная версия плагина автоматически удаляется.
- Параметры Kaspersky Endpoint Agent, которые были недоступны в предыдущей версии плагина, доступны к настройке и имеют значения по умолчанию.

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

- Шаблоны политик, созданные в предыдущей версии плагина, доступны в новой версии плагина.

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

Установка и обновление веб-плагина управления Kaspersky Endpoint Agent

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

Вы можете установить веб-плагин следующими способами:

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

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

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

Обновление предыдущей установленной версии веб-плагина управления Kaspersky Endpoint Agent

При установке плагина на устройство с установленной предыдущей версией плагина:

- Все значения параметров, включая политики, групповые и локальные задачи, переносятся в новую версию плагина, а предыдущая установленная версия плагина автоматически удаляется.
- Параметры Kaspersky Endpoint Agent, которые были недоступны в предыдущей версии плагина, доступны к настройке и имеют значения по умолчанию.

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

- Шаблоны политик, созданные в предыдущей версии плагина, доступны в новой версии плагина.

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

Обновление предыдущей версии Kaspersky Endpoint Agent

Обновление Kaspersky Endpoint Agent доступно только для версий 3.8 и выше. Обновление возможно для версий программы, установленных в составе программ Endpoint Protection Platform и установленных отдельно. Обновление выполняется путем установки новой версии.

При обновлении Kaspersky Endpoint Agent действующая лицензия автоматически применится к Kaspersky Endpoint Agent . Срок действия лицензии остается без изменений. При обновлении программы с истекшим сроком действия лицензии новая версия программы после установки работает в режиме ограниченной функциональности.

Если срок действия лицензии обновляемой версии истек, вы можете добавить лицензионный ключ прямо во время обновления. Можно передать файл ключа одним из указанных способов.

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

Если вы устанавливаете Kaspersky Endpoint Agent на устройство с установленной предыдущей версией Kaspersky Endpoint Agent, для подключения к Kaspersky Security Center и перенесения данных предыдущей версии в новую версию необходимо создать учетную запись. Для учетной записи используется логин по умолчанию AutoIOC_Admin и пароль, заданный пользователем.

При обновлении предыдущей версии Kaspersky Endpoint Agent, защищенной паролем, необходимо передать установщику этот пароль одним из следующих способов:

- При установке локально через интерфейс Мастера установки или в интерактивном режиме через командную строку указать пароль на соответствующем шаге.
- При установке локально через командную строку в неинтерактивном режиме указать пароль в качестве значения ключа `UNLOCK_PASSWORD`.
- При установке удаленно через Kaspersky Security Center передать текущий пароль в параметрах инсталляционного пакета.

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

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

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

При установке плагина на устройство с установленной предыдущей версией плагина:

- Все значения параметров, включая политики, групповые и локальные задачи, переносятся в новую версию плагина, а предыдущая установленная версия плагина автоматически удаляется.
- Параметры Kaspersky Endpoint Agent, которые были недоступны в предыдущей версии плагина, доступны к настройке и имеют значения по умолчанию.

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

- Шаблоны политик, созданные в предыдущей версии плагина, доступны в новой версии плагина.

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

Восстановление Kaspersky Endpoint Agent

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

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

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

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

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

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

Изменения в системе после установки Kaspersky Endpoint Agent

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

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

Папки Kaspersky Endpoint Agent на защищаемом устройстве

При установке Kaspersky Endpoint Agent на устройстве создаются следующие папки:

- Заданная по умолчанию папка установки Kaspersky Endpoint Agent, содержащая исполняемые файлы Kaspersky Endpoint Agent:
  - В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\
  - В 64-х разрядной версии Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\
- Папка, содержащая драйверы Kaspersky Endpoint Agent(x86):
  - В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\drivers\<версия_ОС>\<имя драйвера>
  - В 64-х разрядной версии Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\drivers\x64\<версия ОС>\<имя драйвера>
- Папки, содержащие файлы IOC:
  - В 32-х разрядной версии Microsoft Windows:
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.1
  - В 64-х разрядной версии Microsoft Windows:
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.1

- Папки, содержащие служебные файлы Kaspersky Endpoint Agent:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Images
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kata
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kmp
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Syslog
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Hunts
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\killchain
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Settings
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Tasks
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\DSKM
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp\Tasks
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Bases
- Папка, содержащая служебные файлы для работы с Kaspersky Security Network.
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Ksn
- Папка, содержащая файлы, помещенные на карантин:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Quarantine
- Папка, содержащая файлы, восстановленные из карантина:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Restored
- Папка, содержащая файлы конфигурации политики Kaspersky Security Center:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Policy
- Папки, содержащие служебные файлы для работы с Kaspersky Sandbox:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox\Queue

- Папка, содержащая файлы обновляемых компонентов:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Update
- Папка, содержащая файлы ярлыков для меню Пуск:
  - %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Kaspersky Endpoint Agent

Службы и драйверы Kaspersky Endpoint Agent

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

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

Следующие драйверы Kaspersky Endpoint Agent регистрируются на устройстве:

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

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

Ключи системного реестра

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

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

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdDispl
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdVersi
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\NagentMi

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\ProductCode
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\NoPPL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\BFESDDL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EnableKillChain]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\SvmUpdateMode]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\MsiPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\AgentPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EventsExpirationTimeout]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallTime]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLCID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLocalization]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallPlatformType]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\Version]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration(Example)]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\StartMenu]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\UninstallShortcut2]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\RelNotes]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\License]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Ksn]

- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Kmp]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\ProductUrl]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\angara]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncap]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncapxp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klsnsr]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vostok]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\soyuz]

Активация Kaspersky Endpoint Agent

Этот раздел содержит информацию об активации Kaspersky Endpoint Agent.

Управление активацией Kaspersky Endpoint Agent

Вы можете активировать Kaspersky Endpoint Agent одним из следующих способов:

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

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

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

При обновлении Kaspersky Endpoint Agent действующая лицензия автоматически применится к Kaspersky Endpoint Agent . Срок действия лицензии остается без изменений. При обновлении программы с истекшим сроком действия лицензии новая версия программы после установки работает в режиме ограниченной функциональности.

Если срок действия лицензии обновляемой версии истек, вы можете добавить лицензионный ключ прямо во время обновления. Можно передать файл ключа одним из указанных способов.

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

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

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

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

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

Функциональные ограничения после окончания срока действия лицензии

Когда заканчивается срок действия текущей лицензии, возникают следующие ограничения в работе функциональных компонентов Kaspersky Endpoint Agent:

- Прекращается сбор телеметрии.
- Невозможно включить сетевую изоляцию.

  Если сетевая изоляция была включена на момент окончания срока действия лицензии, программа отключает сетевую изоляцию в соответствии с заданными параметрами автоматического отключения сетевой изоляции.
- Невозможно включить функцию Запрет запуска.

  Если функция Запрет запуска была включена на момент окончания срока действия лицензии, программа прекращает блокирование объектов, которые подпадают под заданные правила запрета.
- Останавливаются и становятся недоступными для запуска следующие задачи: Запустить процесс, Завершить процесс, Удалить файл.
- Останавливаются и становятся недоступными для запуска стандартные задачи поиска IOC.
- Прекращается использование KSN/KPSN.

При попытке использования перечисленных функциональных компонентов программы после окончания срока действия лицензии программа записывает критическое событие `LicenseViolation` в журнал событий Windows и в журнал Сервера администрирования Kaspersky Security Center. При работе через командную строку, программа возвращает код `8` (`AccessDenied`).

Просмотр информации о действующей лицензии

Информацию о действующей лицензии можно посмотреть в Kaspersky Security Center в разделе **Лицензии "Лаборатории Касперского"** или в свойствах устройства в разделе **Ключи**. Подробную информацию об управлении ключами с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Чтобы посмотреть информацию о действующей лицензии в Консоли администрирования Kaspersky Security Center:

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

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

   В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
6. Выберите программу Kaspersky Endpoint Agent и откройте окно ее свойств одним из следующих способов:

   - Двойным щелчком мыши по названию программы.
   - В контекстном меню программы выберите пункт **Свойства**.
   - Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".
7. Выберите раздел **Ключи**.

Информация о действующей лицензии отобразится в рабочей области окна.

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

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

Отобразится основная информация об активных и резервных лицензионных ключах.

Управление Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center

Программа Kaspersky Security Center предназначена для централизованного решения основных задач управления и обслуживания системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Agent, настраивать параметры работы программы, запускать и останавливать задачи программы. В Kaspersky Security Center предусмотрено разграничение прав доступа к Kaspersky Endpoint Agent, реализованное на основе технологии управления доступом на основе ролей (Role Based Access Control, RBAC).

Подробную информацию о Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

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

Вы можете управлять Kaspersky Endpoint Agent в Консоли администрирования Kaspersky Security Center с помощью плагина управления Kaspersky Endpoint Agent.

Далее в разделе приведена основная информация об управлении Kaspersky Endpoint Agent с помощью Консоли администрирования Kaspersky Security Center.

Управление политиками Kaspersky Endpoint Agent

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

Создание политики Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы создать политику Kaspersky Endpoint Agent в Kaspersky Security Center:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.

3. Нажмите на кнопку **Создать политику**.

   Запустится мастер создания политики.

4. В окне **Выбор программы для создания групповой политики** выберите Kaspersky Endpoint Agent.

5. Нажмите на кнопку **Далее**.

6. В окне **Ввод названия групповой политики** выполните следующие действия:

   a. Введите имя, под которым создаваемая политика будет отображаться в списке политик.

   b. Если вы хотите импортировать параметры существующей политики Kaspersky Endpoint Agent в новую политику:

      1. Установите флажок **Использовать параметры политики для предыдущей версии программы**.

      2. Нажмите на кнопку **Выбрать** и в открывшемся окне выберите политику, параметры которой требуется импортировать.

      3. Нажмите на кнопку **ОК**.

   c. Нажмите на кнопку **Далее**.

7. В окне **Создать политику** выберите один из следующих вариантов:

   - **Создать новую политику и настроить параметры**.
   - **Создать новую политику с параметрами по умолчанию**.

   Если на предыдущем шаге вы включили параметр **Использовать параметры политики для предыдущей версии программы**, то по умолчанию выбирается вариант **Создать новую политику и настроить параметры**, а в процессе создания политики отображаются параметры, заданные в импортируемой политике. В этом случае положение переключателя применения политики в правом верхнем углу каждого из разделов с параметрами зависит от положения переключателей в блоках параметров импортируемой политики.

8. Нажмите на кнопку **Далее**.

9. В окне **Выбрать тип политики** выберите необходимый способ развертывания Kaspersky Endpoint Agent:

   - **Интеграция с Kaspersky Sandbox**
   - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks**

10. Нажмите на кнопку **Далее**.

11. Если вы выбрали вариант **Создать новую политику и настроить параметры**, выполните одно из следующих действий во всех последовательно отображающихся окнах с параметрами:

    - Чтобы настроить параметры программы из отображаемых разделов во время создания политики:

        a. Нажмите на кнопку **Настроить** рядом с названием необходимого раздела.

        b. В открывшемся окне настройте необходимые параметры и нажмите на кнопку **OK.**

        c. Нажмите на кнопку **Далее**.

    - Чтобы настроить параметры программы из отображаемых разделов позднее, нажмите на кнопку **Далее**.

    Настройка параметров программы состоит из следующих этапов:

    > Состав этапов зависит от выбранного на предыдущем шаге типа политики и может отличаться от приведенного ниже.

    - Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Sandbox.
    - Настройка интеграции Kaspersky Endpoint Agent с компонентами Endpoint Detection and Response Expert (KATA EDR) и Kaspersky Industrial CyberSecurity for Networks (KICKS for Networks).
    - Настройка параметров реагирования на угрозы.
    - Настройка репозиториев программы.
    - Настройка параметров безопасности программы.
    - Настройка общих параметров программы.

12. В окне **Целевая группа** выберите группу администрирования Kaspersky Security Center, на которую должна распространяться создаваемая политика, выполнив следующие действия:

    a. Нажмите на кнопку **Обзор**.

    Откроется окно выбора группы администрирования.

    b. Выберите группу администрирования в списке.

    Например, вы можете выбрать группу **Управляемые устройства**.

    c. Если вы хотите создать подгруппу устройств в группе **Управляемые устройства**:

        1. Нажмите на кнопку **Новая группа**.

        2. В открывшемся окне введите имя подгруппы устройств.

        3. Нажмите на кнопку **OK**.

    d. Нажмите на кнопку **Далее**.

13. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:

    - **Активная политика**, чтобы политика начала действовать сразу после создания.
    - **Неактивная политика**, чтобы активировать политику позже.
    - **Политика для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организаций.

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

15. Нажмите на кнопку **Готово**.

    Созданная политика отобразится в списке политик.

Включение параметров в политике Kaspersky Endpoint Agent

При настройке параметров политики Kaspersky Endpoint Agent по умолчанию значения параметров сохраняются, но не применяются до тех пор, пока вы их не включите. Параметры в разделах политики разделены на блоки. В рамках одной политики вы можете включить как часть блоков, так и все блоки.

Чтобы включить блок параметров в политике Kaspersky Endpoint Agent:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

    - Двойным щелчком мыши по названию политики.
    - В контекстном меню политики выберите пункт **Свойства**.
    - В правой части окна выберите пункт **Настроить параметры политики**.

4. Выберите политику, для которой вы хотите включить параметры.
5. В открывшемся окне выберите раздел и блок параметров, к которым относятся нужные параметры.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

    Все параметры блока будут применяться в политике после сохранения изменений.

Настройка параметров Kaspersky Endpoint Agent

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

Открытие окна параметров Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы открыть окно параметров Kaspersky Endpoint Agent:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
3. Выберите группу администрирования, для которой требуется настроить параметры программы.
4. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>** двойным щелчком мыши по названию политики или выбрав пункт **Свойства** в контекстном меню.
   - Чтобы настроить параметры программы для отдельного устройства, выберите закладку **Устройства** и выполните следующие действия:
     a. Откройте окно **Свойства: <Название устройства>** двойным щелчком мыши по названию устройства или выбрав пункт **Свойства** в контекстном меню.
     b. Выберите раздел **Программы**.
     c. Откройте окно **Параметры: <Название программы>** двойным щелчком мыши по названию программы в рабочей области окна или нажав на кнопку **Свойства** под списком программ.

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**, кроме параметров сетевой изоляции.

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

Настройка параметров безопасности Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Настройка прав пользователей

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете предоставить доступ к Kaspersky Endpoint Agent отдельным пользователям или группам пользователей. В результате только заданные пользователи смогут управлять параметрами или службами программы.

Чтобы настроить права пользователей:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
5. В блоке параметров **Права пользователей** нажмите на кнопку **Настроить** рядом с названием нужного параметра.

   Откроется окно разрешений для группы Kaspersky Endpoint Agent.
6. В верхнем блоке параметров групп или пользователей выберите группу или пользователя, которому вы хотите предоставить права.
7. В нижнем блоке параметров разрешений для групп или пользователей установите флажки в строках с требуемыми правами.
8. Нажмите на кнопку **OK**.

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

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

Права пользователей на управление параметрами и службами программы настроены и применены.

Включение защиты паролем

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Неограниченный доступ пользователей к программе и ее параметрам может привести к снижению уровня безопасности устройства. Защита паролем позволяет ограничить доступ пользователей к программе.

Чтобы включить защиту паролем:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли откройте папку **Политики**.

3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.

4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.

5. В блоке параметров **Защита паролем** установите флажок **Применить защиту паролем**.

6. Задайте пароль и подтвердите его.

   Мы рекомендуем задать пароль, который удовлетворяет следующим условиям:

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

- цифры (0-9);
- специальные символы (!$#%).

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

Защита паролем будет включена. При попытке пользователя выполнить действие, защищенное паролем, программа предложит пользователю ввести пароль.

Программа не проверяет надежность заданного пароля. Мы рекомендуем использовать сторонние средства для проверки надежности пароля. Пароль считается надежным, если по результатам проверки подтверждена невозможность подбора пароля минимум за 6 месяцев.

Программа не блокирует возможность ввода пароля после множества попыток ввода некорректного пароля.

Включение и отключение механизма самозащиты

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Для защиты от вредоносных программ, которые пытаются заблокировать работу Kaspersky Endpoint Agent или удалить программу, в программе реализован механизм самозащиты. Этот механизм предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

Чтобы включить или отключить механизм самозащиты:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.

5. В блоке параметров **Самозащита** включите или выключите параметр **Включить самозащиту модулей программы в памяти**.

   По умолчанию параметр включен.

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

7. Нажмите на кнопку **ОК**.

Механизм самозащиты будет включен или отключен.

Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

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

Чтобы настроить параметры соединения с прокси-сервером:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли откройте папку **Политики**.

3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.

4. В разделе **Параметры программы** выберите подраздел **Общие параметры**.

5. Выберите один из следующих вариантов использования прокси-сервера:

   - **Не использовать прокси-сервер**.
   - **Автоматически определять адрес прокси-сервера.**
   - **Использовать прокси-сервер с указанными параметрами**.

6. Если вы выбрали вариант **Автоматически определять адрес прокси-сервера**, прокси-сервер определяется автоматически для дальнейшей передачи телеметрии.

7. Если вы выбрали вариант **Использовать прокси-сервер с указанными параметрами**, в полях **Имя или IP-адрес сервера** и **Порт** введите адрес и порт прокси-сервера, соединение с которым вы хотите установить.

   По умолчанию используется порт 8080.

8. Если вы хотите использовать NTLM-аутентификацию (протокол сетевой аутентификации NT LAN Manager) при подключении к прокси-серверу:

   a. Установите флажок **Использовать NTLM-аутентификацию по имени пользователя и паролю**.

   b. В поле **Имя пользователя** введите имя пользователя из учетной записи, которая будет использоваться для авторизации на прокси-сервере.

   c. В поле **Пароль** введите пароль подключения к прокси-серверу.

      Вы можете включить отображение символов пароля, нажав на кнопку **Показать** справа от поля **Пароль**.

9. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.

10. Нажмите на кнопку **Применить**.

    При этом вы вернетесь в окно свойств политики.

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

12. Нажмите на кнопку **ОК**.

Параметры соединения с прокси-сервером настроены.

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

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли откройте папку **Политики**.

3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.

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

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

Настройка использования KSN в Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Agent использует данные, полученные от пользователей во всем мире. Сеть Kaspersky Security Network предназначена для получения этих данных.

Kaspersky Security Network (далее также KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программы EPP на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, информация о которых еще не вошла в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы.

Во время участия в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Endpoint Agent, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

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

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

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

Чтобы включить использование KSN:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. Выберите раздел **Kaspersky Security Network**.
5. Ознакомьтесь с Положением о KSN.
6. Если вы согласны с условиями Положения, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Положения о KSN**.
7. Установите флажок **Включить использование Kaspersky Security Network ("KSN")**.
8. Если вы хотите использовать Kaspersky Security Center в качестве посредника для передачи телеметрии, установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.
9. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
10. Нажмите на кнопку **OK**.

Использование KSN будет включено.

Настройка интеграции Kaspersky Endpoint Agent с KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с компонентом KATA Central Node с помощью Консоли администрирования Kaspersky Security Center.

Настройка параметров передачи данных

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры передачи данных:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Серверы сбора телеметрии** выберите подраздел **Общие параметры**.
5. В блоке параметров **Параметры передачи данных** выполните следующие действия:
   - Укажите значения в поле **Максимальное время передачи событий (сек.)**.

     По умолчанию задано 30 секунд.
   - Укажите значения в поле **Максимальное количество событий в одном пакете**.

     По умолчанию задано 1024 событий в одном пакете.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.
7. Нажмите на кнопку **OK**.

Настройка параметров регулирования количества запросов

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Чтобы настроить параметры регулирования количества запросов:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Серверы сбора телеметрии** выберите подраздел **Общие параметры**.
5. В блоке параметров **Регулирование количества запросов** вы можете выполнить следующие действия:
   - Включить или выключить параметр **Включить регулирование количества запросов**.

     По умолчанию параметр включен.
   - Указать количество событий в поле **Максимальное количество событий в час**.

     Программа анализирует поток данных телеметрии и ограничивает передачу событий низкой важности, если поток передаваемых событий стремится превысить указанную в этом поле величину. По умолчанию задано 3000 событий в час.
   - Указать порог потока однотипных событий низкой важности в поле **Процент превышения лимита событий**.

     Если поток однотипных событий низкой важности превысит указанный в этом поле порог в процентах от общего количества событий, то именно этот тип событий будет ограничен. Можно задать величину от 5% до 100%. По умолчанию задано 15%.
6. В правом верхнем углу блока параметров измените положение переключателя с **Политика не применяется** на **Политика применяется**.

   По умолчанию переключатель находится в положении **Политика применяется**.
7. Нажмите на кнопку **OK**.

Включение и отключение интеграции с KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы используете Nginx в качестве прокси-сервера между устройством с Kaspersky Endpoint Agent и сервером KATA, настройте параметр `client_max_body_size:` значение параметра `client_max_body_size` должно быть равно максимальному размеру объекта, отправляемого программой Kaspersky Endpoint Agent на обработку в KATA. Иначе Nginx не будет пропускать объекты, размер которых превышает установленное значение. Значение по умолчанию – 1 МБ.

Чтобы включить или отключить интеграцию с компонентом KATA Central Node:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Серверы сбора телеметрии** выберите подраздел **Интеграция с KATA**.
5. В блоке **Параметры подключения** выполните одно из следующих действий:
   - Чтобы включить интеграцию с KATA Central Node:
     a. Установите флажок **Включить интеграцию с KATA**.
     b. В блоке параметров **Список серверов KATA** для одного или нескольких серверов KATA укажите IP-адрес или полное доменное имя сервера KATA, а также порт подключения к серверу.

        Kaspersky Endpoint Agent подключается к первому серверу из списка. Если подключение не удается, Kaspersky Endpoint Agent подключается ко второму серверу и так далее по списку.
   - Чтобы отключить интеграцию с KATA Central Node, снимите флажок **Включить интеграцию с KATA**.
6. В блоке параметров **Параметры подключения** включите или выключите параметр **Подключаться через прокси-сервер, если это задано в общих параметрах**.

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

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

8. Нажмите на кнопку **OK**.

Интеграция с KATA Central Node будет включена или отключена.

Настройка доверенного соединения с KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить доверенное соединение Kaspersky Endpoint Agent с KATA Central Node, выполните следующие действия на стороне Kaspersky Endpoint Agent:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли откройте папку **Политики**.

3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.

4. В разделе **Серверы сбора телеметрии** выберите подраздел **Интеграция с KATA**.

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

6. Нажмите на кнопку **Добавить TLS-сертификат**.

   Откроется окно **Добавление TLS-сертификата**.

7. Выполните одно из следующих действий по добавлению TLS-сертификата:

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

В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера KATA. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

8. Нажмите на кнопку **Добавить**.

   Информация о добавленном TLS-сертификате отобразится в блоке параметров **Данные TLS-сертификата**.

9. Если вы хотите настроить дополнительную защиту подключения с использованием пользовательского сертификата, нажмите на кнопку **Добавить сертификат клиента**.

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

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

    b. Нажмите на кнопку **Загрузить**, в открывшемся окне выберите архив формата PFX и нажмите на кнопку **Открыть**.

    c. Введите пароль к архиву формата PFX.

    d. Нажмите на кнопку **ОК**.

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

12. Нажмите на кнопку **ОК**.

Доверенное соединение с сервером KATA будет настроено.

Настройка параметров синхронизации Kaspersky Endpoint Agent с KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры синхронизации Kaspersky Endpoint Agent с KATA Central Node:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли откройте папку **Политики**.

3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.

4. В разделе **Серверы сбора телеметрии** выберите подраздел **Интеграция с KATA**.

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

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

   - **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)**. Укажите период отправки запросов на синхронизацию параметров и задач Kaspersky Endpoint Agent с KATA Central Node. Можно указать значение в пределе от 1 до 60 минут. По умолчанию задано 5 минут.

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

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

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

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

7. Нажмите на кнопку **OK**.

Настройка параметров EDR-телеметрии

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе содержится информация о том, как настроить:

- Исключения EDR-телеметрии о процессах программ, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.

- Оптимизацию объема EDR-телеметриии, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом Kaspersky Industrial CyberSecurity for Networks.

- Исключения EDR-телеметрии о сетевых коммуникациях, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом Kaspersky Industrial CyberSecurity for Networks.

Включение и настройка исключений и оптимизации объема отправляемой EDR-телеметрии о процессах программ

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить исключения и оптимизацию объема отправляемой EDR-телеметрии о процессах программ с помощью Консоли администрирования Kaspersky Security Center в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии о процессах программ доступны при интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks данные об исключенных процессах программ.

Управление (включение / выключение) оптимизацией объема отправляемой EDR-телеметрии о процессах программ доступно при интеграции Kaspersky Endpoint Agent с серверами с установленным Kaspersky Industrial CyberSecurity for Networks.

Если включена оптимизация объема отправляемой EDR-телеметрии, Kaspersky Endpoint Agent не отправляет события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и Агента администрирования klnagent.exe о процессах программ на сервер с установленным Kaspersky Industrial CyberSecurity for Networks.

Чтобы включить и настроить исключения и оптимизацию объема отправляемой EDR-телеметрии о процессах программ:

1. Выполните одно из следующих действий:

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

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

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

        В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
     6. Выберите программу Kaspersky Endpoint Agent и откройте окно ее свойств одним из следующих способов:

        - Двойным щелчком мыши по названию программы.
        - В контекстном меню программы выберите пункт **Свойства**.
        - Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".

- **Откройте окно свойств политики программы**.

  1. Откройте Консоль администрирования Kaspersky Security Center.
  2. В дереве консоли откройте папку **Политики**.
  3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

     - Двойным щелчком мыши по названию политики.
     - В контекстном меню политики выберите пункт **Свойства**.
     - В правой части окна выберите пункт **Настроить параметры политики**.

2. Перейдите в раздел **EDR-телеметрия → Исключенные процессы**.
3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.
4. Настройте оптимизацию объема отправляемой EDR-телеметрии:

   При интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node оптимизация объема отправляемой EDR-телеметрии должна быть всегда включена.

   - Выключите параметр **Оптимизировать объем отправляемой телеметрии**, если хотите, чтобы Kaspersky Endpoint Agent отправляла события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB, службы WinRM и процесса Агента администрирования klnagent.exe.
   - Включите параметр **Оптимизировать объем отправляемой телеметрии**, если хотите, чтобы Kaspersky Endpoint Agent не отправляла события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и Агента администрирования klnagent.exe.

   Если параметр **Использовать исключения** выключен, Kaspersky Endpoint Agent не отправляет события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и процесса Агента администрирования klnagent.exe вне зависимости от значения параметра **Оптимизировать объем отправляемой телеметрии**.

5. Создайте список исключений:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Свойства правила настройте параметры исключения**.

      Параметры исключения применяются по правилу логического И.

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

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

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

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

     Этот тип события выбран по умолчанию.
   - **Загрузка модуля процесса**.
   - **Изменения в реестре**.

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

Новое исключение создано и отображается в списке.

d. Если необходимо экспортировать список исключений в файл формата XML, нажмите на кнопку **Экспорт**.

e. Если необходимо испортировть список исключений из файла формата XML, нажмите на кнопку **Импорт**.

f. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.

g. Если необходимо удалить исключение из списка, выберите исключение и нажмите на кнопку **Удалить**.

6. Если вы настраиваете параметры политики, убедитесь, что переключатель в правом верхнем углу блока параметров находится в активном положении. Переключатель находится в этом положении по умолчанию.

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

Включение и настройка исключений отправляемой EDR-телеметрии о сетевых коммуникациях

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить исключения отправляемой EDR-телеметрии о сетевых коммуникациях с помощью Консоли администрирования Kaspersky Security Center в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии о сетевых коммуникациях применимы при интеграции Kaspersky Endpoint Agent с серверами с установленным Kaspersky Industrial CyberSecurity for Networks.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks данные, подпадающие под параметры исключений.

Чтобы включить и настроить исключения отправляемой EDR-телеметрии о сетевых коммуникациях:

1. Выполните одно из следующих действий:

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

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

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

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

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

        Откроется окно свойств устройства.

    5. Выберите раздел **Программы**.

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

6. Выберите программу Kaspersky Endpoint Agent и откройте окно ее свойств одним из следующих способов:

   - Двойным щелчком мыши по названию программы.
   - В контекстном меню программы выберите пункт **Свойства**.
   - Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".

- **Откройте окно свойств политики программы**.

  1. Откройте Консоль администрирования Kaspersky Security Center.
  2. В дереве консоли откройте папку **Политики**.
  3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

     - Двойным щелчком мыши по названию политики.
     - В контекстном меню политики выберите пункт **Свойства**.
     - В правой части окна выберите пункт **Настроить параметры политики**.

2. Перейдите в раздел **EDR-телеметрия** → **Исключенные сетевые коммуникации**.
3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.
4. Создайте список исключений:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Свойства правила настройте параметры исключения.**

   > Параметры исключения применяются по правилу логического И.

   1. В поле **Имя** введите название исключения.
   2. В раскрывающемся списке **Направление** выберите направление сетевого трафика.
   3. В раскрывающемся списке **Протокол** выберите сетевой протокол передачи данных.
   4. Если вы выбрали пользовательский протокол, в поле **Номер** введите номер сетевого протокола.
   5. Установите флажок **Локальный порт ИЛИ диапазон** и введите номер порта или диапазон номеров.

      Для входящих подключений (в раскрывающемся списке **Направление** выбрано **Входящее**) введите порт или диапазон портов для локального устройства.

      Для исходящих подключений (в раскрывающемся списке **Направление** выбрано **Исходящее**) введите порт или диапазон портов для удаленного устройства.

      Для номера порта доступны значения 1–65535.

Для диапазона портов доступны значения 1–10, 20–30000 и 1–65535.

Ограничения:

- Для сетевых подключений локального устройства с операционной системой Windows XP можно указать только один порт, поскольку в Windows XP не поддерживается диапазон портов.
- Для сетевых подключений удаленного устройства с операционной системой Windows XP можно указать диапазон портов, но правило применяется только к первому порту заданного диапазона, поскольку в Windows XP не поддерживается диапазон портов.

6. Установите флажок **Удаленный порт ИЛИ диапазон** и введите номер порта или диапазон номеров.

   Для входящих подключений (в раскрывающемся списке **Направление** выбрано **Входящее**) введите порт или диапазон портов для удаленного устройства.

   Для исходящих подключений (в раскрывающемся списке **Направление** выбрано **Исходящее**) введите порт или диапазон портов для локального устройства.

   Для номера порта доступны значения 1–65535.

   Для диапазона портов доступны значения 1–10, 20–30000 и 1–65535.

   Ограничения:

   - Для сетевых подключений локального устройства с операционной системой Windows XP можно указать только один порт, поскольку в Windows XP не поддерживается диапазон портов.
   - Для сетевых подключений удаленного устройства с операционной системой Windows XP можно указать диапазон портов, но правило применяется только к первому порту заданного диапазона, поскольку в Windows XP не поддерживается диапазон портов.

7. Установите флажок **Локальный адрес** и введите сетевой адрес устройства, для которого Kaspersky Endpoint Agent не будет анализировать и передавать EDR-телеметрию сетевого трафика в соответствии с параметрами исключения.

   Для входящих подключений (в раскрывающемся списке **Направление** выбрано **Входящее**) введите сетевой адрес для локального устройства.

   Для исходящих подключений (в раскрывающемся списке **Направление** выбрано **Исходящее**) введите сетевой адрес для удаленного устройства.

   > Для IP-адресов поддерживается только формат IPv4.

8. Установите флажок **Удаленный адрес** и введите сетевой адрес устройства, для которого Kaspersky Endpoint Agent не будет анализировать и передавать EDR-телеметрию сетевого трафика в соответствии с параметрами исключения.

   Для входящих подключений (в раскрывающемся списке **Направление** выбрано **Входящее**) введите сетевой адрес для удаленного устройства.

Для исходящих подключений (в раскрывающемся списке **Направление** выбрано **Исходящее**) введите сетевой адрес для локального устройства.

Для IP-адресов поддерживается только формат IPv4.

9. **Сформируйте список программ,** для которых Kaspersky Endpoint Agent не будет анализировать и передавать EDR-телеметрию сетевого трафика в соответствии с параметрами исключения.

    1. Установите флажок **Программы**.
    2. В поле ниже укажите путь к исполняемому файлу программы, которую вы хотите добавить в список. Вы можете ввести путь вручную или с помощью кнопки **Обзор**.
    3. Нажмите на кнопку **Добавить**.
    4. Повторите пункты 2 и 3 инструкции для каждой программы, которую вы хотите добавить в список.
    5. Если необходимо удалить програму из списка:
        a. Выделите программу в списке.
        b. Нажмите на кнопку **Удалить**.

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

    Новое исключение создано и отображается в списке.

c. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.

d. Если необходимо удалить исключение, выберите исключение и нажмите на кнопку **Удалить**.

5. Если вы настраиваете параметры политики, убедитесь, что положение переключателя в правом верхнем углу блока параметров находится в активном положении. Переключатель находится в этом положении по умолчанию.

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

Настройка параметров хранилищ в Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

О карантине Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Карантин – это специальное локальное хранилище на устройстве. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

По умолчанию локальное хранилище карантина расположено в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Quarantine`. По умолчанию объекты, восстановленные из карантина, хранятся в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Restored`.

Kaspersky Security Center формирует общий список объектов, помещенных на карантин на устройствах с программой Kaspersky Endpoint Agent. Агенты администрирования устройств передают информацию о файлах на карантине на Сервер администрирования.

Агент администрирования Kaspersky Security Center не копирует файлы из карантина на Сервер администрирования . Все объекты находятся на защищаемых устройствах с программой Kaspersky Endpoint Agent. Восстановление объектов из карантина также выполняется на защищаемых устройствах.

Об управлении карантином в Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Через Kaspersky Security Center можно настраивать параметры карантина, просматривать свойства объектов, находящихся на карантине на защищаемых устройствах, удалять объекты, находящиеся на карантине, а также восстанавливать объекты из карантина. Подробную информацию об управлении объектами, находящимися на карантине, через Kaspersky Security Center см. в документации Kaspersky Security Center.

Для того чтобы Kaspersky Endpoint Agent отправлял данные об объектах, помещенных на карантин, на Сервер администрирования Kaspersky Security Center, необходимо включить эту опцию в параметрах карантина в политике Kaspersky Endpoint Agent. По умолчанию опция включена.

Через интерфейс командной строки на устройстве можно просматривать информацию о параметрах карантина и свойствах объектов, находящихся на карантине.

Kaspersky Endpoint Agent помещает объект на карантин под системной учетной записью (SYSTEM).

Удаление объектов, помещенных на карантин, через командную строку доступно только под локальной учетной записью пользователя защищаемого устройства.

Настройка параметров карантина и восстановления объектов из карантина

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры карантина:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:
   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.
4. В разделе **Репозитории** выберите подраздел **Карантин**.
5. В разделе **Параметры Карантина** настройте параметры карантина:
   a. В поле **Папка Карантина** укажите путь, по которому будет создана папка карантина на устройствах, или нажмите на кнопку **Обзор** и выберите путь.

      По умолчанию используется путь `%SOYUZAPPDATA%\Quarantine\`. Папка Quarantine будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

      Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent. Например, если программа Kaspersky Endpoint Agent установлена на диске C, путь к папке карантина будет следующим: C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Quarantine.

   b. Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер Карантина (МБ)** и укажите или выберите в списке максимальный размер карантина в МБ.

      Например, вы можете задать максимальный размер карантина 200 МБ.

      При достижении максимального размера карантина Kaspersky Endpoint Agent публикует соответствующее событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

   c. Чтобы задать пороговое значение карантина (место в карантине, оставшееся до достижения максимального размера карантина), установите флажок **Пороговое значение места на диске (МБ)**.

      Например, вы можете задать пороговое значение карантина 50 МБ.

      При достижении порогового значения карантина, Kaspersky Endpoint Agent публикует соответствующее событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

6. В разделе **Восстановление объектов из Карантина** в поле **Папка для восстановленных объектов** укажите путь, по которому будет создана папка для объектов, восстановленных из карантина.

   По умолчанию используется путь `%SOYUZAPPDATA%\Restored\`. Папка Restored будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

   Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent. Например, если программа Kaspersky Endpoint Agent установлена на диске C, путь к папке восстановленных из карантина объектов будет следующим: C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored.

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

8. Нажмите на кнопку **Применить** и затем на кнопку **ОК**.

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

Настройка синхронизации данных с Сервером администрирования

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить синхронизацию данных об объектах, помещенных на карантин на управляемых устройствах, с Сервером администрирования Kaspersky Security Center. Синхронизация данных нужна для управления карантином через Kaspersky Security Center.

Чтобы настроить синхронизацию данных с Сервером администрирования:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли откройте папку **Политики**.

3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

   - Двойным щелчком мыши по названию политики.
   - В контекстном меню политики выберите пункт **Свойства**.
   - В правой части окна выберите пункт **Настроить параметры политики**.

4. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.

5. В разделе **Параметры**, в подразделе **Отправлять следующие данные на Сервер администрирования** установите флажок **Данные об объектах в Карантине на управляемых устройствах**.

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

7. Нажмите на кнопку **Применить** и затем на кнопку **ОК**.

Синхронизация данных с Сервером администрирования будет настроена.

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

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

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

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

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли откройте папку **Политики**.

3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

   - Двойным щелчком мыши по названию политики.

   - В контекстном меню политики выберите пункт **Свойства**.

   - В правой части окна выберите пункт **Настроить параметры политики**.

4. Выберите раздел **Managed Detection and Response**.

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

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

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

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

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

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

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

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

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

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

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

Настройка диагностики сбоев

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Чтобы настроить диагностику сбоев:

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

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

       В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве.
    6. Выберите программу Kaspersky Endpoint Agent и откройте окно ее свойств одним из следующих способов:
        - Двойным щелчком мыши по названию программы.
        - В контекстном меню программы выберите пункт **Свойства**.
        - Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".
2. В разделе **Параметры программы** выберите подраздел **Диагностика сбоев**.
3. Если вы хотите включить запись отладочной информации в файлы трассировки:
    a. Включите параметр **Записывать отладочную информацию в файлы трассировки**.
    b. В поле **Папка файлов трассировки** укажите путь к папке на устройстве, в которую программа должна сохранять файлы трассировки.

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

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

По умолчанию задано 50 МБ. При достижении заданного размера файла программа продолжает запись в новый файл.

4. Если вы хотите, чтобы программа выполняла перезапись старых файлов трассировки:

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

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

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

5. Если вы хотите включить запись файлов дампа:

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

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

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

6. Нажмите на кнопку **ОК**.

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

Управление задачами Kaspersky Endpoint Agent

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

Создание локальной задачи

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

Чтобы создать локальную задачу:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве Консоли администрирования откройте папку **Управляемые устройства**.

3. В папке **Управляемые устройства** откройте папку с названием группы администрирования, в состав которой входит требуемое устройство.

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

5. Выберите устройство, для которого вы хотите создать локальную задачу.

6. Выполните одно из следующих действий:

   - В контекстном меню устройства выберите пункт **Все задачи** → **Создать задачу**.

   - В контекстном меню устройства выберите пункт **Свойства** и в открывшемся окне **Свойства: <Название устройства>** на закладке **Задачи** нажмите на кнопку **Добавить**.

   - В раскрывающемся списке **Выполнить действие** выберите элемент **Создать задачу**.

   Запустится мастер создания задачи.

7. Выберите нужную задачу и нажмите **Далее**.

8. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

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

Чтобы создать групповую задачу:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Выполните одно из следующих действий:

   - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать групповую задачу для всех устройств, управляемых с помощью программы Kaspersky Security Center.

   - В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят требуемые устройства.

3. В рабочей области выберите закладку **Задачи**.

4. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.

5. Выберите нужную задачу и нажмите **Далее**.

6. Следуйте указаниям мастера создания задачи.

Просмотр списка задач

Чтобы просмотреть список задач на сервере Kaspersky Security Center:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

Отобразится список задач.

Удаление задач из списка

Чтобы удалить задачи из списка задач на сервере Kaspersky Security Center:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.
3. В списке задач выберите задачи, которые вы хотите удалить, и правой клавишей мыши откройте контекстное меню.

   Отобразится список действий, которые можно выполнить над задачами.
4. Выберите действие **Удалить**.

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

Выбранные задачи будут удалены из списка.

Запуск задач вручную

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

Чтобы вручную запустить одну задачу:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В контекстном меню нужной задачи выберите действие **Запустить**.

Задача запустится.

Запуск задач по расписанию

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить запуск задачи по расписанию:

1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.
2. В списке **Периодичность** выберите один из следующих вариантов запуска задачи по расписанию: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю**, **При запуске программы** или **После обновления баз программы**.
3. Если вы выбрали запуск задачи **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.
4. Если вы выбрали запуск задачи **Каждый час**, **Каждый день** или **Каждую неделю**, в разделе **Запускать по расписанию** настройте параметры запуска задачи:
   a. В списке **Каждый** выберите периодичность запуска задачи. Например, один раз в день или два раза в неделю, по вторникам и четвергам.
   b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.
5. Чтобы выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и настройте следующие параметры в окне **Дополнительно**:
   - **Завершать задачи, выполняющиеся более**

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

     Включите этот параметр, если вы хотите указать дату окончания действия расписания. После указанной даты расписание перестает действовать.
   - **Запускать пропущенные задачи**

     Включите этот параметр, если вы хотите, чтобы программа при первой возможности запускала задачи, не выполненные вовремя.
   - **Запускать задачу каждые**

     Включите этот параметр, если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение указанного интервала времени.
6. Нажмите на кнопку **OK**.

Запуск задач по расписанию настроен и применяется на устройствах.

Просмотр результатов выполнения задач

Вы можете просмотреть результаты выполнения задач в течение срока их хранения. Вы также можете изменить срок хранения результатов выполнения задач.

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

Чтобы просмотреть результат выполнения задачи:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. В меню выберите пункт **Результаты**.

Откроется окно **Результат выполнения задачи**.

Изменение срока хранения результатов выполнения задач на Сервере администрирования

По умолчанию результаты выполнения задач хранятся на Сервере администрирования в течение семи дней.

Чтобы изменить срок хранения результатов выполнения задач на Сервере администрирования:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. Выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. В левой части окна выберите раздел **Уведомление**.
6. Убедитесь, что в разделе **Сохранять информацию о результатах** установлен флажок **На Сервере администрирования в течение (сут)** и укажите, в течение какого времени (в сутках) требуется хранить результат выполнения задачи.
7. Нажмите на кнопку **Применить**, а затем на кнопку **ОК**.

Не рекомендуется сокращать срок хранения результатов выполнения задач поиска IOC.

Создание задачи активации Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете активировать Kaspersky Endpoint Agent с помощью ключа или кода активации.

При активации с помощью кода активации данные отправляются на сервер активации для проверки введенного кода.

Для активации программы с помощью кода активации защищаемое устройство должно быть подключено к интернету.

Чтобы создать задачу активации Kaspersky Endpoint Agent:

1. Запустите мастер создания задачи **Активация программы** для нужной области действия одним из следующих способов:

   - Запустите мастер создания локальной задачи.
   - **Запустите мастер создания групповой задачи**.

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

     Чтобы создать групповую задачу:

     1. Откройте Консоль администрирования Kaspersky Security Center.
     2. Выполните одно из следующих действий:

        - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать групповую задачу для всех устройств, управляемых с помощью программы Kaspersky Security Center.
        - В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят требуемые устройства.

     3. В рабочей области выберите закладку **Задачи**.
     4. Нажмите на кнопку **Новая задача**.

        Запустится мастер создания задачи.

     5. Выберите нужную задачу и нажмите **Далее**.
     6. Следуйте указаниям мастера создания задачи.

2. Если вы хотите активировать программу с помощью кода активации, выполните следующие действия в окне **Параметры активации**:

   a. Выберите **Активировать при помощи кода активации** и нажмите на кнопку **Выбрать**.

   b. В открывшемся окне введите код активации и нажмите **OK**.

3. Если вы хотите активировать программу с помощью файла ключа или ключа из хранилища ключей Kaspersky Security Center, выполните следующие действия в окне **Параметры активации**:

   a. Выберите **Активировать при помощи файла ключа или ключа** и нажмите на кнопку **Выбрать**.

   b. В раскрывающемся списке выберите нужный способ распространения ключа.

   c. Если вы выбрали **Файл ключа из папки**, в открывшемся окне укажите расположение файла ключа и нажмите на кнопку **Открыть**.

   d. Если вы выбрали **Файл ключа из хранилища Kaspersky Security Center**, в открывшемся окне выберите нужный ключ и нажмите **OK**.

   Подробная информация о хранилище ключей Kaspersky Security Center приведена в документации Kaspersky Security Center.

4. Если вы хотите добавить этот лицензионный ключ в качестве дополнительного для автоматического продления срока действия лицензии, установите флажок **Использовать в качестве дополнительного ключа**.

5. Нажмите на кнопку **Далее**.

6. В окне **Расписание** настройте параметры расписания запуска задачи и нажмите на кнопку **Далее**.

   Подробная информация о настройке параметров в этом окне приведена в документации Kaspersky Security Center.

7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой будет выполняться задача, и нажмите на кнопку **Далее**.

   Подробная информация о настройке параметров в этом окне приведена в документации Kaspersky Security Center.

8. В окне **Определение названия задачи** задайте имя задачи и нажмите на кнопку **Далее**.

9. Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

10. Нажмите на кнопку **Завершить**.

Будет создана новая задача активации программы для выбранного устройства или группы устройств.

Управление задачами обновления баз и модулей Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Создание задачи обновления баз и модулей программы

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы создать задачу обновления баз и модулей программы Kaspersky Endpoint Agent в Kaspersky Security Center:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Выберите программу, для которой будет создана задача – **Kaspersky Endpoint Agent**, и тип задачи **Обновление баз и модулей программы**.
5. Нажмите на кнопку **Далее**.

   Запустится мастер создания задачи обновления баз.

Мастер создания задачи обновления баз состоит из следующих шагов:

1. **Выбор источника обновления баз**

   Выполните следующие действия:

   1. В блоке **Источник обновлений баз** выберите один из следующих источников обновления баз:

      - **Сервер администрирования Kaspersky Security Center**.
      - **Серверы обновлений "Лаборатории Касперского"**.
      - **Другие HTTP-, FTP-серверы или сетевые папки**.

2. Если вы хотите включить параметр **Использовать серверы обновлений "Лаборатории Касперского", если указанные пользователем серверы недоступны**, установите флажок слева от названия параметра.

3. Если вы выбрали источник обновления баз **Серверы обновлений "Лаборатории Касперского"** и хотите использовать прокси-сервер для обновления баз, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.

4. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые папки**, выполните следующие действия:

   a. Нажмите на ссылку **Другие HTTP-, FTP-серверы или сетевые папки**.

   b. Добавьте серверы обновлений в список:

      1. Нажмите на кнопку **Серверы обновлений**.

      2. В добавленной строке введите адрес сервера обновлений (HTTP или FTP), либо путь к сетевой или локальной папке, содержащей файлы обновлений.

      3. Если вы хотите использовать этот сервер для обновления баз, установите флажок рядом с его адресом. Вы также можете добавить в список серверы и снять флажки рядом с адресами серверов, которые вы не хотите использовать сейчас, а планируете использовать в будущем.

         Выполняйте аналогичные действия по добавлению каждого сервера.

      4. Нажмите на кнопку **ОК**.

      5. Окно **Серверы обновлений** закроется.

   c. Если вы хотите использовать прокси-сервер для соединения с серверами обновлений, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

2. **Настройка параметров обновления модулей программы**

Выполните следующие действия:

1. В блоке **Параметры обновления** выберите, при каких условиях программа будет проверять доступность обновлений модулей программы:

   - **Не проверять доступность обновлений**. Kaspersky Endpoint Agent не будет проверять доступность обновлений модулей программы.
   - **Только проверять наличие важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.
   - **Загружать и устанавливать критические обновления модулей программы**. Kaspersky Endpoint Agent будет проверять доступность обновлений модулей программы и будет загружать и устанавливать критические обновления модулей программы.

2. Если вы хотите, чтобы программа отображала уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений, установите флажок **Получать информацию о доступных запланированных обновлениях модулей программы**.

3. **Настройка расписания обновления баз**

   Выполните следующие действия:

   1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.

   2. В списке **Периодичность** выберите один из следующих вариантов запуска задачи по расписанию: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю**, **При запуске программы** или **После обновления баз программы**.

   3. Если вы выбрали запуск задачи обновления баз **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.

   4. Если вы выбрали запуск задачи обновления баз **Каждый час**, **Каждый день** или **Каждую неделю**, в разделе **Запускать по расписанию** настройте параметры запуска задачи:

      a. В списке **Каждый** выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.

      b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

   5. Чтобы выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:

      a. Если вы хотите задать максимальное время ожидания выполнения задачи обновления баз, установите флажок **Завершать задачи, выполняющиеся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.

      b. Если вы хотите, чтобы расписание запуска задачи обновления баз действовало до определенной даты, установите флажок **Отменить расписание с** и укажите дату окончания действия расписания.

      c. Если вы хотите, чтобы программа при первой возможности запускала задачи обновления баз, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.

      d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Запускать задачу каждые** и задайте интервал запуска в минутах.

      e. Нажмите на кнопку **ОК**.

4. **Выбор устройств, на которых будет выполняться задача**

   В открывшемся окне выбора устройств выберите устройства, на который вы хотите назначить задачу и нажмите на кнопку **Далее**.

   Например, вы можете выбрать вариант **Назначить задачу группе администрирования** и выбрать группу администрирования из списка.

5. **Выбор учетной записи пользователя Kaspersky Security Center, с правами которой будет выполняться задача**

   В окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:

   - Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.
   - Введите имя и пароль пользователя, под учетной записью которого вы хотите выполнять задачу и нажмите на кнопку **Далее**.

6. **Указание названия задачи**

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

7. **Запуск задачи сразу после создания**

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

Настройка параметров задачи обновления баз и модулей программы

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Чтобы изменить параметры задачи:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.

3. В разделе **Обновление баз и модулей программы** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.

5. В левой части окна выберите раздел параметров, которые вы хотите настроить.
6. В правой части окна внесите необходимые изменения и нажмите на кнопки **Применить** и **ОК**.

Вы можете настроить следующие параметры задачи:

- **Название задачи**

  Выполните следующие действия:

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

- **Устройства, на которых будет выполняться задача**

  В правой части окна отображаются текущие устройства, на которые назначена задача. Если вы хотите добавить устройства, выполните следующие действия:

  1. Нажмите на кнопку **Добавить**.

     Откроется окно со списком управляемых устройств.

  2. Установите флажки рядом с теми устройствами, которые вы хотите добавить.
  3. Если вы хотите добавить устройства, которых нет в списке, нажмите на кнопку **Добавить** в правой части окна и выполните действия по добавлению устройств.

     Например, вы можете задать адреса устройств вручную или импортировать их из списка

     Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым вы хотите назначить задачу.

  Подробнее о работе с управляемыми устройствами см. в *Справке Kaspersky Security Center*.

- **Источник обновления баз**

  Выполните следующие действия:

  1. В блоке **Источник обновлений баз** выберите один из следующих источников обновления баз:

     - **Сервер администрирования Kaspersky Security Center**.
     - **Серверы обновлений "Лаборатории Касперского"**.
     - **Другие HTTP-, FTP-серверы или сетевые папки**.

  2. Если вы хотите включить параметр **Использовать серверы обновлений "Лаборатории Касперского", если указанные пользователем серверы недоступны**, установите флажок слева от названия параметра.
  3. Если вы выбрали источник обновления баз **Серверы обновлений "Лаборатории Касперского"** и хотите использовать прокси-сервер для обновления баз, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.

4. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые папки**, выполните следующие действия:

   a. Нажмите на ссылку **Другие HTTP-, FTP-серверы или сетевые папки**.

   b. Добавьте серверы обновлений в список:

      1. Нажмите на кнопку **Серверы обновлений**.

      2. В добавленной строке введите адрес сервера обновлений (HTTP или FTP), либо путь к сетевой или локальной папке, содержащей файлы обновлений.

      3. Если вы хотите использовать этот сервер для обновления баз, установите флажок рядом с его адресом. Вы также можете добавить в список серверы и снять флажки рядом с адресами серверов, которые вы не хотите использовать сейчас, а планируете использовать в будущем.

         Выполняйте аналогичные действия по добавлению каждого сервера.

      4. Нажмите на кнопку **ОК**.

      5. Окно **Серверы обновлений** закроется.

   c. Если вы хотите использовать прокси-сервер для соединения с серверами обновлений, в блоке **Параметры соединения с источниками обновлений** установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

- **Настройка дополнительных параметров обновления баз**

  Выполните следующие действия:

  1. В блоке **Параметры обновления** выберите, при каких условиях программа будет проверять доступность обновлений модулей программы:

     - **Не проверять доступность обновлений**. Kaspersky Endpoint Agent не будет проверять доступность обновлений модулей программы.

     - **Только проверять наличие важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.

     - **Загружать и устанавливать критические обновления модулей программы**. Kaspersky Endpoint Agent будет проверять доступность обновлений модулей программы и будет загружать и устанавливать критические обновления модулей программы.

  2. Если вы хотите, чтобы программа отображала уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений, установите флажок **Получать информацию о доступных запланированных обновлениях модулей программы**.

- **Расписание обновления баз**

  Выполните следующие действия:

  1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.

  2. В списке **Периодичность** выберите один из следующих вариантов запуска задачи по расписанию: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю**, **При запуске программы** или **После обновления баз программы**.

  3. Если вы выбрали запуск задачи обновления баз **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.

  4. Если вы выбрали запуск задачи обновления баз **Каждый час**, **Каждый день** или **Каждую неделю**, в разделе **Запускать по расписанию** настройте параметры запуска задачи:

     a. В списке **Каждый** выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.

     b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

  5. Чтобы выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:

     a. Если вы хотите задать максимальное время ожидания выполнения задачи обновления баз, установите флажок **Завершать задачи, выполняющиеся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.

     b. Если вы хотите, чтобы расписание запуска задачи обновления баз действовало до определенной даты, установите флажок **Отменить расписание с** и укажите дату окончания действия расписания.

     c. Если вы хотите, чтобы программа при первой возможности запускала задачи обновления баз, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.

     d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Запускать задачу каждые** и задайте интервал запуска в минутах.

     e. Нажмите на кнопку **ОК**.

- **Учетную запись пользователя Kaspersky Security Center, с правами которой будет выполняться задача**

  В окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:

  - Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.

  - Введите имя и пароль пользователя, под учетной записью которого вы хотите выполнять задачу.

- **Срок хранения результатов выполнения задачи на Сервере администрирования**

  Выполните следующие действия:

  1. Выберите раздел **Уведомление**.
  2. В блоке **Сохранять информацию о результатах** убедитесь, что флажок **На Сервере администрирования в течение (сут)** установлен и укажите, сколько суток вы хотите хранить результат выполнения задачи.

     По умолчанию результат выполнения задачи хранится на Сервере администрирования 7 дней.

Управление задачами поиска IOC в Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

О задачах поиска IOC в Kaspersky Endpoint Agent

Задачи поиска IOC – это задачи, в ходе выполнения которых Kaspersky Endpoint Agent использует IOC-файлы (файлы индикаторов компрометации открытого стандарта описания OpenIOC) для поиска этих индикаторов на устройствах.

Kaspersky Endpoint Agent поддерживает следующие типы задач поиска IOC:

- *Стандартные задачи поиска IOC* – групповые или локальные задачи, которые создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки. Для запуска задач используются IOC-файлы, подготовленные пользователем.
- *Поиск IOC по IOC-файлам, загружаемым вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform* – пользователи программы могут использовать IOC-файлы для поиска признаков целевых атак, зараженных и возможно зараженных объектов в базе событий и обнаружений, а также для проверки компьютеров с установленным компонентом Kaspersky Endpoint Agent.

Задачи отличаются возможностями управления, доступными для настройки параметрами, а также областью действия. Описание каждого типа задач поиска IOC приведено в следующей таблице.

Типы задач поиска IOC

Тип задач	Описание задач	Область действия задач
Стандартные задачи поиска IOC	Задачи создаются и настраиваются вручную в Kaspersky Security Center или через интерфейс командной строки, без интеграции со сторонними системами. Для запуска задач используются IOC-файлы, подготовленные пользователем. Параметры задач не зависят от настроек в параметрах политик. Для задач доступен режим **Ретроспективный поиск IOC**. Вы можете задать следующие действия по реагированию на найденные IOC (недоступно при запуске задач из командной строки): • Запуск на устройстве задач проверки по требованию при помощи EPP. • Включение сетевой изоляции устройства. Просмотр отчетов доступен как в результатах выполнения задач в виде сводной таблицы, так и в карточке обнаруженных IOC.	Локальные или групповые
Поиск IOC по IOC-файлам, загружаемым вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform	IOC-файлы загружаются вручную через веб-интерфейс Kaspersky Anti Targeted Attack Platform. Также есть возможность настроить расписание IOC-проверки компьютеров с программой Kaspersky Endpoint Agent в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Управление задачами с помощью Kaspersky Security Center или через командную строку не предусмотрено. Автоматических действий при обнаружении IOC не предусмотрено. Параметры задач не зависят от политик Kaspersky Endpoint Agent.	Не применимо

Результаты выполнения групповых задач поиска IOC доступны для просмотра в Kaspersky Security Center в течение семи дней с момента выполнения задачи или до момента удаления задачи.

Управление задачами поиска IOC в Kaspersky Endpoint Agent

Вы можете управлять задачами поиска IOC через Kaspersky Security Center или через интерфейс командной строки Kaspersky Endpoint Agent, а также загружать IOC-файлы и настраивать расписание IOC-проверки через веб-интерфейс Kaspersky Anti Targeted Attack Platform. Описание каждого типа задач поиска IOC и информация о доступных возможностях управления задачами поиска IOC приведены в таблице ниже.

Тип задачи	С помощью Kaspersky Security Center	С помощью компонента Central Node	Через интерфейс командной строки

Стандартная задача поиска IOC	• Создание, удаление и запуск задачи вручную.
	• Просмотр детальных отчетов в результатах выполнения задачи в виде сводной таблицы и в карточке обнаруженных IOC.
	• Экспорт IOC-коллекции.
	• Настройка следующих параметров в мастере создания задачи или в свойствах задачи после ее создания:
	  • Параметры IOC-коллекции.
	  • Параметры поиска IOC.
	  • Действия программы при обнаружении IOC (сетевая изоляция устройства и запуск проверки на устройстве с помощью EPP).
	  • Параметры расписания запуска задачи.
	  • Срок хранения результатов выполнения задачи на Сервере администрирования (недоступно в мастере создания задачи).
		Управление не предусмотрено.	• Создание и запуск задачи с требуемыми параметрами.
			• Просмотр данных о выполнении задачи.

Задача поиска IOC, созданная в Central Node	Управление не предусмотрено.	Загрузка IOC-файлов, настройка расписания IOC-проверки.	Управление не предусмотрено.

Управление стандартными задачами поиска IOC

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

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

Требования к IOC-файлам

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

- Kaspersky Endpoint Agent поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.
- Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
- Если при создании задачи Поиск IOC все загруженные вами IOC-файлы не поддерживаются Kaspersky Endpoint Agent, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации.
- Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Размер одного IOC-файла не должен превышать 3 МБ. Использование файлов большего размера приводит к завершению задач Поиск IOC с ошибкой. При этом суммарный размер всех добавленных файлов в IOC-коллекции может превышать 3 МБ.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

В таблице ниже приведены особенности и ограничения поддержки стандарта OpenIOC программой.

Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1

Поддерживаемые условия	OpenIOC 1.0:
	
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Поддерживаемые атрибуты условий	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Поддерживаемые операторы	`AND` `OR`

Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is, greater-than, less-than`)

Особенности интерпретации типов данных	Типы данных `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` интерпретируются как строка (string).
	
	Программа поддерживает интерпретацию параметра `Content` для типов данных `int` и `date`, заданного в виде промежутков:
	
	OpenIOC 1.0:
	С использованием оператора `TO` в поле `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	С помощью условий `greater-than` и `less-than`
	С использованием оператора `TO` в поле `Content`
	Программа поддерживает интерпретацию типов данных `date` и `duration`, если индикаторы заданы в формате `ISO 8601, Zulu time zone, UTC`.

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

Поддерживаемые IOC-термины

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX

Создание и настройка стандартной задачи поиска IOC

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

Чтобы создать и настроить стандартную задачу поиска IOC,

в зависимости от требуемой области действия задачи выполните одно из следующих действий:

- Запустите мастер создания локальной задачи.
- **Запустите мастер создания групповой задачи**.

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

Чтобы создать групповую задачу:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать групповую задачу для всех устройств, управляемых с помощью программы Kaspersky Security Center.
   - В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят требуемые устройства.
3. В рабочей области выберите закладку **Задачи**.
4. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
5. Выберите нужную задачу и нажмите **Далее**.
6. Следуйте указаниям мастера создания задачи.

Мастер создания задачи позволяет настроить следующие параметры:

- **IOC-коллекция**

  Чтобы настроить IOC-коллекцию, выполните следующие действия:

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

     Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
  4. Чтобы посмотреть список всех IOC-файлов, которые включены в IOC-коллекцию, а также получить информацию о каждом IOC-файле, нажмите на кнопку **Просмотр**.

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

6. Чтобы экспортировать созданную IOC-коллекцию, нажмите на кнопку **Экспортировать**.

   В открывшемся окне можно задать имя файла, а также выбрать папку, в которую вы хотите его сохранить.

7. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной папке.

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

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

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

     Откроется окно **IOC термины и документы**.

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

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

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

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

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

        Откроется окно **Параметры проверки документа ProcessItem**.

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

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

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

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

        Откроется окно **Параметры проверки документа FileItem**.

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

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

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

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

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

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

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

Откроется окно **Параметры проверки документа RegistryItem**.

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

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

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

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

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

Откроется окно **Параметры проверки документа EventLogItem**.

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

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

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

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

Сохраненные параметры будут применены при выполнении задачи.

- **Ретроспективный поиск IOC**

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

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

Чтобы включить режим Ретроспективный поиск IOC:

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

2. Укажите временной интервал.

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

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

- **Действия программы при обнаружении IOC**

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

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

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

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

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

- **Расписание запуска задачи**

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

  1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.

  2. В списке **Периодичность** выберите один из следующих вариантов запуска задач поиска IOC: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.

  3. Если вы выбрали запуск задачи **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.

4. Если вы выбрали запуск задачи **Каждый час**, **Каждый день** или **Каждую неделю**, в разделе **Запускать по расписанию** настройте параметры запуска задачи:

   a. В списке **Каждый** выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.

   b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

5. Чтобы выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:

   a. Если вы хотите задать максимальное время ожидания выполнения задачи, установите флажок **Завершать задачи, выполняющиеся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.

   b. Если вы хотите, чтобы расписание запуска задачи действовало до определенной даты, установите флажок **Отменить расписание с** и укажите дату окончания действия расписания.

   c. Если вы хотите, чтобы программа при первой возможности запускала задачи поиска IOC, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.

   d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Запускать задачу каждые** и задайте интервал запуска в минутах.

   e. Нажмите на кнопку **OK**.

- **Учетную запись пользователя Kaspersky Security Center для запуска задачи**

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

  в блоке параметров выбора учетной записи для запуска задачи выполните одно из следующих действий:

  - Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.
  - Введите имя и пароль пользователя, с правами учетной записью которого вы хотите выполнять задачу.

- **Название задачи**

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

Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.

Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.

Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.

Настройка параметров стандартной задачи поиска IOC

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

Чтобы настроить параметры стандартной задачи поиска IOC:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   В рабочей области отобразится список задач.
3. Откройте параметры требуемой задачи одним из следующих способов:

   - Двойным щелчком мыши по названию задачи.
   - Откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Выберите задачу и нажмите на ссылку **Настроить параметры задачи** в правой части окна.

   Откроется окно **Свойства: <Название задачи>**.
4. В левой части окна выберите раздел параметров, которые вы хотите настроить.
5. В правой части окна внесите необходимые изменения и нажмите на кнопку **Применить**, а затем на кнопку **ОК**.

   Настройка параметров стандартной задачи поиска IOC завершена.

Вы можете настроить следующие параметры задачи:

- **Название задачи**

  Выполните следующие действия:

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

- **Срок хранения результатов выполнения задачи на Сервере администрирования**

  Выполните следующие действия:

  1. Выберите раздел **Уведомление**.
  2. В блоке **Сохранять информацию о результатах** убедитесь, что флажок **На Сервере администрирования в течение (сут)** установлен и укажите, сколько суток вы хотите хранить результат выполнения задачи.

     По умолчанию результат выполнения задачи хранится на Сервере администрирования 7 дней.

- **IOC-коллекция**

  Чтобы настроить IOC-коллекцию, выполните следующие действия:

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

     Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.

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

     Откроется окно **Выбрать папку**. В этом окне можно исключить любой файл из базы, сняв флажок, расположенный рядом с именем IOC-файла.

  5. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Выбрать папку**.
  6. Чтобы экспортировать созданную IOC-коллекцию, нажмите на кнопку **Экспортировать**.

     В открывшемся окне можно задать имя файла, а также выбрать папку, в которую вы хотите его сохранить.

  7. Нажмите на кнопку **Сохранить**.

     Программа создаст файл формата ZIP в указанной папке.

- **Ретроспективный поиск IOC**

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

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

  Чтобы включить режим Ретроспективный поиск IOC:

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

  2. Укажите временной интервал.

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

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

- **Действия программы при обнаружении IOC**

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

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

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

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

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

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

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

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

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

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

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

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

        Откроется окно **Параметры проверки документа ProcessItem**.

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

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

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

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

        Откроется окно **Параметры проверки документа FileItem**.

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

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

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

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

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

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

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

        Откроется окно **Параметры проверки документа RegistryItem**.

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

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

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

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

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

Откроется окно **Параметры проверки документа EventLogItem**.

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

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

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

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

Сохраненные параметры будут применены при выполнении задачи.

- **Расписание запуска задачи поиска IOC**

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

1. В разделе **Расписание запуска задач** установите флажок **Запускать по расписанию**.

2. В списке **Периодичность** выберите один из следующих вариантов запуска задач поиска IOC: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.

3. Если вы выбрали запуск задачи **В указанное время**, в разделе **Запускать по расписанию** укажите время и дату запуска задачи.

4. Если вы выбрали запуск задачи **Каждый час**, **Каждый день** или **Каждую неделю**, в разделе **Запускать по расписанию** настройте параметры запуска задачи:

a. В списке **Каждый** выберите периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.

b. В списках **Время** и **Дата** выберите время и дату начала действия расписания.

5. Чтобы выполнить расширенную настройку расписания, нажмите на кнопку **Дополнительно** и выполните следующие действия в окне **Дополнительно**:

a. Если вы хотите задать максимальное время ожидания выполнения задачи, установите флажок **Завершать задачи, выполняющиеся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.

b. Если вы хотите, чтобы расписание запуска задачи действовало до определенной даты, установите флажок **Отменить расписание с** и укажите дату окончания действия расписания.

c. Если вы хотите, чтобы программа при первой возможности запускала задачи поиска IOC, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.

d. Если вы хотите избежать одновременного обращения большого количества рабочих станций к Серверу администрирования и запускать задачу на рабочих станциях не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Запускать задачу каждые** и задайте интервал запуска в минутах.

e. Нажмите на кнопку **OK**.

- **Учетная запись пользователя Kaspersky Security Center для запуска задачи**

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

  в блоке параметров выбора учетной записи для запуска задачи выполните одно из следующих действий:

  - Выберите учетную запись по умолчанию и нажмите на кнопку **Далее**.
  - Введите имя и пароль пользователя, с правами учетной записью которого вы хотите выполнять задачу.

- **Исключение групп устройств из области действия задачи**

  Если вы хотите исключить группы хостов из области действия задачи, в разделе **Исключения из области действия задачи** выберите группы устройств, к которым не будет применяться задача.

  Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

Экспорт IOC-коллекции

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы экспортировать IOC-коллекцию:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   Отобразится список задач.
3. В разделе **Запустить поиск IOC** выберите задачу в списке и правой клавишей мыши раскройте меню действий над задачами.
4. Выберите пункт меню **Свойства**.

   Откроется окно свойств задачи.
5. Выберите раздел **Параметры поиска IOC**.
6. В разделе **IOC-коллекция** нажмите на кнопку **Экспортировать**.
7. В открывшемся окне задайте имя файла, а также выберите папку, в которую вы хотите его сохранить.

8. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной вами папке.

Просмотр результатов выполнения задачи поиска IOC

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы просмотреть результаты выполнения задачи Поиск IOC:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования откройте папку **Задачи**.

   В рабочей области отобразится список задач.
3. Откройте параметры нужной задачи одним из следующих способов:

   - Двойным щелчком мыши по названию задачи.
   - Откройте контекстное меню задачи и выберите пункт **Свойства**.
   - Выберите задачу и нажмите на ссылку **Настроить параметры задачи** в правой части окна.

   Откроется окно **Свойства: <Имя задачи>**.
4. Выберите раздел **Результаты**.
5. В списке **Показать результаты по устройству** выберите, по каким устройствам вы хотите просмотреть результаты выполнения задач поиска IOC.
6. Чтобы просмотреть подробную информацию об определенной задаче, раскройте ее двойным щелчком мыши.
7. Чтобы просмотреть подробную информацию об обнаруженном индикаторе компрометации, нажмите на кнопку **Показать карточку**.

   Карточка обнаруженных IOC содержит информацию об объектах, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.

   Просмотр карточки обнаруженных IOC недоступен для IOC-файлов, при проверке которых не было обнаружено индикаторов компрометации.

Управление Kaspersky Endpoint Agent в Kaspersky Security Center Web Console

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленной программой Kaspersky Endpoint Agent, объединенными в группу администрирования, с помощью веб-плагина управления Kaspersky Endpoint Agent. Kaspersky Security Center Web Console также позволяет отдельно настраивать параметры работы для каждого защищаемого устройства, входящего в группу администрирования.

Группа администрирования формируется вручную на стороне Kaspersky Security Center Web Console и включает несколько устройств с установленной программой Kaspersky Endpoint Agent, для которых вы хотите настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в Справке Kaspersky Security Center.

Параметры программы для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Endpoint Agent на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Endpoint Agent из Kaspersky Security Center Web Console следующими способами:

- С помощью политик Kaspersky Security Center. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне свойств устройства в Kaspersky Security Center Web Console.

- С помощью политик вы можете настроить общие параметры работы программы, параметры задач постоянной защиты, контроля активности на компьютерах, а также параметры запуска системных задач по расписанию.

- С помощью групповых задач Kaspersky Security Center. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств.

- С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.

- С помощью задач для набора устройств. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.

- С помощью окна свойств отдельного устройства. В окне свойств устройства можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Endpoint Agent, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center Web Console позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы защищаемых устройств, так и для отдельного защищаемого устройства.

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

Управление политиками Kaspersky Endpoint Agent

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

Создание политики Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы создать политику Kaspersky Endpoint Agent в Kaspersky Security Center Web Console:

1. В главном окне перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
3. Выберите программу Kaspersky Endpoint Agent и нажмите **Далее**.
4. Выберите необходимый способ развертывания Kaspersky Endpoint Agent, установив соответствующие флажки:

   - **Интеграция с Kaspersky Sandbox;**
   - **Endpoint Detection and Response Optimum;**
   - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks.**

   Выбор типа политики и интеграция с Kaspersky Sandbox и KATA EDR недоступны в Kaspersky Security Center Cloud Console.
5. Нажмите **Далее**.

6. На закладке **Общие** вы можете выполнить следующие действия:

   - Изменить имя политики.
   - Выбрать состояние политики:
     - **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.
     - **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.
     - **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.
   - Настроить наследование параметров:
     - **Наследовать параметры родительской политики**. Если переключатель включен, значения параметров политики наследуются из политики верхнего уровня иерархии. Параметры политики недоступны для изменения, если в родительской политике установлен переключатель **Обеспечить принудительное наследование параметров для дочерних политик**.
     - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики будут распространены на дочерние политики. В свойствах дочерней политики будет автоматически включен и недоступен для выключения переключатель **Наследовать параметры родительской политики**.

7. На закладке **Параметры программы** вы можете настроить параметры политики Kaspersky Endpoint Agent.

8. Нажмите на кнопку **Сохранить**.

Включение параметров в политике Kaspersky Endpoint Agent

При настройке параметров политики Kaspersky Endpoint Agent по умолчанию значения параметров сохраняются, но не применяются до тех пор, пока вы их не включите.

Включение параметров доступно для блоков, в которых находятся эти параметры. В рамках одной политики вы можете включить как часть блоков параметров, так и все блоки параметров.

Чтобы включить блок параметров в политике Kaspersky Endpoint Agent:

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

2. Выберите раздел и блок параметров, к которым относятся нужные параметры.

3. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

Все параметры блока будут применяться в политике.

Настройка параметров Kaspersky Endpoint Agent

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

Открытие окна параметров Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы открыть окно параметров политики Kaspersky Endpoint Agent, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.

2. Выберите политику, которую вы хотите настроить.

3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

Чтобы открыть окно параметров Kaspersky Endpoint Agent для отдельного устройства:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.

2. Выберите устройство.

3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.

4. Выберите **Kaspersky Endpoint Agent**.

5. В открывшемся окне выберите закладку **Параметры программы**.

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**, кроме параметров сетевой изоляции.

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

Настройка параметров безопасности Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

- Ограничение прав пользователей на управление параметрами и службами программы.
- Защита действий в программе паролем.
- Механизм самозащиты программы.

Настройка прав пользователей

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете предоставить доступ к Kaspersky Endpoint Agent отдельным пользователям или группам пользователей. В результате только заданные пользователи смогут управлять параметрами или службами программы.

Чтобы настроить права пользователей:

1. Выполните одно из следующих действий:
   - **Откройте окно свойств программы для отдельного устройства**.
     1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
     2. Выберите устройство.
     3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
     4. Выберите **Kaspersky Endpoint Agent**.
     5. В открывшемся окне выберите закладку **Параметры программы**.

- **Откройте окно свойств политики программы**.

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

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. В блоке параметров **Права пользователей на управление службами программы** нажмите на кнопку **Настроить** рядом с названием нужного параметра (**Права пользователей на управление программой** или **Настройка прав пользователей на управление программой**).

   Чтобы добавить пользователей и группы пользователей, необходимо указать строки дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL).
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **OK**.
6. Нажмите на кнопку **Сохранить**.

Включение защиты паролем

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Неограниченный доступ пользователей к программе и ее параметрам может привести к снижению уровня безопасности устройства. Защита паролем позволяет ограничить доступ пользователей к программе.

Чтобы включить защиту паролем:

1. Выполните одно из следующих действий:

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

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

- **Откройте окно свойств политики программы**.

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

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. В блоке параметров **Защита паролем** установите флажок **Применить защиту паролем**.
4. Задайте пароль и подтвердите его.

   Рекомендуется задать пароль, который удовлетворяет следующим условиям:

   - Длина пароля должна быть не менее 8 символов.
   - Пароль не должен содержать имени учетной записи пользователя.
   - Пароль не должен совпадать с именем устройства, на котором установлена программа Kaspersky Endpoint Agent.
   - Пароль должен содержать символы как минимум трех групп из следующего списка:
     - верхний регистр (A-Z);
     - нижний регистр (a-z);
     - цифры (0-9);
     - специальные символы (!$#%).
5. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**.

Защита паролем будет включена. При попытке пользователя выполнить действие, защищенное паролем, программа предложит пользователю ввести пароль.

Программа не проверяет надежность заданного пароля. Рекомендуется использовать сторонние средства для проверки надежности пароля. Пароль считается надежным, если по результатам проверки подтверждена невозможность подбора пароля минимум за 6 месяцев.

Программа не блокирует возможность ввода пароля после множества попыток ввода некорректного пароля.

Включение и отключение механизма самозащиты

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Для защиты от вредоносных программ, которые пытаются заблокировать работу Kaspersky Endpoint Agent или удалить программу, в программе реализован *механизм самозащиты*. Этот механизм предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

Чтобы включить или отключить механизм самозащиты:

1. Выполните одно из следующих действий:

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

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

   - **Откройте окно свойств политики программы**.

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

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. В блоке параметров **Самозащита** включите или выключите параметр **Включить самозащиту модулей программы в памяти**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**.

Механизм самозащиты будет включен или отключен.

Настройка параметров соединения Kaspersky Endpoint Agent с прокси-сервером

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Если вы хотите **Использовать прокси-сервер с указанными параметрами** при соединении с сервером KATA, Kaspersky Industrial CyberSecurity for Networks или Kaspersky Sandbox, убедитесь, что выбрана опция **Подключаться через прокси-сервер, если это задано в общих параметрах** при настройке интеграции с KATA, Kaspersky Industrial CyberSecurity for Networks или Kaspersky Sandbox. По умолчанию опция не выбрана.

Чтобы настроить параметры соединения с прокси-сервером:

1. Выполните одно из следующих действий:

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

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

   - **Откройте окно свойств политики программы**.

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

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.

3. Выберите один из следующих вариантов использования прокси-сервера:

   - **Не использовать прокси-сервер**.
   - **Автоматически определять адрес прокси-сервера**.
   - **Использовать прокси-сервер с указанными параметрами**.

4. Если вы выбрали вариант **Автоматически определять адрес прокси-сервера**, прокси-сервер определяется автоматически для дальнейшей передачи телеметрии.

5. Если вы выбрали вариант **Использовать прокси-сервер с указанными параметрами**, в полях **Имя или IP-адрес сервера** и **Порт** введите адрес и порт прокси-сервера, соединение с которым вы хотите установить.

   По умолчанию используется порт 8080.

6. Если вы хотите использовать NTLM-аутентификацию при подключении к прокси-серверу, выполните следующие действия:

   a. Установите флажок **Использовать NTLM-аутентификацию по имени пользователя и паролю**.

   b. В поле **Имя пользователя** введите имя пользователя, учетная запись которого будет использоваться для авторизации на прокси-сервере.

   c. В поле **Пароль** введите пароль подключения к прокси-серверу.

      Вы можете включить отображение символов пароля, нажав на кнопку **Показать** справа от поля **Пароль**.

7. Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.

8. Если вы настраиваете свойства политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

9. Нажмите на кнопку **ОК**.

10. В окне свойств политики нажмите на кнопку **Сохранить**.

Параметры соединения с прокси-сервером настроены.

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

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

1. Выполните одно из следующих действий:

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

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

   - **Откройте окно свойств политики программы**.

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

2. В разделе **Параметры программы** выберите подраздел **Параметры безопасности**.
3. В блоке параметров **Лицензирование** установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.
4. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.
5. Нажмите на кнопку **ОК**.
6. В окне свойств политики нажмите на кнопку **Сохранить**.

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

Настройка типа политики Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Выбор типа политики Kaspersky Endpoint Agent необходим для того, чтобы состав отображаемых в политике параметров соответствовал выбранному способу развертывания Kaspersky Endpoint Agent.

Чтобы настроить тип политики:

1. **Откройте окно свойств политики программы**.
    1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
    2. Выберите политику, которую вы хотите настроить.
    3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
2. В разделе **Параметры программы** выберите подраздел **Интерфейс и управление**.
3. В открывшемся окне выберите необходимый способ развертывания Kaspersky Endpoint Agent, установив соответствующие флажки:
    - **Интеграция с Kaspersky Sandbox;**
    - **Endpoint Detection and Response Optimum;**
    - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks.**

    Выбор типа политики и интеграция с Kaspersky Sandbox и KATA EDR недоступны в Kaspersky Security Center Cloud Console.
4. Нажмите на кнопку **OK**.

Тип политики изменен. В политике доступны параметры для выбранного способа развертывания Kaspersky Endpoint Agent.

Настройка использования KSN в Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Agent использует данные, полученные от пользователей во всем мире. Сеть Kaspersky Security Network предназначена для получения этих данных.

Kaspersky Security Network (далее также KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программы EPP на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, информация о которых еще не вошла в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы.

Во время участия в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Endpoint Agent, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

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

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

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

Чтобы включить использование KSN:

1. Выполните одно из следующих действий:

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

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

   - **Откройте окно свойств политики программы**.

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

2. В разделе **Kaspersky Security Network** нажмите на ссылку **Ознакомиться с условиями Положения о KSN** и выполните следующие действия:

   a. В правой части окна ознакомьтесь с условиями Положения о KSN.

   b. Если вы согласны с условиями Положения, установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Положения о KSN**.

   c. Нажмите на кнопку **OK**.

3. Установите флажок **Включить использование Kaspersky Security Network (KSN)**.

4. Если вы хотите использовать Kaspersky Security Center в качестве посредника для передачи телеметрии, установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.

5. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

6. Нажмите на кнопку **OK**.

7. В окне свойств политики нажмите на кнопку **Сохранить**.

Использование KSN будет включено.

Настройка интеграции Kaspersky Endpoint Agent с KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе содержится информация о том, как настроить интеграцию Kaspersky Endpoint Agent с компонентом KATA Central Node с помощью Kaspersky Security Center Web Console.

Настройка параметров передачи данных

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры передачи данных, выполните следующие действия:

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

    Откроется окно **Общие параметры**.
3. В блоке параметров **Параметры передачи данных** выполните следующие действия:
    - Укажите значения в поле **Максимальное время передачи событий (сек.)**.
    - Укажите значения в поле **Максимальное количество событий в одном пакете**.
4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

    По умолчанию переключатель находится в положении **Принудительно**.
5. Нажмите на кнопку **OK**.

Настройка параметров регулирования количества запросов

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Чтобы настроить параметры регулирования количества запросов:

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

    Откроется окно **Общие параметры**.

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

   - Установить или снять флажок **Включить регулирование количества запросов**, чтобы включить или отключить функцию.

     По умолчанию функция включена.

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

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

   - Указать значения в поле **Процент превышения лимита событий**.

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

4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

5. Нажмите на кнопку **ОК**.

Включение и отключение интеграции с KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы используете Nginx в качестве прокси-сервера между устройством с Kaspersky Endpoint Agent и сервером KATA, настройте параметр `client_max_body_size:` значение параметра `client_max_body_size` должно быть равно максимальному размеру объекта, отправляемого программой Kaspersky Endpoint Agent на обработку в KATA. Иначе Nginx не будет пропускать объекты, размер которых превышает установленное значение. Значение по умолчанию – 1 МБ.

Чтобы включить или отключить интеграцию с компонентом KATA Central Node:

1. **Откройте окно свойств политики программы**.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Политики и профили политик**.

   2. Выберите политику, которую вы хотите настроить.

   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KATA**.

   Откроется окно **Интеграция с KATA**.

3. В блоке **Параметры подключения** выполните одно из следующих действий:

   - Чтобы включить интеграцию с KATA Central Node:

     a. Установите флажок **Включить интеграцию с KATA**.

     b. В блоке параметров **Список серверов KATA** для одного или нескольких серверов KATA укажите IP-адрес или полное доменное имя сервера KATA, а также порт подключения к серверу.

     Kaspersky Endpoint Agent подключается к первому серверу из списка. Если подключение не удается, Kaspersky Endpoint Agent подключается ко второму серверу и так далее по списку.

   - Чтобы отключить интеграцию с KATA Central Node, снимите флажок **Включить интеграцию с KATA**.

4. Включите или выключите параметр **Подключаться через прокси-сервер, если это задано в общих параметрах**.

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

5. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

6. Нажмите на кнопку **ОК**.

Интеграция с KATA Central Node будет включена или отключена.

Настройка доверенного соединения с KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить доверенное соединение Kaspersky Endpoint Agent с KATA Central Node, выполните следующие действия на стороне Kaspersky Endpoint Agent:

1. **Откройте окно свойств политики программы**.

   1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Политики и профили политик**.

   2. Выберите политику, которую вы хотите настроить.

   3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KATA**.

   Откроется окно **Интеграция с KATA**.

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

4. Нажмите на кнопку **Добавить TLS-сертификат**.

   Откроется окно добавления TLS-сертификата.

5. Выполните одно из следующих действий по добавлению TLS-сертификата:

   - Добавьте файл сертификата. Для этого нажмите на кнопку **Загрузить**, в открывшемся окне выберите файл сертификата и нажмите на кнопку **Открыть**.
   - Скопируйте содержимое файла сертификата в поле **Данные TLS-сертификата**.

   В Kaspersky Endpoint Agent может быть только один TLS-сертификат сервера KATA. Если вы добавляли TLS-сертификат ранее и снова добавили TLS-сертификат, только последний добавленный сертификат будет актуальным.

6. Нажмите на кнопку **OK**.

   Информация о добавленном TLS-сертификате отобразится в блоке параметров **Данные TLS-сертификата**.

7. Если вы хотите настроить дополнительную защиту подключения с использованием пользовательского сертификата, выполните следующие действия:

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

   b. Нажмите на кнопку **Загрузить криптоконтейнер**.

   c. В открывшемся окне выберите архив формата PFX и нажмите на кнопку **Открыть**.

   d. В поле **Пароль криптоконтейнера** введите пароль к архиву формата PFX.

   e. Нажмите на кнопку **OK**.

8. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

   По умолчанию переключатель находится в положении **Принудительно**.

9. Нажмите на кнопку **OK**.

Доверенное соединение с сервером KATA настроено.

Файл TLS-сертификата должен удовлетворять следующим требованиям:

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

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

Настройка параметров синхронизации Kaspersky Endpoint Agent с KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры синхронизации Kaspersky Endpoint Agent с KATA Central Node:

1. **Откройте окно свойств политики программы**.
    1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Политики и профили политик**.
    2. Выберите политику, которую вы хотите настроить.
    3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
2. В разделе **Серверы сбора телеметрии** выберите **Интеграция с KATA**.

    Откроется окно **Интеграция с KATA.**
3. В блоке параметров **Дополнительные параметры** настройте следующие параметры:
    - **Время ожидания (сек.)**. Укажите максимальное время ожидания ответа от сервера KATA. По умолчанию задано 10 секунд.
    - **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)**. Укажите период отправки запросов на синхронизацию параметров и задач Kaspersky Endpoint Agent с KATA Central Node. Можно указать значение в пределе от 1 до 60 минут. По умолчанию задано 5 минут.
    - Установите или снимите флажок **Использовать период TTL при отправке событий**. По умолчанию флажок снят.

      При установленном флажке Kaspersky Endpoint Agent не отправляет на сервер KATA информацию о процессах, которые запускаются повторно. Kaspersky Endpoint Agent не считает запуск процесса повторным, если запуск происходит после окончания очередного периода TTL.
    - Если вы установили флажок **Использовать период TTL при отправке событий**, укажите время в поле **Период TTL (мин.)**. По умолчанию задано 1440 минут.
4. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

    По умолчанию переключатель находится в положении **Принудительно**.
5. Нажмите на кнопку **OK**.

Настройка параметров EDR-телеметрии

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В этом разделе содержится информация о том, как настроить:

- Исключения EDR-телеметрии о процессах программ, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.
- Оптимизацию объема EDR-телеметриии, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом Kaspersky Industrial CyberSecurity for Networks.
- Исключения EDR-телеметрии о сетевых коммуникациях, которую Kaspersky Endpoint Agent обрабатывает и передает на сервер с компонентом Kaspersky Industrial CyberSecurity for Networks.

Включение и настройка исключений и оптимизации объема отправляемой EDR-телеметрии о процессах программ

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете включить и настроить исключения и оптимизацию объема отправляемой EDR-телеметрии о процессах программ с помощью Kaspersky Security Center Web Console в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии о процессах программ доступны при интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks данные об исключенных процессах программ.

Управление (включение / выключение) оптимизацией объема отправляемой EDR-телеметрии о процессах программ доступно при интеграции Kaspersky Endpoint Agent с серверами с установленным Kaspersky Industrial CyberSecurity for Networks.

Если включена оптимизация объема отправляемой EDR-телеметрии, Kaspersky Endpoint Agent не отправляет события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и Агента администрирования klnagent.exe о процессах программ на сервер с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks.

Чтобы включить и настроить исключения и оптимизацию объема отправляемой EDR-телеметрии о процессах программ:

1. Выполните одно из следующих действий:

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

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

   - **Откройте окно свойств политики программы**.

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

2. В разделе **EDR-телеметрия** выберите **Исключенные процессы**.

   Откроется окно **Исключенные процессы**.

3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.

4. Настройте оптимизацию объема отправляемой EDR-телеметрии:

   При интеграции Kaspersky Endpoint Agent с серверами с установленным KATA Central Node оптимизация объема отправляемой EDR-телеметрии должна быть всегда включена.

   - Выключите параметр **Оптимизировать объем отправляемой телеметрии**, если хотите, чтобы Kaspersky Endpoint Agent отправляла события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB, службы WinRM и процесса Агента администрирования klnagent.exe.
   - Включите параметр **Оптимизировать объем отправляемой телеметрии**, если хотите, чтобы Kaspersky Endpoint Agent не отправляла события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и Агента администрирования klnagent.exe.

   Если параметр **Использовать исключения** выключен, Kaspersky Endpoint Agent не отправляет события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB и процесса Агента администрирования klnagent.exe вне зависимости от значения параметра **Оптимизировать объем отправляемой телеметрии**.

5. Создайте список исключений:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Свойства правила настройте параметры исключения**.

   Параметры исключения применяются по правилу логического И.

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

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

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

   1. В блоке **Информация о процессе** задайте значения в следующих полях:

      - **Полный путь**. Полный путь к файлу, включая его имя и расширение. Можно использовать маски файлов (с помощью символов ? и *), а также системные переменные окружения.
      - **Текст командной строки**. Командная строка для запуска объекта.
      - **Родительский путь**. Путь до папки, в которой находится файл.

   2. В блоке **Свойства файла** задайте значения в следующих полях:

      - **Описание файла**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo).
      - **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo).
      - **Версия файла**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo).

   3. В блоке **Контрольные суммы файла** задайте значения в следующих полях:

      - **MD5**. MD5-хеш файла.
      - **SHA256**. SHA256-хеш файла.

   4. В списке **Использовать это исключение для следующих типов событий** выберите как минимум одно из значений:

      - **Изменение файла**.
      - **Сетевые события**.

- **Интерактивный ввод в консоли**.

  Этот тип события выбран по умолчанию.

- **Загрузка модуля процесса**.

- **Изменения в реестре**.

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

Новое исключение создано и отображается в списке.

d. Если необходимо экспортировать список исключений в файл формата XML, нажмите на кнопку **Экспорт**.

e. Если необходимо испортировть список исключений из файла формата XML, нажмите на кнопку **Импорт**.

f. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.

g. Если необходимо удалить исключение из списка, выберите исключение и нажмите на кнопку **Удалить**.

6. Если вы настраиваете параметры политики, убедитесь, что переключатель в правом верхнем углу блока параметров находится в активном положении. Переключатель находится в этом положении по умолчанию.

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

Включение и настройка исключений отправляемой EDR-телеметрии о сетевых коммуникациях

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить исключения отправляемой EDR-телеметрии о сетевых коммуникациях с помощью Kaspersky Security Center Web Console в свойствах отдельного устройства или и в свойствах политики для группы устройств.

Исключения отправляемой EDR-телеметрии о сетевых коммуникациях применимы при интеграции Kaspersky Endpoint Agent с серверами с установленным Kaspersky Industrial CyberSecurity for Networks.

Kaspersky Endpoint Agent не анализирует и не передает на сервер с установленным KATA Central Node или Kaspersky Industrial CyberSecurity for Networks данные, подпадающие под параметры исключений.

Чтобы включить и настроить исключения отправляемой EDR-телеметрии о сетевых коммуникациях:

1. Выполните одно из следующих действий:

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

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

   - **Откройте окно свойств политики программы**.

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

2. В разделе **EDR-телеметрия** выберите **Исключенные сетевые коммуникации**.

   Откроется окно **Исключенные сетевые коммуникации процессы**.

3. В блоке параметров **Исключения** включите параметр **Использовать исключения**, чтобы включить применение исключений для EDR-телеметрии.

4. Создайте список исключений:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Свойства правила настройте параметры исключения.**

   > Параметры исключения применяются по правилу логического И.

      1. В поле **Имя** введите название исключения.
      2. В раскрывающемся списке **Направление** выберите направление сетевого трафика.
      3. В раскрывающемся списке **Протокол** выберите сетевой протокол передачи данных.
      4. Если вы выбрали пользовательский протокол, в поле **Номер** введите номер сетевого протокола.
      5. Установите флажок **Локальный порт ИЛИ диапазон** и введите номер порта или диапазон номеров.

         Для входящих подключений (в раскрывающемся списке **Направление** выбрано **Входящее**) введите порт или диапазон портов для локального устройства.

Для исходящих подключений (в раскрывающемся списке **Направление** выбрано **Исходящее**) введите порт или диапазон портов для удаленного устройства.

Для номера порта доступны значения 1–65535.

Для диапазона портов доступны значения 1–10, 20–30000 и 1–65535.

Ограничения:

- Для сетевых подключений локального устройства с операционной системой Windows XP можно указать только один порт, поскольку в Windows XP не поддерживается диапазон портов.
- Для сетевых подключений удаленного устройства с операционной системой Windows XP можно указать диапазон портов, но правило применяется только к первому порту заданного диапазона, поскольку в Windows XP не поддерживается диапазон портов.

6. Установите флажок **Удаленный порт ИЛИ диапазон** и введите номер порта или диапазон номеров.

   Для входящих подключений (в раскрывающемся списке **Направление** выбрано **Входящее**) введите порт или диапазон портов для удаленного устройства.

   Для исходящих подключений (в раскрывающемся списке **Направление** выбрано **Исходящее**) введите порт или диапазон портов для локального устройства.

   Для номера порта доступны значения 1–65535.

   Для диапазона портов доступны значения 1–10, 20–30000 и 1–65535.

   Ограничения:

   - Для сетевых подключений локального устройства с операционной системой Windows XP можно указать только один порт, поскольку в Windows XP не поддерживается диапазон портов.
   - Для сетевых подключений удаленного устройства с операционной системой Windows XP можно указать диапазон портов, но правило применяется только к первому порту заданного диапазона, поскольку в Windows XP не поддерживается диапазон портов.

7. Установите флажок **Локальный адрес** и введите сетевой адрес устройства, для которого Kaspersky Endpoint Agent не будет анализировать и передавать EDR-телеметрию сетевого трафика в соответствии с параметрами исключения.

   Для входящих подключений (в раскрывающемся списке **Направление** выбрано **Входящее**) введите сетевой адрес для локального устройства.

   Для исходящих подключений (в раскрывающемся списке **Направление** выбрано **Исходящее**) введите сетевой адрес для удаленного устройства.

   > Для IP-адресов поддерживается только формат IPv4.

8. Установите флажок **Удаленный адрес** и введите сетевой адрес устройства, для которого Kaspersky Endpoint Agent не будет анализировать и передавать EDR-телеметрию сетевого трафика в соответствии с параметрами исключения.

   Для входящих подключений (в раскрывающемся списке **Направление** выбрано **Входящее**) введите сетевой адрес для удаленного устройства.

Для исходящих подключений (в раскрывающемся списке **Направление** выбрано **Исходящее**) введите сетевой адрес для локального устройства.

> Для IP-адресов поддерживается только формат IPv4.

9. **Сформируйте список программ,** для которых Kaspersky Endpoint Agent не будет анализировать и передавать EDR-телеметрию сетевого трафика в соответствии с параметрами исключения.

    1. Установите флажок **Программы**.
    2. В поле ниже укажите путь к исполняемому файлу программы, которую вы хотите добавить в список. Вы можете ввести путь вручную или с помощью кнопки **Обзор**.
    3. Нажмите на кнопку **Добавить**.
    4. Повторите пункты 2 и 3 инструкции для каждой программы, которую вы хотите добавить в список.
    5. Если необходимо удалить програму из списка:
        a. Выделите программу в списке.
        b. Нажмите на кнопку **Удалить**.
10. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Свойства правила**.

    Новое исключение создано и отображается в списке.

c. Если необходимо изменить исключение, выберите исключение и нажмите на кнопку **Изменить**.

d. Если необходимо удалить исключение, выберите исключение и нажмите на кнопку **Удалить**.

5. Если вы настраиваете параметры политики, убедитесь, что положение переключателя в правом верхнем углу блока параметров находится в активном положении. Переключатель находится в этом положении по умолчанию.

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

Настройка интеграции Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

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

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

Чтобы настроить интеграцию Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response с помощью Kaspersky Security Center Web Console:

1. Откройте Kaspersky Security Center Web Console.
2. Перейдите на закладку **Устройства** → **Политики и профили**.
3. В списке политик выберите название политики Kaspersky Endpoint Agent, которую вы хотите настроить.

   Откроется окно параметров политики.
4. Включите **Использование KSN**.

   Откройте главное окно Kaspersky Security Center Web Console.
5. В дереве Консоли администрирования настройте параметры **Локального KSN** (Подробнее о настройке параметров прокси-сервера Kaspersky Security Network см. в *Справке Kaspersky Security Center*).

   Загрузите файл конфигурации Kaspersky Managed Detection and Response с расширением pkcs7, который включен в архив mdr_config.zip.
6. Для продолжения настройки интеграции Kaspersky Endpoint Agent с Kaspersky Managed Detection and Response откройте главное окно Kaspersky Security Center Web Console.
7. Перейдите на закладку **Устройства** → **Политики и профили**.

8. В списке политик выберите название политики Kaspersky Endpoint Agent, которую вы хотите настроить.

   Откроется окно параметров политики.

9. На закладке **Параметры программы** выберите пункт **Managed Detection and Response**.

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

    a. Установите переключатель в положение **Managed Detection and Response включен**.

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

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

    d. В правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

11. Нажмите **Сохранить**, чтобы сохранить внесенные изменения.

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

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

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

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

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

Настройка параметров хранилищ в Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

О карантине Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Карантин – это специальное локальное хранилище на устройстве. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

По умолчанию локальное хранилище карантина расположено в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Quarantine`. По умолчанию объекты, восстановленные из карантина, хранятся в папке `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<версия>\Restored`.

Kaspersky Security Center формирует общий список объектов, помещенных на карантин на устройствах с программой Kaspersky Endpoint Agent. Агенты администрирования устройств передают информацию о файлах на карантине на Сервер администрирования.

Агент администрирования Kaspersky Security Center не копирует файлы из карантина на Сервер администрирования . Все объекты находятся на защищаемых устройствах с программой Kaspersky Endpoint Agent. Восстановление объектов из карантина также выполняется на защищаемых устройствах.

Об управлении карантином в Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Через Kaspersky Security Center можно настраивать параметры карантина, просматривать свойства объектов, находящихся на карантине на защищаемых устройствах, удалять объекты, находящиеся на карантине, а также восстанавливать объекты из карантина. Подробную информацию об управлении объектами, находящимися на карантине, через Kaspersky Security Center см. в документации Kaspersky Security Center.

Для того чтобы Kaspersky Endpoint Agent отправлял данные об объектах, помещенных на карантин, на Сервер администрирования Kaspersky Security Center, необходимо включить эту опцию в параметрах карантина в политике Kaspersky Endpoint Agent. По умолчанию опция включена.

Через интерфейс командной строки на устройстве можно просматривать информацию о параметрах карантина и свойствах объектов, находящихся на карантине.

Kaspersky Endpoint Agent помещает объект на карантин под системной учетной записью (SYSTEM).

Удаление объектов, помещенных на карантин, через командную строку доступно только под локальной учетной записью пользователя защищаемого устройства.

Настройка параметров карантина и восстановления объектов из карантина

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить параметры карантина:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. В разделе **Репозитории** выберите подраздел **Карантин**.
5. В разделе **Параметры Карантина** настройте параметры карантина:
   a. В поле **Папка Карантина** укажите путь, по которому будет создана папка карантина на устройствах, или нажмите на кнопку **Обзор** и выберите путь.

      По умолчанию используется путь `%SOYUZAPPDATA%\Quarantine\`. Папка Quarantine будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

      Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent.

      Пример:
      Если на устройстве установлена операционная система Windows 7 и программа Kaspersky Endpoint Agent установлена на диске C, путь к папке карантина будет следующим:
      `C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Quarantine`

b. Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер Карантина (МБ)** и укажите или выберите в списке максимальный размер карантина в мегабайтах.

Например, вы можете задать максимальный размер карантина 200 МБ.

При достижении максимального размера карантина Kaspersky Endpoint Agent публикует соответствующее событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

c. Чтобы задать пороговое значение карантина (место в карантине, оставшееся до достижения максимального размера карантина), установите флажок **Пороговое значение места на диске (МБ)**.

Например, вы можете задать пороговое значение карантина 50 МБ.

При достижении порогового значения карантина Kaspersky Endpoint Agent публикует соответствующее событие на сервере Kaspersky Security Center и в Журнале событий Windows, но не перестает помещать новые объекты на карантин.

6. В разделе **Восстановление объектов из Карантина** в поле **Папка для восстановленных объектов** укажите путь, по которому будет создана папка для объектов, восстановленных из карантина.

По умолчанию используется путь `%SOYUZAPPDATA%\Restored\`. Папка Restored будет создана на всех устройствах с Kaspersky Endpoint Agent по следующему пути: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

Значение переменной `%ALLUSERSPROFILE%` зависит от операционной системы устройства, на котором установлена программа Kaspersky Endpoint Agent.

Пример:
Если на устройстве установлена операционная система Windows 7 и программа Kaspersky Endpoint Agent установлена на диске C, путь к папке восстановленных из карантина объектов будет следующим:
`C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored`

7. Если вы настраиваете параметры политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

8. Нажмите на кнопки **Применить** и **ОК**.

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

Настройка синхронизации данных с Сервером администрирования

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете настроить синхронизацию данных об объектах, помещенных на карантин на управляемых устройствах, с Сервером администрирования Kaspersky Security Center.

Чтобы настроить синхронизацию данных с Сервером администрирования:

1. Выполните одно из следующих действий:

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

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

   - **Откройте окно свойств политики программы**.

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

2. В разделе **Репозитории** выберите подраздел **Синхронизация с Сервером администрирования**.
3. Установите флажок **Данные об объектах в Карантине на управляемых устройствах**.
4. Нажмите на кнопку **ОК**.
5. Нажмите на кнопку **Сохранить**.

Синхронизация данных с Сервером администрирования будет настроена.

Настройка диагностики сбоев

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Чтобы настроить диагностику сбоев:

1. **Откройте окно свойств программы для отдельного устройства**.
    1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
    2. Выберите устройство.
    3. В открывшемся окне **<Имя устройства>** выберите закладку **Программы**.
    4. Выберите **Kaspersky Endpoint Agent**.
    5. В открывшемся окне выберите закладку **Параметры программы**.
2. В разделе **Параметры программы** выберите подраздел **Диагностика сбоев**.
3. Если вы хотите включить запись отладочной информации в файлы трассировки:
    a. Включите параметр **Записывать отладочную информацию в файлы трассировки**.
    b. В поле **Папка файлов трассировки** укажите путь к папке на устройстве, в которую программа должна сохранять файлы трассировки.

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

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

    По умолчанию задано 50 МБ. При достижении заданного размера файла программа продолжает запись в новый файл.
4. Если вы хотите, чтобы программа выполняла перезапись старых файлов трассировки:
    a. Включите параметр **Перезаписывать старые файлы трассировки**.
    b. В поле **Максимальное количество файлов для одного журнала трассировки** укажите желаемое значение.

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

5. Если вы хотите включить запись файлов дампа:

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

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

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

6. Нажмите на кнопку **OK**.

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

Управление задачами Kaspersky Endpoint Agent

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

Создание задач

> В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы создать задачу:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Agent**.
4. В раскрывающемся списке **Тип задачи** выберите нужный тип задачи и следуйте дальнейшим шагам мастера.
5. Чтобы изменить заданные по умолчанию значения параметров задачи сразу после ее создания, установите флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**.

   Если вы не установите этот флажок, задача будет создана с заданными по умолчанию значениями параметров, которые вы можете изменить позже в любое время для каждого из следующих типов задач:

   - Активация программы
   - Поиск IOC
   - Аудит безопасности

- **Удалить файл**
- **Поместить файл на карантин**
- **Завершить процесс**
- **Запустить процесс**
- **Обновление баз и модулей программы**

6. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Просмотр списка задач

Чтобы просмотреть список задач,

в главном окне веб-консоли перейдите в раздел **Устройства** → **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям программ, к которым они относятся.

Удаление задач из списка

Чтобы удалить задачи из списка задач на сервере Kaspersky Security Center:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
   Отобразится список задач.
2. В отобразившемся списке задач установите флажки напротив задач, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
   Откроется окно подтверждения действия.
4. Нажмите на кнопку **Да**.

Выбранные задачи будут удалены из списка.

Настройка расписания запуска задач

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить запуск задачи по расписанию:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. На закладке **Расписание** в разделе **Общие** переведите переключатель из положения **Расписание выключено** в положение **Запускать по расписанию**.
4. В раскрывающемся списке **Периодичность** выберите один из следующих вариантов: **В указанное время**, **Каждый час**, **Каждый день**, **Каждую неделю** или **При запуске программы**.
5. Если вы выбрали запуск задачи **В указанное время**, укажите время и дату запуска задачи.
6. Если вы выбрали запуск задачи **Каждый час**, **Каждый день** или **Каждую неделю**, настройте параметры запуска задачи:
   a. В поле **Каждый** задайте периодичность запуска задачи. Например, 1 раз в день или 2 раза в неделю по вторникам и четвергам.
   b. В полях **Время запуска** и **Дата запуска** задайте время и дату начала действия расписания.
7. Чтобы выполнить расширенную настройку расписания, выберите раздел **Дополнительно** и выполните следующие действия:
   a. Если вы хотите задать максимальное время ожидания выполнения задачи, установите флажок **Завершать задачу, выполняющуюся более** и укажите, через сколько часов и минут задача будет автоматически завершаться.
   b. Если вы хотите, чтобы расписание запуска задачи действовало до определенной даты, установите флажок **Отменить расписание с** и укажите дату окончания действия расписания.
   c. Если вы хотите, чтобы программа при первой возможности запускала задачи, не выполненные вовремя, установите флажок **Запускать пропущенные задачи**.
   d. Если вы хотите избежать одновременного обращения большого количества устройств к Серверу администрирования и запускать задачу на устройствах не точно по расписанию, а случайным образом в течение определенного интервала времени, установите флажок **Распределять время запуска задач в интервале** и задайте интервал запуска в минутах.
8. Нажмите на кнопку **Сохранить**.

Запуск задач вручную

Программа запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время.

Чтобы запустить задачу вручную:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

   Задача будет запущена. Вы можете проверить статус задачи в графе **Статус** или нажав на кнопку **Результат выполнения**.

Создание задач активации Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете активировать Kaspersky Endpoint Agent с помощью лицензионного ключа из хранилища ключей Kaspersky Security Center. Подробную информацию об управлении лицензионными ключами с помощью Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Чтобы создать задачу активации Kaspersky Endpoint Agent:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Agent**.
4. В раскрывающемся списке **Тип задачи** выберите **Активация программы**.
5. В поле **Название задачи** задайте отображаемое имя задачи.
6. Если вы хотите создать задачу для устройств определенной группы Сервера администрирования, выполните следующие действия:

   a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Группа устройств** и нажмите **Далее**.

   b. Выберите нужную группу Сервера администрирования и нажмите **Далее**.

7. Если вы хотите создать задачу для определенных устройств по диапазону IP-адресов, NetBIOS-именам, DNS-именам или выбрать из списка устройств, обнаруженных в сети Сервером администрирования, выполните следующие действия:

   a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Выбранные устройства или импортируемые устройства из списка** и нажмите **Далее**.

   b. Добавьте в список устройства по нужным критериям и нажмите **Далее**.

8. Если вы хотите создать задачу для устройств из определенной выборки, выполните следующие действия:

   a. В блоке параметров **Выбор устройств, которым будет назначена задача** выберите **Выборка** и нажмите **Далее**.

   b. Укажите нужную выборку из списка и нажмите **Далее**.

9. В окне **Выберите лицензионный ключ** выберите нужный лицензионный ключ из списка доступных в хранилище ключей Kaspersky Security Center.

10. Если вы хотите добавить этот лицензионный ключ в качестве дополнительного для автоматического продления срока действия лицензии, установите флажок **Использовать в качестве дополнительного ключа**.

11. Нажмите **Далее**.

12. В окне **Выбор учетной записи для запуска задачи** выберите нужную учетную запись и нажмите **Далее**.

13. Чтобы изменить заданные по умолчанию значения параметров задачи сразу после ее создания, установите флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**.

14. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Настройка параметров задачи обновления баз и модулей программы

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи обновления баз и модулей программы:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Параметры подключения**.
5. Если вы используете Kaspersky Security Center, в блоке параметров **Источник обновлений** выберите один из следующих вариантов:
   - **Сервер администрирования Kaspersky Security Center**.
   - **Серверы обновлений "Лаборатории Касперского"**.
   - **Другие HTTP-, FTP-серверы или сетевые папки**.
6. Если вы используете Kaspersky Security Center Cloud Console, в блоке параметров **Источник обновлений** выберите один из следующих вариантов:
   - **Точки распространения**. Использование в качестве источника обновлений устройства с установленным Агентом администрирования.

     Подробная информация об использовании точек распространения доступна в справке Kaspersky Security Center Cloud Console.
   - **Серверы обновлений "Лаборатории Касперского"**. Использование в качестве источника обновлений серверов обновлений "Лаборатории Касперского".
7. Если вы хотите включить параметр **Использовать серверы обновлений "Лаборатории Касперского", если указанные пользователем серверы недоступны**, установите флажок рядом с названием параметра.

   Недоступно в Kaspersky Security Center Cloud Console.
8. Если вы выбрали источник обновления баз **Другие HTTP-, FTP-серверы или сетевые папки**, выполните следующие действия:

   Недоступно в Kaspersky Security Center Cloud Console.

   a. Нажмите на ссылку **Параметры**, чтобы открыть окно **Пользовательские источники обновлений**.

   b. Добавьте источники обновлений в список, выполнив следующие действия:

      1. Нажмите на кнопку **Добавить**.
      2. В открывшемся диалоговом окне в поле **Веб-адрес** введите адрес сервера обновлений (HTTP или FTP), либо путь к сетевой или локальной папке, содержащей файлы обновлений, и нажмите на кнопку **OK**.

3. Если вы хотите использовать этот источник для обновления баз, установите переключатель рядом с его адресом в положение **Включить**.

   Выполняйте аналогичные действия для добавления каждого нового источника.

4. Нажмите на кнопку **OK**.

   Окно **Пользовательские источники обновлений** закроется.

9. Выберите раздел **Параметры обновления**.

10. В блоке параметров **Параметры обновления** выберите, при каких условиях программа будет проверять доступность обновлений модулей программы:

    - **Не проверять доступность обновлений**. Kaspersky Endpoint Agent не будет проверять доступность обновлений модулей программы.
    - **Только проверять наличие важных обновлений модулей программы**. Kaspersky Endpoint Agent будет проверять доступность только важных обновлений модулей программы.
    - **Загружать и устанавливать важные обновления модулей программы**. Kaspersky Endpoint Agent будет проверять доступность обновлений модулей программы и будет загружать и устанавливать критические обновления модулей программы.

11. Если вы хотите, чтобы программа отображала уведомление обо всех плановых обновлениях программных модулей, имеющихся в источнике обновлений, установите флажок **Получать информацию о доступных запланированных обновлениях модулей программы**.

12. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Управление стандартными задачами поиска IOC

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

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

Требования к IOC-файлам

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

- Kaspersky Endpoint Agent поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.
- Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
- Если при создании задачи Поиск IOC все загруженные вами IOC-файлы не поддерживаются Kaspersky Endpoint Agent, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации.
- Семантические ошибки и неподдерживаемые программой IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов программа фиксирует отсутствие совпадения.
- Идентификаторы всех IOC-файлов, которые используются в одной задаче Поиск IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- Размер одного IOC-файла не должен превышать 3 МБ. Использование файлов большего размера приводит к завершению задач Поиск IOC с ошибкой. При этом суммарный размер всех добавленных файлов в IOC-коллекции может превышать 3 МБ.
- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

В таблице ниже приведены особенности и ограничения поддержки стандарта OpenIOC программой.

Поддерживаемые условия	OpenIOC 1.0:
	
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Поддерживаемые атрибуты условий	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Поддерживаемые операторы	`AND` `OR`
Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is, greater-than, less-than`)

Особенности интерпретации типов данных	Типы данных `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` интерпретируются как строка (string).
	
	Программа поддерживает интерпретацию параметра `Content` для типов данных `int` и `date`, заданного в виде промежутков:
	
	OpenIOC 1.0:
	С использованием оператора `TO` в поле `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	С помощью условий `greater-than` и `less-than`
	С использованием оператора `TO` в поле `Content`
	Программа поддерживает интерпретацию типов данных `date` и `duration`, если индикаторы заданы в формате `ISO 8601, Zulu time zone, UTC`.

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

Поддерживаемые IOC-термины

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX

Настройка параметров стандартной задачи поиска IOC

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

Чтобы настроить параметры стандартной задачи поиска IOC:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В разделе **Параметры поиска IOC** настройте IOC-коллекцию, выполнив следующие действия:
   a. В блоке параметров **IOC-коллекция** нажмите на кнопку **Переопределить IOC-файлы**.
   b. В открывшемся диалоговом окне нажмите на кнопку **Добавить IOC-файлы** и укажите IOC-файлы, которые вы хотите использовать для задачи.

      Для одной задачи поиска IOC можно выбрать несколько IOC-файлов.
   c. Нажмите на кнопку **OK**, чтобы закрыть диалоговое окно.

      Если при создании задачи Поиск IOC вы загрузите IOC-файлы, часть из которых не поддерживается Kaspersky Endpoint Agent, то при запуске задачи программа будет использовать только поддерживаемые IOC-файлы.
   d. Если вы хотите посмотреть список всех IOC-файлов, которые включены в IOC-коллекцию, а также получить информацию о каждом IOC-файле, выполните следующие действия:
      1. Нажмите на ссылку с именами всех загруженных IOC-файлов в блоке параметров **IOC-файлы**.

         Откроется окно **Содержимое IOC ()**.
      2. Чтобы просмотреть детальную информацию об отдельном IOC-файле, на закладке **IOC-коллекция** в списке файлов нажмите на имя нужного IOC-файла.

         В открывшемся окне отображена информация о выбранном IOC-файле.

3. Чтобы закрыть окно с информацией о выбранном IOC-файле, нажмите на кнопку **OK** или **Отмена**.

4. Чтобы просмотреть информацию сразу обо всех загруженных IOC-файлах, перейдите на закладку **Данные IOC**.

   В рабочей области окна отображена информация о каждом загруженном IOC-файле.

5. Если вы хотите, чтобы определенный IOC-файл не использовался при запуске задачи поиска IOC, на закладке **IOC-коллекция** переведите переключатель рядом с его именем из положения **Включить** в положение **Исключить**.

6. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Содержимое IOC ()**.

e. Если вы хотите экспортировать созданную IOC-коллекцию, нажмите на кнопку **Экспортировать IOC-коллекцию**.

   В открывшемся окне можно задать имя файла, а также выбрать папку, в которую вы хотите его сохранить.

f. Нажмите на кнопку **Сохранить**.

   Программа создаст файл формата ZIP в указанной папке.

g. В блоке параметров **Ретроспективный поиск IOC** настройте параметры ретроспективного режима поиска IOC:

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

   2. Укажите временной интервал.

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

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

h. В блоке параметров **Действия** настройте ответные действия при обнаружении индикатора компрометации:

   1. Установите флажок **Принять ответные действия при обнаружении индикатора компрометации**.

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

   3. Установите флажок **Поместить на карантин и удалить**, чтобы поместить обнаруженный объект на карантин и удалить его с устройства.

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

Если включен параметр **Поместить на карантин и удалить** или **Запустить проверку важных областей**, в качестве ответных действий Kaspersky Endpoint Agent может признать обнаруженные файлы зараженными и удалить их с устройства.

i. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите защитить критические системные файлы от помещения на карантин и удаления при обнаружении индикатора компрометации.

Опция доступна, только если в блоке параметров **Действия** выбрано **Поместить на карантин и удалить**.

При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.

5. В разделе **Дополнительно** выберите типы данных (IOC-документы), которые необходимо анализировать во время выполнения задачи, и настройте дополнительные параметры поиска:

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

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

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

b. Если установлен флажок **Анализировать данные файлов (FileItem)**, нажмите на ссылку **Дополнительно (FileItem)** и в открывшемся окне **Параметры проверки документа FileItem** выберите области на дисках защищаемого устройства, в которых необходимо искать индикаторы компрометации.

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

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

d. Если установлен флажок **Анализировать данные WEL (EventLogItem)**, нажмите на ссылку **Дополнительно (EventLogItem)** и в открывшемся окне **Параметры проверки документа EventLogItem** настройте дополнительные параметры анализа событий:

- **Проверять только события, зафиксированные в течение указанного периода**.

  Если флажок установлен, во время выполнения задачи учитываются только те события, которые были зафиксированы в указанный период.

- **Проверять события, относящиеся к следующим каналам**.

  Список каналов, которые анализируются во время выполнения задачи.

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

6. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Просмотр результатов выполнения задачи поиска IOC

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы просмотреть результаты выполнения задачи Поиск IOC:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Результаты поиска IOC**.
5. В раскрывающемся списке **Устройство** выберите, для каких устройств вы хотите просмотреть результаты выполнения задачи поиска IOC.

   Отобразится сводная таблица результатов выполнения задачи на выбранных устройствах.

   Если на устройствах обнаружены индикаторы компрометации, в столбце **Результаты** отображается *обнаружены индикаторы компрометации*.
6. Если вы хотите просмотреть подробную информацию об обнаруженных индикаторах компрометации на определенном устройстве, выполните следующие действия:

   a. Нажмите на ссылку **обнаружены индикаторы компрометации** в строке с именем нужного устройства.

      Откроется окно **Результаты поиска IOC** со списком всех IOC-файлов, использованных в рамках задачи. Если на выбранном устройстве присутствует объект, который совпадает с определенным индикатором компрометации, в столбце **Статус** отображается *совпадает*.

   b. Нажмите на ссылку **совпадает** в строке с именем нужного IOC-файла.

      Откроется окно **Карточка инцидента IOC**.

      Карточка инцидента IOC содержит информацию об объектах на устройстве, совпавших с условиями обработанного IOC-файла, а также текст совпавших веток или отдельных условий из этого IOC-файла.

      Просмотр Карточки инцидента IOC недоступен для IOC-файлов, при проверке которых не было обнаружено совпадений на устройстве.

Настройка параметров задачи Поместить файл на карантин

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы считаете, что на компьютере находится зараженный или возможно зараженный файл, вы можете изолировать его, поместив на карантин.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи Поместить файл на карантин:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В раскрывающемся списке **Укажите файл, который требуется поместить на карантин** выберите одно из следующих значений: **Указать файл по полному пути** или **Задать файл по пути к папке и контрольной сумме**.
5. Если вы выбрали **Указать файл по полному пути**, укажите значение в поле **Полный путь к файлу**.
6. Если вы выбрали **Задать файл по пути к папке и контрольной сумме**, настройте следующие параметры:
   - В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **MD5** или **SHA256**.
   - Укажите значение в поле **Контрольная сумма файла**.
   - Укажите значение в поле **Путь к папке файла**.
7. В блоке параметров **Действия после помещения файла на карантин** выберите, необходимо ли удалять файл с защищаемого устройства после помещения на карантин.

   Если файл заблокирован другим процессом, то файл будет удален только после перезагрузки устройства.

8. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

   При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.

9. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет помещен на карантин только после перезагрузки устройства. Рекомендуется проверить успешность выполнения задачи после перезагрузки устройства.

Задача помещения файла на карантин может завершиться с ошибкой *Доступ запрещен*, если вы пытаетесь поместить на карантин исполняемый файл, и он запущен в настоящий момент. Чтобы решить проблему, создайте задачу завершения процесса для этого файла, а затем повторите попытку создания задачи помещения файла на карантин.

Настройка параметров задачи Удалить файл

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи Удалить файл:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В списке **Файл, который нужно удалить** нажмите на кнопку **Добавить**.
5. Откроется диалоговое окно **Файл, который нужно удалить**.

6. В раскрывающемся списке **Укажите файл, который нужно удалить** выберите одно из следующих значений: **Указать файл по полному пути** или **Задать файл по пути к папке и контрольной сумме**.

7. Если вы выбрали **Указать файл по полному пути**, укажите значение в поле **Полный путь к файлу**.

8. Если вы выбрали **Задать файл по пути к папке и контрольной сумме**, настройте следующие параметры:

   - В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **MD5** или **SHA256**.
   - Укажите значение в поле **Контрольная сумма файла**.
   - Укажите значение в поле **Путь к папке файла**.
   - Установите флажок **Включить подпапки**, чтобы программа удаляла все вхождения объекта не только в указанной папке, но и во всех ее подпапках.

9. Нажмите на кнопку **OK**, чтобы добавить заданный объект в список **Файл, который нужно удалить**.

   Вы можете указать несколько объектов для удаления в рамках одной задачи Удалить файл.

10. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

    При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.

11. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки устройства. Рекомендуется проверить успешность удаления файла после перезагрузки устройства.

Удаление файла с подключенного сетевого диска не поддерживается.

Настройка параметров задачи Запустить процесс

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Задача Запустить процесс позволяет запустить необходимую программу или команду на устройстве.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи Запустить процесс:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства** → **Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. Если вы хотите запустить программу с помощью командной строки (cmd.exe) или выполнить команду, введите необходимую команду в поле **Исполняемая команда**.
5. Если вы хотите запустить программу напрямую, выполните следующие действия:
   a. Укажите путь к исполняемому файлу программы в поле **Рабочая папка**.
   b. Укажите ключи запуска программы в поле **Аргументы**.
6. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Настройка параметров задачи Завершить процесс

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Если вы считаете, что запущенный на устройстве процесс может угрожать безопасности устройства или локальной сети организации, вы можете завершить его.

Создание задачи выполняется предварительно отдельным этапом.

Если во время создания задачи, вы установили флажок **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, то переходите сразу к пункту 4 приведенной далее инструкции.

Чтобы настроить параметры задачи Завершить процесс:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Устройства → Задачи**.
2. Чтобы открыть окно настройки параметров задачи, нажмите на имя задачи.
3. Выберите закладку **Параметры программы**.
4. В поле **Полный путь к файлу** укажите путь к файлу процесса, который вы хотите завершить.
5. В раскрывающемся списке **Тип контрольной суммы** выберите одно из следующих значений: **Не задан**, **MD5** или **SHA256**.
6. Если вы выбрали **MD5** или **SHA256**, укажите значение в поле **Контрольная сумма**.
7. Если вы хотите, чтобы программа учитывала регистр символов в пути к файлу процесса, установите флажок **Путь с учетом регистра символов**.
8. В блоке параметров **Защита критических системных файлов** установите флажок **Не выполнять действий над критическими системными файлами**, если вы хотите исключить критические системные файлы из области применения задачи.

   При выбранной опции, если объект оказывается критическим системным файлом, программа не выполняет никаких действий с этим объектом. Информация об этом записывается в отчете о выполнении задачи.
9. Нажмите на кнопку **Сохранить**.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию.

Управление Kaspersky Endpoint Agent через интерфейс командной строки

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Программой Kaspersky Endpoint Agent можно управлять через интерфейс командной строки. Функциональность интерфейса командной строки обеспечивает утилита agent.exe. Утилита agent.exe входит в комплект поставки программы Kaspersky Endpoint Agent и устанавливается на каждое устройство вместе с Kaspersky Endpoint Agent в папку `%ProgramFiles%\Kaspersky Lab\Endpoint Agent` (если на устройстве установлена 32-разрядная операционная система) или `%ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent` (если на устройстве установлена 64-разрядная операционная система).

Пример:
Если на устройстве установлена 64-разрядная операционная система Windows и для установки программы Kaspersky Endpoint Agent вы выбрали установку на диск C, то при установке утилита agent.exe будет размещена в следующую папку:
`C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\`

Чтобы управлять программой Kaspersky Endpoint Agent через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите команду: `agent.exe --<параметр программы, который вы хотите настроить>=<действие над параметром, которое вы хотите выполнить>` и нажмите на клавишу **ENTER**.

   Отобразится результат выполнения команды (код возврата).

Для вызова справки по всем доступным к управлению параметрам программы и их возможным значениям,

выполните команду: `agent.exe --help`

Управление активацией Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы управлять активацией программы через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:

   - Чтобы активировать программу с помощью кода активации или файла ключа:

     `agent.exe --license=add <код активации или путь к файлу ключа>`

     Для активации программы с помощью кода активации защищаемое устройство должно быть подключено к интернету.

   - Чтобы указать дополнительный ключ для автоматического продления срока действия лицензии:

     `agent.exe --license=reserve <код активации или путь к файлу ключа>`

   - Чтобы удалить добавленный основной или дополнительный ключ:

     `agent.exe --license=delete <серийный номер ключа>`

- Чтобы просмотреть статус добавленных ключей:

  `agent.exe --license=show`

Коды возврата команды `--license`:

- `-305` – срок действия добавляемого ключа истек.
- `2` – неопределенная программная ошибка.
- `-302` – добавляемый ключ находится в списке запрещенных ключей.
- `-301` – добавляемый ключ не подходит для активации Kaspersky Endpoint Agent.
- `-303` – файл ключа поврежден.
- `4` – синтаксические ошибки.
- `-304` – указан некорректный путь к файлу ключа.

Управление аутентификацией Kaspersky Endpoint Agent

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

Чтобы управлять аутентификацией программы через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **Enter**.
3. Выполните следующую команду и нажмите на клавишу **Enter**:

   `agent.exe --proxy={enable|disable|show} --mode={auto|custom} --server=<адрес_прокси-сервера> --port=<номер_порта> --use-auth={yes|no} --proxy-user=<имя_пользователя> --proxy-password=<пароль_пользователя> --bypass-local={yes|no}`

Описание параметров аутентификации представлено в следующей таблице:

Параметры команды аутентификации.

Параметры	Описание
`--proxy={enable|disable|show}`	Обязательный параметр. Параметр управляет подключением к прокси-серверу. Доступны следующие значения: `enable` – включает использование прокси-сервера. `disable` – отключает использование прокси-сервера. `show` – отображает текущие настройки использования прокси-сервера. Указанный прокси-сервер будет использоваться для работы с Kaspersky Security Network и для обновления баз. Настройки указанного прокси-сервера можно применять для интеграции с другими системами сбора статистики, при этом в параметрах интеграции потребуется отдельно включить использование указанного прокси-сервера.
--mode={auto|custom}	Обязательный параметр. Параметр устанавливает режим настройки прокси-сервера. Доступны следующие значения: `auto` – автоматическое определение прокси-сервера. `custom` – ручная настройка параметров доступа к прокси-серверу.
--server=< адрес_прокси-сервера >	Обязательный параметр. Параметр указывает адрес прокси-сервера.
--port=< номер_порта >	Обязательный параметр. Параметр указывает порт подключения к прокси-серверу.
--use-auth={yes|no}	Необязательный параметр. Параметр указывает необходимость аутентификации на прокси-сервере. Доступны следующие значения: `yes` – для подключения к прокси-серверу необходимо указать имя пользователя и пароль. `no` – подключение к прокси-серверу возможно без указания имени пользователя и пароля. Используется по умолчанию.
--proxy-user=< имя_пользователя >	Необязательный параметр. Параметр указывает имя пользователя для подключения к прокси-серверу. По умолчанию используется пустое значение.
--proxy-password=< пароль_пользователя >	Необязательный параметр. Параметр указывает пароль для подключения к прокси-серверу. По умолчанию используется пустое значение.
--bypass-local={yes|no}	Необязательный параметр. Параметр устанавливает режим прямого подключения к локальным адресами без использования прокси-сервера. Доступные значения: `yes` –подключения к адресам внутри текущей локальной сети будут осуществляться без прокси-сервера. Используется по умолчанию. `no` – подключения к адресам текущей локальной сети и к внешним адресам будут осуществляться через прокси-сервер.

Настройка трассировки

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

Чтобы настроить трассировку в программе Kaspersky Endpoint Agent через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:

   - `agent.exe --trace=enable --folder <путь к папке для сохранения файлов трассировки>`, чтобы включить трассировку.

     Трассировка будет включена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы трассировки будут создаваться в папке, которую вы указали.

     Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе файлы трассировки не будут созданы.

   - `agent.exe --trace=enable --folder <путь к папке для сохранения файлов трассировки> --rotation=yes --rotate-file-size=<максимальный размер файла в МБ> --rotate-files-count=<максимальное количество файлов>`, чтобы включить трассировку в режиме перезаписи старых файлов трассировки при достижении указанных значений размера и количества файлов.

     Указанное ограничение по количеству файлов применяется для каждого отлаживаемого процесса Kaspersky Endpoint Agent отдельно, поэтому суммарное количество файлов для всех процессов может превышать заданное значение. Если с параметром `--rotation=yes` не указать параметры `--rotate-file-size` или `--rotate-files-count` (один из, или оба), то программа использует значения по умолчанию. По умолчанию задан 1 файл размером в 50 МБ.

   - `agent.exe --trace=disable`, чтобы выключить трассировку.

     Трассировка будет отключена для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент.

   - `agent.exe --trace=show`, чтобы просмотреть текущее состояние трассировки и путь к папке для сохранения файлов трассировки.

     Отобразятся значения параметров `trace.enable` (`true`, если трассировка включена или `false`, если трассировка отключена) и `trace.folder` (путь к папке).

Коды возврата команды `--trace`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.

- 4 – синтаксическая ошибка.
- 5 – объект не найден (не найден путь, указанный в качестве пути к папке с файлами журнала трассировки).
- 9 – неверная операция (например, попытка выполнения команды `--trace=disable`, если трассировка уже отключена).

Настройка создания дампа процессов Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы настроить создание дампа процессов Kaspersky Endpoint Agent через интерфейс командной строки программы:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:

   - `agent.exe --dump=enable --folder <путь к папке, в которой вы хотите создавать дамп>`, чтобы включить создание дампа процессов Kaspersky Endpoint Agent.

     Создание дампа будет включено для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент. Файлы дампа будут создаваться в папке, которую вы указали.

     Убедитесь, что папка, которую вы указали, доступна на управляемом устройстве. Иначе файлы дампа не будут созданы.

   - `agent.exe --dump=disable`, чтобы отключить создание дампа.

     Создание дампа будет отключено для всех процессов Kaspersky Endpoint Agent, запущенных в текущий момент.

   - `agent.exe --dump=show`, чтобы просмотреть текущее состояние создания дампа и путь к папке с файлами дампа.

     Отобразятся значения параметров `dump.enable` (`true`, если создание дампа включено или `false`, если создание дампа отключено) и `dump.folder` (путь к папке).

Коды возврата команды `--dump`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.

- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 5 – объект не найден (не найден путь, указанный в качестве пути к папке с файлами дампа).
- 9 – неверная операция (например, попытка выполнения команды `--dump=disable`, если создание дампа уже отключено).

Просмотр информации о параметрах карантина и объектах на карантине

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы просмотреть информацию о параметрах карантина и объектах, находящихся на карантине, через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите одну из следующих команд и нажмите на клавишу **ENTER**:

   - `agent.exe --quarantine=show [--pwd=<текущий пароль пользователя>]`, чтобы просмотреть список объектов, помещенных на карантин.

   Отобразится следующая информация обо всех объектах, находящихся в папке карантина, указанной при настройке параметров карантина:

   - Идентификаторы объектов, помещенных на карантин к текущему моменту (параметр `ouid`).
   - Имена объектов, помещенных на карантин (имя + расширение).
   - Дата и время помещения объекта на карантин (UTC).
   - Исходный путь к файлу, помещенному на карантин, и путь восстановления файла из карантина, заданный по умолчанию (без имени файла).
   - Размер файла, помещенного на карантин (в байтах).
   - Учетная запись пользователя, с правами которой выполнялась задача помещения файла на карантин.

- Статус объекта:
  - `DETECT`, если файл был помещен на карантин программой EPP или в рамках действий по реагированию на угрозу, обнаруженную Kaspersky Sandbox. Например, в результате локального действия **Поместить на карантин и удалить** или глобального действия **Поместить на карантин и удалить при обнаружении IOC**.
  - `CUSTOM`, если файл был помещен на карантин вручную, в результате выполнения команды `--quarantine=add`.
- Способ, которым файл был помещен на карантин:
  - `AUTOMATIC_<название программы, обнаружившей угрозу в файле, помещенном на карантин>`, если файл был помещен на карантин программой EPP или в рамках действий по реагированию на угрозу, обнаруженную Kaspersky Sandbox. Например, в результате локального действия **Поместить на карантин и удалить** или глобального действия **Поместить на карантин и удалить при обнаружении IOC**.
  - `BY USER`, если файл был помещен на карантин вручную, в результате выполнения команды `--quarantine=add`.
- `agent.exe --quarantine=limits`, чтобы просмотреть текущие значения параметров **Максимальный размер Карантина (МБ)** и **Пороговое значение места на диске (МБ)**, а также статусы применения этих параметров (статусы флажков), заданные при настройке параметров карантина.

Коды возврата команды `--quarantine`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Действия над объектами на карантине

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы выполнить действия над объектами, находящимися на карантине программы Kaspersky Endpoint Agent через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.

2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

3. Выполните следующие действия и нажмите на клавишу **ENTER**:

   - Если вы хотите безвозвратно удалить объекты, находящиеся на карантине, выполните команду:

     `agent.exe --quarantine=delete --ouid=<` идентификаторы объектов на карантине через запятую. Обязательный параметр `> [--pwd=<` текущий пароль пользователя `>]`.

     Объекты с указанными идентификаторами будут удалены из папки карантина , указанной при настройке параметров карантина.

   - Если вы хотите восстановить объекты из карантина, выполните команду:

     `agent.exe --quarantine=restore --ouid=<` идентификаторы объектов на карантине через запятую. Обязательный параметр `> [--path-type=<` один из вариантов выбора папки назначения при восстановлении объекта из карантина: `original|custom|settings`. Необязательный параметр `> --path=<` путь к папке назначения для восстановленных объектов. Обязательный параметр, если передан параметр `--path-type` и указано значение `original>] [--action=<` одно из действий над объектом: `replace|rename`. Необязательный параметр `>] [--pwd=<` текущий пароль пользователя `>]`.

   - Если вы хотите поместить объект на карантин, выполните одну из следующих команд:

     - `agent.exe --quarantine=add [--file=<` полный путь к объекту, который вы хотите поместить на карантин `>] [--pwd=<` текущий пароль пользователя `>]`.

     - `agent.exe --quarantine=add [--hash=<` хеш объекта, который вы хотите поместить на карантин. Обязательный параметр, если вы не указываете полный путь к объекту и передаете параметр `--hashalg >]--hashalg=<` один из типов хеша: `md5|sha256`. Обязательный параметр, если вы не указываете полный путь к объекту `> [--file=<` путь к папке с объектом, который вы хотите поместить на карантин `>] [--pwd=<` текущий пароль пользователя `>]`.

Параметры команд при выполнении действий над объектами на карантине

Параметр	Описание
`--ouid`	Обязательный параметр. В параметре передается уникальный числовой (int64) идентификатор объекта на карантине. Отображается при просмотре информации об объектах на карантине (команда `--quarantine=show`).

`--path-type=<original|custom|settings>`	Параметр описывает логику выбора папки назначения при восстановлении объекта из карантина. • Если параметр не передан, объект будет восстановлен в исходную папку – папку, в которой находился объект до помещения его на карантин. Если исходная папка недоступна, объект будет восстановлен в папку, указанную при настройке параметров карантина. • Если параметр передан со значением `<original>`, объект будет восстановлен в исходную папку – папку, в которой находился объект до помещения его на карантин. Если исходная папка недоступна, объект будет восстановлен в папку, указанную при настройке параметров карантина. • Если параметр передан со значением `<settings>`, объект будет восстановлен в папку, указанную при настройке параметров карантина. Если папка недоступна, задача завершается с ошибкой. • Если параметр передан со значением `<custom>`, объект будет восстановлен в папку, путь к которой вы укажете для параметра `--path`. Если папка недоступна, задача завершается с ошибкой.
`--path=<` путь к папке назначения для восстановленных объектов `>`	Обязательный параметр, если передан параметр `--path-type` со значением `<custom>`. Параметр определяет путь, по которому вы хотите создать папку для объектов, восстановленных из карантина, если вы не хотите использовать папку, в которой находился объект до помещения его на карантин и папку, указанную при настройке параметров карантина.
`--action=<replace|rename>`	Параметр определяет действие над объектом, которое вы хотите выполнить, если при восстановлении объекта из карантина папка назначения для восстановленных объектов содержит файл с таким же именем. • Если параметр не передан, восстановленный объект будет переименован: к первоначальному имени объекта будет добавлен суффикс `_restored`. • Если параметр передан со значением `<rename>`, восстановленный объект будет переименован: к первоначальному имени объекта будет добавлен суффикс `_restored`. • Если параметр передан со значением `<replace>`, первоначальный объект будет заменен на восстановленный объект.
`--file=<` полный путь к объекту, который вы хотите поместить на карантин `>`	Обязательный параметр, если не передан параметр `--hashalg`. Параметр задает полный путь к объекту, который вы хотите поместить на карантин.
`--hashalg=<md5|sha256>`	Обязательный параметр, если не передан параметр `--file` и не указан полный путь к объекту, который вы хотите поместить на карантин. Параметр задает алгоритм хеширования, по которому будет рассчитана контрольная сумма объекта, который вы хотите поместить на карантин. Параметр может быть передан с одним из двух значений: `<md5>` или `<sha256>`.
`--hash=<контрольная сумма файла>`	Обязательный параметр, если передан параметр `--hashalg`. Параметр задает контрольную сумму объекта, который вы хотите поместить на карантин.
`--file=<папка с файлом>`	Обязательный параметр, если передан параметр `--hashalg`. Параметр задает путь к папке с объектом, который вы хотите поместить на карантин и хеш которого вы указали в параметре `--hash`.
`--pwd=<` текущий пароль пользователя `>`	Позволяет ввести пароль пользователя, под учетной записью которого выполняется команда.

Коды возврата команды `--quarantine`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Управление параметрами интеграции с компонентом KATA Central Node

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы управлять параметрами интеграции программы Kaspersky Endpoint Agent с компонентом KATA Central Node через интерфейс командной строки Kaspersky Endpoint Agent:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.

2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   `agent.exe --message-broker=<enable|disable|show> --type=<kata> --use-proxy={yes|no} --compression=<yes|no> --partitioning-strategy=<automatic|user> [--message-key=<ключ сообщения> --topic=<тема> --partition=<user specific partition>] --tls=<yes|no> --servers=<адрес>:<порт>[;<адрес>:<порт>[; …]] [--timeout=<максимальное время ожидания ответа сервера KATA] [--pinned-certificate=<полный путь к файлу TLS-сертификата>] [--client-certificate=<полный путь к файлу сертификата>] --client-password=<пароль к архиву формата PFX> --sync-period=<период отправки запросов на синхронизацию>`

   Параметры команды `--message-broker` при управлении параметрами интеграции Kaspersky Endpoint Agent с компонентом KATA Central Node

Параметр	Описание
`--message-broker=<enable|disable|show>`	Обязательный параметр. Позволяет включить, отключить и просмотреть состояние программы Kaspersky Endpoint Agent с компонентом KATA Central Node. • `--message-broker=<enable>` включает интеграцию. • `--message-broker=<disable>` отключает интеграцию. • `--message-broker=<show>` отображает состояние интеграции Kaspersky Endpoint Agent с компонентом KATA Central Node.
`--type=<kata>`	Обязательный параметр. Позволяет указать компонент KATA Central Node для управления параметрами интеграции программы Kaspersky Endpoint Agent с этим компонентом.
`--use-proxy={yes|no}`	Обязательный параметр. Позволяет включить и отключить использование прокси-сервера в брокере сообщений для отправки сообщений в KATA.
`--compression=<yes|no>`	Необязательный параметр. Позволяет включить или отключить сжатие данных, передаваемых между Kaspersky Endpoint Agent и компонентом KATA Central Node. По умолчанию включено.

`---tls=<yes|no>`	Необязательный параметр. Позволяет включить или отключить использование доверенного соединения Kaspersky Endpoint Agent с компонентом KATA Central Node. • `--tls=<yes>` включает использование доверенного соединения. • `--tls=<no>` отключает использование доверенного соединения.
`--servers=<адрес>:<порт>[;<адрес>:<порт>[; …]]`	Обязательный параметр. Позволяет добавить один или несколько серверов KATA. Kaspersky Endpoint Agent подключается к первому серверу из списка. Если подключение не удается, Kaspersky Endpoint Agent подключается ко второму серверу и так далее по списку.
`--timeout=<максимальное время ожидания ответа сервера KATA>`	Необязательный параметр. Позволяет задать максимальное время ожидания ответа сервера KATA в миллисекундах.
`--pinned-certificate=<полный путь к файлу TLS-сертификата>`	Обязательный параметр, если передан параметр `--tls` со значением `<yes>`. Позволяет добавить TLS-сертификат соединения Kaspersky Endpoint Agent с сервером KATA.
`--client-certificate=<полный путь к файлу сертификата>`	Позволяет добавить пользовательский сертификат соединения Kaspersky Endpoint Agent с сервером KATA.
`--client-password=<пароль к архиву формата PFX>`	Позволяет ввести пароль к архиву формата PFX, содержащему пользовательский сертификат соединения Kaspersky Endpoint Agent с сервером KATA.
`--sync-period=<период отправки запросов на синхронизацию>`	Позволяет задать период отправки запросов на синхронизацию параметров и задач Kaspersky Endpoint Agent с KATA Central Node.
`--throttling=<yes|no>`	Позволяет включить или выключить регулирование количества запросов. Функция регулирования количества запросов позволяет ограничить поток событий низкой важности от Kaspersky Endpoint Agent к компоненту Central Node.
`--event-limit=<количество событий в час>`	Позволяет задать максимальное количество событий в час. Программа анализирует поток данных телеметрии и ограничивает передачу событий низкой важности, если поток передаваемых событий стремится превысить заданную величину.
`--exceed-limit=<величина порога>`	Позволяет задать порог превышения лимита событий. Если поток однотипных событий низкой важности превысит заданный порог в процентах от общего количества событий, то именно этот тип событий будет ограничен. Можно задать величину от 5 до 100 (без символа `%`).

Запуск обновления баз или модулей Kaspersky Endpoint Agent

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы запустить обновление баз или модулей программы Kaspersky Endpoint Agent через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.

2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   ```
   agent.exe --update=bases|modules [--source=<адреса пользовательских источников обновлений баз, разделенные точкой с запятой без пробела>|kl|ksc]
   ```

Параметры команд при запуске обновления баз Kaspersky Endpoint Agent

Параметр	Описание
`--update=bases|modules`	Обязательный параметр. Позволяет указать тип обновления: • `--update=bases` позволяет запустить обновление баз программы. • `--update=modules` позволяет запустить обновление модулей программы.
`--source=<адреса пользовательских источников обновления баз>|kl|ksc]`	Необязательный параметр. Позволяет выбрать источник обновления баз. • `--source=<адреса пользовательских источников обновлений баз>` позволяет указать источник обновлений баз **Другие HTTP-, FTP-серверы или сетевые папки** и задать путь к сетевой папке или IP-адрес, FTP или HTTP-адрес сервера, с которого программа будет загружать обновления баз. Вы можете указать несколько адресов пользовательских источников обновлений баз, разделенных точкой с запятой без пробела (";"). Программа будет загружать обновления с первого доступного источника обновлений баз. Если все адреса будут недоступны, задача завершится с ошибкой. • `--source=kl` позволяет указать источник обновления баз **Серверы обновлений "Лаборатории Касперского"**. Если серверы будут недоступны, задача завершится с ошибкой. • `--source=ksc` позволяет указать источник обновления баз **Сервер администрирования Kaspersky Security Center**. Если Сервер администрирования будет недоступен, задача завершится с ошибкой.

Коды возврата команды `--update=bases`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 8 – ошибка прав доступа.
- 200 – все объекты актуальны.
- -206 – файлы обновлений отсутствуют в указанном источнике обновлений баз или имеют неизвестный формат.
- -209 – ошибка подключения к источнику обновлений баз.
- -232 – ошибка подключения к прокси-серверу.
- -234 – ошибка подключения к Kaspersky Security Center.
- -236 – базы программы повреждены.

Запуск, остановка и просмотр текущего состояния программы

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы запустить, остановить или просмотреть текущее состояние программы Kaspersky Endpoint Agent через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   `agent.exe --product=<start|stop|state> [--pwd=<текущий пароль пользователя>]`

   Параметры команд при запуске, остановке и просмотре текущего состояния Kaspersky Endpoint Agent

Параметр	Описание
`--product=<start|stop|state>`	Позволяет запустить, остановить или просмотреть текущее состояние программы. • `--product=<start>` запускает программу. • `--product=<stop>` останавливает программу. Если в программе настроена защита паролем, для выполнения команды `--product=<stop>` требуется ввести пароль. • `--product=<state>` отображает текущее состояние программы: запущена или остановлена.
`--pwd=<текущий пароль пользователя>`	Позволяет ввести пароль пользователя, с правами учетной записи которого выполняется команда.

Коды возврата команды `--product=<start|stop|state>`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 8 – ошибка прав доступа.
- 9 – неверная операция (например, попытка выполнения команды `--product=start`, если программа уже запущена).

Защита программы паролем

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы ограничить выполнение действий с программой Kaspersky Endpoint Agent, которые могут привести к снижению уровня защиты компьютера пользователя и данных, обрабатываемых на этом компьютере, а также к снижению уровня самозащиты программы, требуется защитить программу паролем.

Ввод пароля требуется для выполнения следующих команд в интерфейсе командной строки Kaspersky Endpoint Agent:

- `--sandbox=disable`
- `--sandbox=show`
- `--sandbox=enable --tls=no`
- `--sandbox=enable --pinned-certificate=<полный путь к файлу TLS-сертификата соединения Kaspersky Endpoint Agent с Kaspersky Sandbox>`
- `--quarantine=delete –ouid`
- `--quarantine=show`
- `--quarantine=restore`
- `--quarantine=add`
- `--product=stop`
- `--password=reset`
- `--isolation=disable`
- `--prevention=disable`
- `--selfdefense`
- `--license=delete`
- `--message-broker --type=kata <параметры>`
- `--event --action=enable`
- `--event --action=disable`

Для ввода пароля используйте параметр `--pwd=<текущий пароль пользователя>`.

Также требуется вводить пароль при выполнении следующих действий над программой:

- удаление программы и удаленная деинсталляция программы с помощью Kaspersky Security Center;
- обновление программы (`upgrade`);
- восстановление программы (`repair`);
- работа в мастере установки программы;
- работа в интерфейсе командной строки.

После включения защиты паролем и применения политики Kaspersky Security Center, на всех устройствах управляемой группы Kaspersky Endpoint Agent применяется единый пароль.

После отключения защиты паролем в политике параметры защиты паролем сохраняются для локального устройства с возможностью редактирования.

Пароль хранится в параметрах программы в зашифрованном виде (как контрольная сумма).

Для ввода пароля используйте параметр `--pwd=<текущий пароль пользователя>`.

Чтобы настроить защиту паролем программы Kaspersky Endpoint Agent через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --password=state`, чтобы просмотреть текущий статус защиты программы паролем.
   - `agent.exe --password=set --pwd=<текущий пароль пользователя> --new=<новый пароль пользователя>`, чтобы установить новый пароль пользователя.
   - `agent.exe --password=reset --pwd=<текущий пароль пользователя>`, чтобы сбросить пароль пользователя.

Защита служб программы технологией PPL

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

В Kaspersky Endpoint Agent реализована защита служб программы с помощью технологии *Protected Process Light (PPL)*.

Защита служб программы с помощью технологии Protected Process Light (PPL) может применяться только для следующих операционных систем:

- для рабочих станций – Windows 10 версия 1703 RS2 и выше;
- для серверов – Windows Server 2016 версия 1709 и выше.

Процессы, исполняющиеся с признаком PPL, не могут быть остановлены или изменены другими процессами без признака PPL.

Использование признака PPL для служб программы позволяет защитить службы от вредоносных воздействий извне и попыток компрометации.

Чтобы настроить защиту служб программы технологией PPL через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните одну из следующих команд и нажмите на клавишу **ENTER**:
   - `agent.exe --ppl=show [--pwd=<текущий пароль пользователя>]`, чтобы просмотреть текущий статус защиты служб программы технологией PPL.
   - `agent.exe --ppl=disable [--pwd=<текущий пароль пользователя>]`, чтобы отключить защиту служб программы технологией PPL.

Коды возврата команды `--ppl`:

- 0 – команда выполнена успешно.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.
- 8 – ошибка прав доступа.

Управление параметрами самозащиты

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы управлять параметрами самозащиты через интерфейс командной строки Kaspersky Endpoint Agent:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   ```
   agent.exe --selfdefense=<enable|disable>
   ```

Управление фильтрацией событий

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Чтобы управлять фильтрацией событий через интерфейс командной строки Kaspersky Endpoint Agent:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Выполните следующую команду и нажмите на клавишу **ENTER**:

   ```
   agent.exe --event =
   <createprocess|loadimage|registry|network|eventlog|filechange|accountloggon|codeinjecti
   --action=<enable|disable|show>
   ```

Управление стандартными задачами поиска IOC

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

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

В задаче поиска IOC можно указать только файл с IOC-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи поиска IOC.

Чтобы создать и настроить стандартную задачу поиска IOC через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.

2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

3. Выполните следующую команду и нажмите на клавишу **Enter**:

   `agent.exe --scan-ioc {[--path=<путь к папке с IOC-файлами>] | [<полный путь к IOC-файлу>]} [--process=no] [--hint=<полный путь к исполняемому файлу процесса|полный путь к файлу>] [--registry=no] [--dnsentry=no] [--arpentry=no] [--ports=no] [--services=no] [--system=no] [--users=no] [--volumes=no] [--eventlog=no] [--datetime=<дата публикации события>] [--channels=<список каналов>] [--files=no] [--network=no] [--url=no] [--drives=<all|system|critical|custom>] [--excludes=<список исключений>][--scope=<настраиваемый список папок>] [--retro]`

   Если команда `--scan-ioc` передана только с обязательными параметрами, Kaspersky Endpoint Agent выполняет проверку с параметрами по умолчанию.

   Если команда `--scan-ioc` передана с двумя обязательными параметрами одновременно (`--path=<путь к папке с IOC-файлами>` и `<полный путь к IOC-файлу>`), Kaspersky Endpoint Agent выполняет проверку всех переданных IOC-файлов.

Параметры команд при запуске и настройке стандартных задач поиска IOC

Параметры	Описание
`--scan-ioc`	Обязательный параметр. Запускает стандартную задачу поиска IOC на устройстве.
`--path=<путь к папке с IOC-файлами>`	Путь к папке с IOC-файлами, по которым требуется выполнять поиск. Обязательный параметр, если не задан параметр `<полный путь к IOC-файлу>`.
`<полный путь к IOC-файлу>`	Полный путь к IOC-файлу с расширением ioc или xml, по которому требуется выполнять поиск. Обязательный параметр, если не задан параметр `--path=<путь к папке с IOC-файлами>`. Передается без аргумента `--path`.
`--process=<no>`	Необязательный параметр. Параметр выключает анализ данных о процессах при проверке. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не учитывает запущенные на устройстве процессы при выполнении проверки. Если в IOC-файле указаны IOC-термины IOC-документа ProcessItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет данные о процессах, только если IOC-документ ProcessItem описан в переданном на проверку IOC-файле.
`--hint=<полный путь к исполняемому файлу процесса|полный путь к файлу>`	Необязательный параметр. Параметр позволяет сузить область анализируемых данных для проверки IOC-документов ProcessItem и FileItem, путем указания конкретного файла. В качестве значения параметра может быть задан: • `<полный путь к исполняемому файлу процесса (ProcessItem)>` – ProcessItem • `<полный путь к файлу>` – FileItem Параметр может быть передан только совместно с аргументами `--process=yes` и `--files=yes`.

`--dnsentry=no`	Необязательный параметр. Параметр выключает анализ данных о записях в локальном кеше DNS (IOC-документ DnsEntryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет локальный кеш DNS. Если в IOC-файле указаны термины IOC-документа DnsEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет локальный кеш DNS, только если IOC-документ DnsEntryItem описан в переданном на проверку IOC-файле.
`--arpentry=no`	Необязательный параметр. Параметр выключает анализ данных о записях в ARP-таблице (документ ArpEntryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет таблицу ARP. Если в IOC-файле указаны термины IOC-документа ArpEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет ARP-таблицу, только если IOC-документ ArpEntryItem описан в переданном на проверку IOC-файле.
`--ports=no`	Необязательный параметр. Параметр выключает анализ данных о портах, открытых на прослушивание (документ PortItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет таблицу активных соединений на устройстве. Если в IOC-файле указаны термины IOC-документа PortItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет таблицу активных соединений, только если IOC-документ PortItem описан в переданном на проверку IOC-файле.
`--services=no`	Необязательный параметр. Параметр выключает анализ данных о службах, установленных на устройстве (документ ServiceItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет данные о службах, установленных на устройстве. Если в IOC-файле указаны термины IOC-документа ServiceItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет данные о службах, только если IOC-документ ServiceItem описан в переданном на проверку IOC-файле.
`--volumes=no`	Необязательный параметр. Параметр выключает анализ данных о томах (документ VolumeItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет данные о томах на устройстве. Если в IOC-файле указаны термины IOC-документа VolumeItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет данные о томах, только если IOC-документ VolumeItem описан в переданном на проверку IOC-файле.
`--eventlog=no`	Необязательный параметр. Параметр выключает анализ данных о записях в журнале событий Windows (документ EventLogItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не проверяет записи в журнале событий Windows. Если в IOC-файле указаны термины IOC-документа EventLogItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent проверяет записи в журнале событий Windows, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.

`--datetime=< дата публикации события >`	Необязательный параметр. Параметр позволяет включать и выключать учет даты публикации события в журнале событий Windows при определении области поиска IOC для соответствующего IOC-документа. При поиске IOC Kaspersky Endpoint Agent будет обрабатывать только события, опубликованные в период с указанного времени и даты и до момента выполнения задачи. В качестве значения параметра Kaspersky Endpoint Agent позволяет задать дату публикации события. Проверка будет выполняться только для событий, опубликованных в журнале событий Windows после указанной даты и до момента выполнения проверки. Если параметр не передан, Kaspersky Endpoint Agent проверяет события с любой датой публикации. Параметр TaskSettings::BaseSettings::EventLogItem::datetime недоступен для редактирования. Параметр используется, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.
`--channel=< список каналов >`	Необязательный параметр. Параметр позволяет передать список имен каналов (журналов), для которых требуется выполнить поиск IOC. Если этот параметр передан, при выполнении задачи поиска IOC Kaspersky Endpoint Agent будет учитывать только события, опубликованные в указанных журналах. Имя журнала задается в формате строки, в соответствии с именем журнала (канала), указанного в свойствах этого журнала (параметр Full Name) или в свойствах события (параметр <Channel></Channel> в xml-схеме события). По умолчанию (в том числе, если параметр не передан) поиск IOC выполняется для каналов Application, System, Security. Параметру может быть передано несколько значений (через пробел). Параметр используется только в том случае, если IOC-документ EventLogItem описан в переданном на проверку IOC.
`--system=no`	Необязательный параметр. Параметр выключает анализ данных об окружении (IOC-документ SystemInfoItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не анализирует данные об окружении. Если в IOC-файле указаны термины IOC-документа SystemInfoItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent анализирует данные об окружении, только если IOC-документ SystemInfoItem описан в переданном на проверку IOC-файле.
`--users=no`	Необязательный параметр. Параметр выключает анализ данных о пользователях (IOC-документ UserItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не анализирует данные о пользователях, созданных в системе. Если в IOC-файле указаны термины IOC-документа UserItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent анализирует данные о пользователях, созданных в системе, только если IOC-документ UserItem описан в переданном на проверку IOC-файле.
`--files=no`	Необязательный параметр. Параметр выключает анализ данных о файлах (IOC-документ FileItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Endpoint Agent не анализирует данные о файлах. Если в IOC-файле указаны термины IOC-документа FileItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent анализирует данные о файлах, только если IOC-документ FileItem описан в переданном на проверку IOC-файле.
--network=no	Необязательный параметр. Параметр включает поиск угроз на основе IOC-документа Network при поиске IOC. Если параметр передан со значением <no>, Kaspersky Endpoint Agent не выполняет поиск угроз на основе IOC-документа Network. Если в IOC-файле указаны термины IOC-документа Network, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent включает поиск угроз на основе IOC-документа Network, только если IOC-документ Network описан в переданном на проверку IOC-файле.

`--url=no`	Необязательный параметр. Параметр включает поиск угроз на основе IOC-документа UrlHistoryItem при поиске IOC. Если параметр передан со значением <no>, Kaspersky Endpoint Agent не выполняет поиск угроз на основе IOC-документа UrlHistoryItem. Если в IOC-файле указаны термины IOC-документа UrlHistoryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Endpoint Agent включает поиск угроз на основе IOC-документа UrlHistoryItem, только если IOC-документ UrlHistoryItem описан в переданном на проверку IOC-файле.
`--drives=<all|system|critical|custom>`	Необязательный параметр. Параметр позволяет задать область поиска IOC при анализе данных для IOC-документа FileItem. Можно задать одно из следующих значений параметра: • `<all>` – программа проверяет все доступные файловые области. • `<system>` – программа проверяет только файлы, расположенные в папках, в которых установлена ОС. • `<critical>` – программа проверяет только временные файлы в пользовательских и системных папках. • `<custom>` – программа проверяет только файлы в указанных пользователем областях. Если параметр не передан, проверка выполняется в критических областях.
`--excludes=< список исключений >`	Необязательный параметр. Параметр позволяет задать области исключений при анализе данных для IOC-документа FileItem. В параметре можно передать несколько путей через пробел. Если параметр не передан, проверка выполняется без исключений.
`--scope=< настраиваемый список папок >`	Необязательный параметр. Параметр становится обязательным, если передан параметр `--drives=custom`. Параметр позволяет задать список областей проверки. В параметре можно передать несколько путей через пробел.
`--retro`	Необязательный параметр. Параметр передается для запуска задачи в режиме **Ретроспективный поиск IOC** Дополнительно с этим параметром можно передать временной интервал, в рамках которого программа должна выполнять ретроспективный поиск IOC при помощи параметров: • `--start-time=< дата и время начала интервала >` • `--end-time=< время окончания интервала >` Пример: `agent.exe --scan-ioc --path=<путь к папке с IOC-файлами> --retro --start-time=2021-05-21T10:30:00Z --end-time=2021-05-24T10:30:00Z` Если временной интервал не передан, то используется интервал, начинающийся за сутки от момента запуска задачи и заканчивающийся датой и временем в момент запуска задачи.

Коды возврата команды `--scan-ioc`:

- `-1` – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Agent выводит в командную строку следующие данные о результатах выполнения задачи:

Данные, которые программа выводит в командную строку при обнаружении IOC

`Uuid`	Идентификатор IOC-файла из заголовка структуры IOC-файла (тег `<ioc id="">`)
`Name`	Описание IOC-файла из заголовка структуры IOC-файла (тег `<description></description>`)
`Matched Indicator Items`	Перечень идентификаторов всех сработавших индикаторов.
`Matched objects`	Данные о каждом документе IOC, в котором было найдено совпадение.
`Date`	Дата создания файла, в котором обнаружены маркеры компрометации.
`Created`	Только для FileItem. Время создания объекта, в котором обнаружены маркеры компрометации.
`Pid`	Идентификатор процесса, для которого обнаружены маркеры компрометации.
`Upid`	Уникальный идентификатор процесса, для которого обнаружены маркеры компрометации.
`ParentPid`	Идентификатор родительского объекта, содержащего процесс, для которого обнаружены маркеры компрометации.
`Username`	Имя пользователя, который вносил изменения в объект сканирования.
`StartTime`	Время запуска процесса, для которого обнаружены маркеры компрометации.

Управление сканированием файлов и процессов по YARA-правилам

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

Сканирование YARA представляет собой процессы, которые вы можете создавать и настраивать вручную через интерфейс командной строки. Для запуска сканирования используются YARA-файлы.

В задаче сканирования YARA можно указать только файл с YARA-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи сканирования YARA.

Чтобы запустить сканирование YARA через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.

2. С помощью команды cd перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду cd "`C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\`" и нажать на клавишу **Enter**.

3. Выполните следующую команду и нажмите на клавишу **Enter**:

   ```
   agent.exe --scan-yara [< путь к yara-файлу >] [--path=< путь к папке с yara-правилами >] [--fast-scan] [--tag-hint=< тег правила >] [--id-hint=< идентификатор правила >] [--max-rules=< максимальное количество правил сканирования >] [--timeout=< остановка сканирования по истечении указанного времени в секундах >] [--recursive] [--scan_folders [< список папок для сканирования >] [--scan-memory] [--scan-process < имя процесса >][--max-size=< размер файла в байтах >] [--excludes < список объектов для сканирования >] [--includes < список объектов для сканирования >]
   ```

Если команда `--scan-yara` передана только с обязательными параметрами, Kaspersky Endpoint Agent выполняет проверку с параметрами по умолчанию.

Описание параметров сканирования представлено в следующей таблице.

Параметры команд при запуске и настройке сканирования YARA

Параметры	Описание
`--scan-yara [< полный путь к yara-файлу >]`	Обязательный параметр. Запускает сканирование YARA на устройстве. Проверка выполняется по правилам из YARA-файлов с расширением yara или yar. Параметру может быть передано несколько значений через пробел. Хотя бы одно значение < `полный путь к yara-файлу` > должен быть указано, если не задан параметр --path. Если в дополнение к аргументам параметра --scan-yara также задан параметр --path, при сканировании используются как указанные в аргументах файлы с YARA-правилами, так и файлы из папки параметра --path.
`--path=< путь к папке с yara-файлами >`	Путь к папке с YARA-файлами, по которым требуется выполнять поиск. Обязательный параметр, если не задан параметр < `полный путь к yara-файлу` >.
`--fast-scan`	Необязательный параметр. Параметр запускает проверку в режиме быстрого сканирования. Для каждого объекта сканирования в журнале фиксируется одно вхождение обнаруженного маркера, при этом дубликаты обнаруженных маркеров не отображаются в журнале. Использование данного параметра позволяет сократить время проверки больших файлов. Если параметр не передан, выполняется стандартная проверка и дубликаты обнаруженных маркеров отображаются в журнале.
`--tag-hint=< тег правила >`	Необязательный параметр. Параметр позволяет учитывать при сканировании только правила с указанным тегом. Можно указать только одно значение параметра. Правила без тегов или с другими тегами, помимо указанных в параметре, игнорируются при сканировании. Если параметр не передан, при сканировании учитываются все правила.
`--id-hint=< идентификатор правила >`	Необязательный параметр. Параметр позволяет учитывать при сканировании только правила с указанным идентификатором. Можно указать только одно значение параметра. Правила без идентификаторов или с другими идентификаторами, помимо указанных в параметре, игнорируются при сканировании. Если параметр не передан, при сканировании учитываются все правила.
`--max-rules=< максимальное количество правил сканирования >`	Необязательный параметр. Параметр задаёт лимит уникальных сработавших правил обнаружения, при превышении которого проверка прекращается. Если значение параметра не задано или равно 0, проверка выполняется без ограничений.
`--timeout=< остановка сканирования по истечении указанного времени в секундах >`	Необязательный параметр. Параметр указывает продолжительность проверки в секундах. По истечении указанного времени проверка будет остановлена. Если значение параметра не задано или равно 0, проверка выполняется без ограничений.
`--recursive`	Необязательный параметр. Параметр запускает рекурсивную проверку вложенных папок в рамках значения [<список папок для сканирования>].

`--scan_folders [<список папок для сканирования>]`	Необязательный параметр. Параметр запускает сканирование файлов по указанному списку папок. Если значение параметра <`список папок для сканирования`> не задано, сканирование производится рекурсивно на всех локальных дисках, кроме сетевых, облачных и подключаемых.
`--scan-memory`	Необязательный параметр. Параметр запускает сканирование памяти всех запущенных процессов.
`--scan-process <имя процесса>`	Необязательный параметр. Параметр запускает сканирование памяти только для указанных процессов. Для значения <`имя процесса`> поддерживаются стандартные маски "`?`" и "`*`".
`--max-size=<размер файла в байтах>`	Необязательный параметр. Сканирование выполняется только для тех файлов, размер которых не превышает заданное значение. Файлы большего размера пропускаются при сканировании.
`--includes <список объектов для сканирования>`	Необязательный параметр. Параметр позволяет ограничить область сканирования. Можно задать несколько значений параметра через пробел. Доступные значения: • имя файла; • путь к файлу; • маска имени файла; • маска пути к файлу. Передается с параметром --scan-folders. Пример: --scan-folders c:*.* --recursive --includes *.exe c:\temp*.* *.dll – сканирование будет проведено для всех файлов с расширениями "exe" и "dll" на диске C:, а также будут просканированы рекурсивно все файлы в папке c:\temp
`--excludes <список объектов для сканирования>`	Необязательный параметр. Параметр исключает указанные файлы или папки из сканирования. Можно задать несколько значений параметра через пробел. Доступные значения: • имя файла; • путь к файлу; • маска имени файла; • маска пути к файлу. Передается с параметром --scan-folders. Пример: --scan-folders c:*.* --excludes readme.txt c:\trusted*.* *.xml – при сканировании будут пропущены файлы readme.txt, все файлы из папки c:\trusted, а также все файлы с расширением xml в корневой папке на диске C:.

Коды возврата команды `--scan-yara`:

- `-1` – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.
- `4` – синтаксическая ошибка.
- `5` – не найден один или несколько файлов с YARA-правилами из указанных в значении параметра.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Agent выводит в командную строку результаты сканирования. Описание результатов сканирования представлено в следующей таблице:

Данные, которые программа выводит в командную строку при обнаружении сигнатур YARA.

`Offset`	Смещение в объекте, для которого Kaspersky Endpoint Agent выполняет сканирование.
`Data`	Сигнатуры, которые Kaspersky Endpoint Agent ищет во время сканирования.
`Object Name`	Имя объекта сканирования.
`Rule Name`	Имя правила, которое используется во время сканирования.

Управление сканированием объектов точек автозапуска по YARA-правилам

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

Сканирование YARA для точек автозапуска представляет собой процессы, которые вы можете создавать и настраивать вручную через интерфейс командной строки. Для запуска сканирования используются YARA-файлы.

В задаче сканирования YARA для объектов точек автозапуска можно указать только файл с YARA-правилами. Файлы с другими типами правил не поддерживаются в рамках задачи сканирования YARA.

По умолчанию сканирование объектов по правилам YARA осуществляется для следующих типов точек автозапуска:

- Logon
- Run
- Explorer
- Shell
- Office
- Internet Explorer
- Tasks
- Services
- Drivers
- Telephony
- Cryptography
- Debuggers
- COM

- Session Manager
- Network
- LSA
- Applications
- Codecs
- Shellex
- Unspecified

Чтобы запустить сканирование YARA для точек автозапуска через интерфейс командной строки:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, вы можете ввести команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажать на клавишу **Enter**.
3. Выполните следующую команду и нажмите на клавишу **Enter**:

   `agent.exe --scan-yara [<путь к yara-файлу>] [--path=<путь к папке с yara-правилами>] --scan-autoruns=yes [--fast-scan] [--tag-hint=<тег правила>] [--id-hint=<идентификатор правила>] [--max-rules=<максимальное количество правил сканирования>] [--timeout=<остановка сканирования по истечении указанного времени в секундах>] [--max-size=<размер файла в байтах>] [--exclude-autoruns=COM]`

   Если команда `--scan-yara --scan-autoruns` передана только с обязательными параметрами, Kaspersky Endpoint Agent выполняет проверку с параметрами по умолчанию.

Описание параметров сканирования представлено в следующей таблице.

Параметры команд при запуске и настройке сканирования YARA

Параметры	Описание
`--scan-yara [<полный путь к yara-файлу>]`	Обязательный параметр. Запускает сканирование YARA для файлов точек автозапуска на устройстве. Проверка выполняется по правилам из YARA-файлов с расширением yara или yar. Параметру может быть передано несколько значений через пробел. Хотя бы одно значение <`полный путь к yara-файлу`> должно быть указано, если не задан параметр --path. Если в дополнение к аргументам параметра `--scan-yara --scan-autoruns` также задан параметр `--path`, при сканировании используются как указанные в аргументах файлы с YARA-правилами, так и файлы из папки параметра `--path`.
`--path=<путь к папке с yara-файлами>`	Путь к папке с YARA-файлами, по которым требуется выполнять поиск файлов точек автозапуска. Обязательный параметр, если не задан параметр `<полный путь к yara-файлу>`.
`--scan-autoruns=yes`	Обязательный параметр. Параметр обращается к точкам автозапуска и сканирует объекты для всех типов точек автозапуска по указанным YARA-правилам. Для запуска сканирования необходимо передать значение `yes`. Если значение параметра не указано, параметр будет проигнорирован.

`--fast-scan`	Необязательный параметр. Параметр запускает проверку в режиме быстрого сканирования. Для каждого объекта сканирования в журнале фиксируется одно вхождение обнаруженного маркера, при этом дубликаты обнаруженных маркеров не отображаются в журнале. Использование этого параметра позволяет сократить время проверки больших файлов. Если параметр не передан, выполняется стандартная проверка и дубликаты обнаруженных маркеров отображаются в журнале.
`--tag-hint=< тег правила >`	Необязательный параметр. Параметр позволяет учитывать при сканировании только правила с указанным тегом. Можно указать только одно значение параметра. Правила без тегов или с другими тегами, помимо указанных в параметре, игнорируются при сканировании. Если параметр не передан, при сканировании учитываются все правила.
`--id-hint=< идентификатор правила >`	Необязательный параметр. Параметр позволяет учитывать при сканировании только правила с указанным идентификатором. Можно указать только одно значение параметра. Правила без идентификаторов или с другими идентификаторами, помимо указанных в параметре, игнорируются при сканировании. Если параметр не передан, при сканировании учитываются все правила.
`--max-rules=< максимальное количество правил сканирования >`	Необязательный параметр. Параметр задает лимит уникальных сработавших правил обнаружения, при превышении которого проверка прекращается. Если значение параметра не задано или равно 0, проверка выполняется без ограничений.
`--timeout=< остановка сканирования по истечении указанного времени в секундах >`	Необязательный параметр. Параметр указывает продолжительность проверки каждого объекта в секундах. По истечении указанного времени проверка будет остановлена. Если значение параметра не задано или равно 0, проверка выполняется без ограничений.
`--max-size=< размер файла в байтах >`	Необязательный параметр. Сканирование выполняется только для тех файлов, размер которых не превышает заданное значение. Файлы большего размера пропускаются при сканировании.
`--exclude-autoruns=< список объектов для сканирования >`	Необязательный параметр. Параметр исключает из сканирования файлы в указанной точке автозапуска. Можно задать несколько значений параметра через пробел. Доступное значение: COM (в настоящее время поддерживается исключение только этого типа точек автозапуска). Пример: `--exclude-autoruns=COM` При сканировании будут пропущены файлы из области точки автозапуска COM. **Ограничения** В полученных списках точек автозапуска для COM-объектов могут отсутствовать сборки компонентов, написанные на .NET ввиду особенностей их регистрации в системе.

Коды возврата команды `--scan-yara`:

- `-1` – команда не поддерживается версией Kaspersky Endpoint Agent, которая установлена на устройстве.
- `0` – команда выполнена успешно.
- `1` – команде не передан обязательный аргумент.
- `2` – общая ошибка.

- `4` – синтаксическая ошибка.
- `5` – не найден один или несколько файлов с YARA-правилами из указанных в значении параметра.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Endpoint Agent выводит в командную строку результаты сканирования. Описание результатов сканирования представлено в следующей таблице:

Данные, которые программа выводит в командную строку при обнаружении сигнатур YARA.

`Offset`	Смещение в объекте, для которого Kaspersky Endpoint Agent выполняет сканирование.
`Data`	Сигнатуры, которые Kaspersky Endpoint Agent ищет во время сканирования.
`Object Name`	Имя объекта сканирования.
`Rule Name`	Имя правила, которое используется во время сканирования.

Создание дампа памяти

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете создать дамп памяти компьютера, на котором установлена программа Kaspersky Endpoint Agent.

Перед созданием дампа памяти рекомендуем завершить процессы критически важных программ. После создания дампа памяти рекомендуем перезагрузить компьютер, для которого создан дамп памяти.

Чтобы создать дамп памяти через интерфейс командной строки Kaspersky Endpoint Agent:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.
3. Введите команду:

   `agent.exe --memory-dump --path=<путь к локальной или сетевой папке, в которой вы хотите сохранить дамп памяти> [--user=<имя пользователя> --pwd=<пароль>]`.

   Имя пользователя и пароль необходимы, если доступ к папке для сохранения дампа памяти защищен паролем.

   Убедитесь, что папка для сохранения дампа памяти, доступна для записи. Иначе файл дампа не будет создан.
4. Нажмите на клавишу **ENTER**.

   В указанной папке Kaspersky Endpoint Agent создаст файл дампа памяти с названием MemoryDump_<имя хоста>_<дата и время старта записи файла>.dmp.

Параметры команды для создания дампа памяти

Параметр	Описание
`--path`	Обязательный параметр. Параметр передает полный путь к локальной или сетевой папке, в которую программа сохраняет дамп памяти. Имя сетевой папки должно быть указано в UNC-формате.
`--user`	Параметр передает логин для доступа к папке, указанной с помощью параметра `--path`. Если параметр не задан, для создания дампа памяти необходим доступ к папке для учетной записи SYSTEM.
`--pwd`	Параметр передает пароль для доступа к папке, указанной с помощью параметра `--path`. Если параметр не задан, для создания дампа памяти необходим доступ к папке для учетной записи SYSTEM.

Коды возврата команды `--memory-dump`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Kaspersky Endpoint Agent не выполняет шифрование и сжатие файла дампа памяти. Если необходимо, вы можете настроить шифрование и сжатие папки для сохранения дампа памяти с помощью сторонних инструментов.

Чтобы Kaspersky Endpoint Agent мог сохранять файл дампа памяти в сетевую папку в зашифрованном виде, требуется настроить использование SMB-протокола версии 3 или выше.

Создание дампа диска

В разделе приведена инструкция для Kaspersky Endpoint Agent для Windows. Эта инструкция может быть частично или полностью неприменима к Kaspersky Endpoint Agent для Linux. Актуальную инструкцию для Kaspersky Endpoint Agent для Linux смотрите в справке решения, в составе которого вы используете программу: Kaspersky Anti Targeted Attack Platform или Kaspersky Managed Detection and Response.

Вы можете создать дамп физического или логического диска компьютера, на котором установлена программа Kaspersky Endpoint Agent.

Чтобы создать дамп диска через интерфейс командной строки Kaspersky Endpoint Agent:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt cmd.exe) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл agent.exe.

   Например, введите команду `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` и нажмите на клавишу **ENTER**.

Введите команду:

`agent.exe --disk-image --volume=<имя диска> [--format=<формат файла, RAW или EWF>] [--max-size=<размер в байтах>] [--segment-size=<размер в байтах>] --path=<путь к локальной или сетевой папке, в которой вы хотите сохранить дамп диска> [--user=<имя пользователя> --pwd=<пароль>]`

Имя пользователя и пароль необходимы, если доступ к папке для сохранения дампа диска защищен паролем.

Убедитесь, что папка для сохранения дампа диска, доступна для записи. Иначе файл дампа не будет создан.

3. Нажмите на клавишу **ENTER**.

В указанной папке Kaspersky Endpoint Agent создаст файл дампа диска с названием в формате <имя диска>_<дата и время старта записи файла>.<расширение>.

Расширение файла дампа диска может быть следующим:

- Если в команде для создания дампа диска указан формат RAW (`--format=RAW`):
  - если дамп диска не разделен (не задан параметр `--segment-size`), то файл дампа диска имеет расширение raw;
  - если дамп диска разделен (задан параметр `--segment-size`), то части дампа имеют расширение 001, 002, 003 и далее по порядку до 999.
- Если в команде для создания дампа диска указан формат EWF (`--format=EWF`):
  - если дамп диска не разделен (не задан параметр `--segment-size`), то файл дампа диска имеет расширение E01;
  - если дамп диска разделен (задан параметр `--segment-size`), то части дампа имеют расширение E01, E02, ..., E99; EAA, EAB, ..., EAZ; FAA, FAB, ..., FZZ, <...>; ZAA, ZAB, ..., ZZZ.

Параметры команды для создания дампа диска

Параметр	Описание
`--volume`	Обязательный параметр. Параметр передает номер физического диска или имя логического диска, для которого будет создан дамп. Формат номера физического диска: \??\PHYSICALDRIVEN или PHYSICALDRIVEN, где N – порядковый номер диска. Например: \??\PHYSICALDRIVE0, PHYSICALDRIVE1. Формат имени логического диска: N:, где N – буквенное обозначение логического диска. Например, C:. Если вы создаете дамп для логического диска, с которого осуществляется загрузка операционной системы, в качестве имени диска используйте переменную %SystemDrive%.
`--format`	Параметр передает формат файла с дампом диска. Возможные значения: RAW или EWF. Если параметр не задан, программа создает дамп диска в формате RAW.
`--max-size`	Параметр передает максимальное допустимое значение размера дампа диска в байтах. Если параметр не задан, программа создает дамп диска с максимальным размером 1 099 511 627 776 байт.
`--segment-size`	Параметр передает максимальное значение размера частей дампа диска в байтах. При этом минимальный размер частей дампа должен быть больше 33 554 432 байт. Если параметр задан, программа разбивает дамп диска на части указанного размера и архивирует их. Размер архивированных частей дампа меньше указаного с помощью параметра значения. Если параметр не задан, программа не производит разбиение дампа диска на части.
`--path`	Обязательный параметр. Параметр передает полный путь к локальной или сетевой папке, в которую программа сохраняет дамп диска. Имя сетевой папки должно быть указано в UNC-формате.

Параметр	Описание
`--user`	Параметр передает логин для доступа к папке, указанной с помощью параметра `--path`. Если параметр не задан, для создания дампа диска необходим доступ к папке для учетной записи SYSTEM.
`--pwd`	Параметр передает пароль для доступа к папке, указанной с помощью параметра `--path`. Если параметр не задан, для создания дампа диска необходим доступ к папке для учетной записи SYSTEM.

Коды возврата команды `--memory-dump`:

- -1 – команда не поддерживается.
- 0 – команда выполнена успешно.
- 1 – команде не передан обязательный аргумент.
- 2 – общая ошибка.
- 4 – синтаксическая ошибка.

Kaspersky Endpoint Agent не выполняет шифрование и сжатие файла дампа памяти. Если необходимо, вы можете настроить шифрование и сжатие папки для сохранения дампа памяти с помощью сторонних инструментов.

Чтобы Kaspersky Endpoint Agent мог сохранять файл дампа памяти в сетевую папку в зашифрованном виде, требуется настроить использование SMB-протокола версии 3 или выше.

Управление программой Kaspersky Endpoint Agent для Linux

В этом разделе приведена информация для Kaspersky Endpoint Agent для Linux. Информацию для Kaspersky Endpoint Agent для Windows см. в отдельном разделе.

Kaspersky Endpoint Agent для Linux устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации и работающие под управлением одной из операционных систем Linux. Программа осуществляет постоянное наблюдение за процессами, запущенными на этих устройствах, открытыми сетевыми соединениями и изменяемыми файлами.

Kaspersky Endpoint Agent для Linux обеспечивает взаимодействие защищаемого устройства с другими решениями "Лаборатории Касперского" для обнаружения комплексных угроз (таких как таргетированные атаки).

Взаимодействие программы с Kaspersky Anti Targeted Attack Platform выполняется с помощью компонента KATA Central Node. При настроенной интеграции Kaspersky Endpoint Agent с KATA Central Node, программа выполняет задачи и применяет настройки, поступающие от компонента KATA Central Node, а также отправляет на сервер с компонентом KATA Central Node данные телеметрии с защищаемого устройства.

Вы можете управлять программой Kaspersky Endpoint Agent для Linux удаленно в веб-консоли Kaspersky Security Center, с помощью Консоли администрирования Kaspersky Security Center и с помощью командной строки.

Установка и удаление Kaspersky Endpoint Agent для Linux

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Agent для Linux на устройство, как обновить предыдущую версию программы, как восстановить и удалить программу с устройства.

Подготовка к установке Kaspersky Endpoint Agent для Linux

Перед установкой Kaspersky Endpoint Agent для Linux на устройство или обновлением предыдущей версии программы требуется проверить, выполняются ли аппаратные и программные требования.

Установка Kaspersky Endpoint Agent для Linux с помощью Консоли администрирования Kaspersky Security Center

В данном разделе содержится информация об удаленной установке Kaspersky Endpoint Agent на локальное устройство с помощью Консоли администрирования Kaspersky Security Center.

Установка плагина управления Kaspersky Endpoint Agent для Linux

Управление Kaspersky Endpoint Agent посредством Консоли администрирования Kaspersky Security Center выполняется с помощью плагина управления. Поэтому для получения доступа к управлению программой требуется установить плагин управления на рабочее место администратора.

Чтобы установить плагин управления Kaspersky Endpoint Agent,

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

Запустится мастер установки программы.

Добавление устройств для установки Kaspersky Endpoint Agent для Linux

Для удаленной установки программы с помощью Kaspersky Security Center требуется добавить устройства, на которые будет произведена установка, в группу управляемых устройств.

Чтобы добавить устройства для установки программы, выполните следующие действия:

1. Установите на устройство Агент администрирования Kaspersky Security Center.

   Описание подготовки устройства с операционной системой Linux к удаленной установке Агента администрирования см. в *справке Kaspersky Security Center*.

2. В командной строке выполните команду `/opt/kaspersky/klnagent/bin/klmover --address <адрес IP сервера Kaspersky Security Center>`.

   Устройство станет доступно для управления с помощью Kaspersky Security Center.

   > Если Агент администрирования был установлен на устройстве ранее, первые два пункта этой инструкции выполнять не требуется.

3. Откройте Консоль администрирования Kaspersky Security Center.

4. В дереве консоли выберите папку **Управляемые устройства**.

   > Если на устройстве установлена программа Kaspersky Endpoint Security for Linux, устройство будет находиться в группе, в которой действует политика Kaspersky Endpoint Security for Linux. При этом перемещать устройство не требуется.

5. В рабочей области папки выберите закладку **Устройства**.

6. Нажмите на кнопку **Переместить устройства в группу**.

   Откроется окно мастера перемещения устройств.

7. Нажмите на кнопку **Выбрать устройства, обнаруженные в сети Сервером администрирования**.

8. В следующем окне мастера в списке устройств установите флажок напротив устройства, на которое требуется установить программу.

9. Нажмите на кнопку **Далее**.

   Устройство будет перемещено в группу управляемых устройств.

10. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Устройство станет доступно для удаленной установки программы.

Создание инсталляционного пакета Kaspersky Endpoint Agent для Linux

Для удаленной установки программы с помощью Kaspersky Security Center требуется создать инсталляционный пакет Kaspersky Endpoint Agent из репозитория программ "Лаборатории Касперского" или из файла.

Перед тем как приступить к созданию инсталляционного пакета Kaspersky Endpoint Agent, убедитесь, что плагин управления установлен на рабочее место администратора.

Чтобы создать инсталляционный пакет для программы из репозитория программ "Лаборатории Касперского", выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли в папке **Сервер администрирования → Дополнительно → Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

3. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.

4. В окне мастера **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.

   В процессе создания инсталляционного пакета для программы вам может быть предложено ознакомиться с Лицензионным соглашением на эту программу и Политикой конфиденциальности программы. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **Положения и условия настоящего Лицензионного соглашения**;
   - **Политику конфиденциальности, которая описывает обработку данных**.

5. В следующем окне мастера введите имя для нового инсталляционного пакета.

6. В следующем окне мастера выберите инсталляционный файл Kaspersky Endpoint Agent с расширением kud.

7. В следующем окне мастера выберите компоненты Kaspersky Endpoint Agent, которые необходимо установить, директорию и режим установки программы.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты** в дереве консоли.

Чтобы создать инсталляционный пакет для программы из файла, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли в папке **Сервер администрирования → Дополнительно → Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
4. В окне мастера **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы, указанной пользователем**.

   В процессе создания инсталляционного пакета для программы вам может быть предложено ознакомиться с Лицензионным соглашением на эту программу и Политикой конфиденциальности программы. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **Положения и условия настоящего Лицензионного соглашения**;
   - **Политику конфиденциальности, которая описывает обработку данных**.
5. В следующем окне мастера введите название инсталляционного пакета.
6. В следующем окне мастера выберите установочный файл программы и завершите создание инсталляционного пакета, следуя указаниям мастера.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты** в дереве консоли.

Удаленная установка Kaspersky Endpoint Agent для Linux на выбранные устройства

Kaspersky Security Center позволяет удаленно устанавливать программы на устройства с помощью задач удаленной установки.

Чтобы создать и запустить задачу удаленной установки Kaspersky Endpoint Agent на выбранные устройства, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В рабочей области папки выберите инсталляционный пакет программы Kaspersky Endpoint Agent.
4. В контекстном меню инсталляционного пакета выберите пункт **Установить программу**.
5. Запустится мастер удаленной установки.
6. В окне **Выбор устройств для установки** можно сформировать список устройств, на которые будет установлена программа.
7. В окне **Определение параметров задачи удаленной установки** настройте параметры удаленной установки программы.

8. В окне **Выбор параметра перезагрузки операционной системы** определите, перезагружать ли устройства, если в ходе установки программ на них потребуется перезагрузка операционной системы.

9. В окне **Выбор учетных записей для доступа к устройствам** можно добавить учетные записи, которые будут использоваться для запуска задачи удаленной установки.

10. В окне **Запуск установки** нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

    Если в окне **Запуск установки** установлен флажок **Не запускать задачу после завершения работы мастера удаленной установки**, задача удаленной установки не будет запущена. Вы можете запустить эту задачу позже вручную. Имя задачи соответствует имени инсталляционного пакета для установки программы: **Установка <Имя инсталляционного пакета>**.

Установка Kaspersky Endpoint Agent для Linux с помощью Kaspersky Security Center Web Console

В данном разделе содержится информация об удаленной установке Kaspersky Endpoint Agent для Linux на локальное устройство с помощью Kaspersky Security Center Web Console.

Установка веб-плагина управления Kaspersky Endpoint Agent

Управление Kaspersky Endpoint Agent для Linux посредством Kaspersky Security Center Web Console выполняется с помощью веб-плагина управления. Поэтому для получения доступа к управлению программой требуется установить веб-плагин управления на рабочее место администратора (см. информацию об установке и обновлении веб-плагина управления в разделе справки, описывающем управление программой Kaspersky Endpoint Agent для Windows).

Перед установкой следует ознакомиться с информацией о совместимых версиях веб-плагина управления.

Добавление устройств для установки Kaspersky Endpoint Agent для Linux

Для удаленной установки программы с помощью Kaspersky Security Center требуется добавить устройства, на которые будет произведена установка, в группу управляемых устройств.

Чтобы добавить устройства для установки программы, выполните следующие действия:

1. Установите на устройство Агент администрирования Kaspersky Security Center.

   Описание подготовки устройства с операционной системой Linux к удаленной установке Агента администрирования см. в *справке Kaspersky Security Center*.

2. В командной строке выполните команду `/opt/kaspersky/klnagent/bin/klmover --address <адрес IP сервера Kaspersky Security Center>`.

   Устройство станет доступно для управления с помощью Kaspersky Security Center.

   > Если Агент администрирования был установлен на устройстве ранее, первые два пункта этой инструкции выполнять не требуется.

3. Войдите в программу Kaspersky Security Center Web Console.
4. В главном окне веб-консоли выберите **Обнаружение устройств** -> **Нераспределенные устройства**.

   Если на устройстве установлена программа Kaspersky Endpoint Security for Linux, устройство будет находиться в группе, в которой действует политика Kaspersky Endpoint Security for Linux. При этом перемещать устройство не требуется.

5. В списке устройств установите флажок напротив устройства, на которое требуется установить программу.
6. Нажмите на кнопку **Переместить в группу**.
7. В открывшемся меню справа установите флажок напротив группы **Управляемые устройства**.
8. Нажмите на кнопку **Переместить**.

Устройство станет доступно для удаленной установки программы.

Создание инсталляционного пакета Kaspersky Endpoint Agent для Linux

Для удаленной установки программы с помощью Kaspersky Security Center Web Console требуется создать инсталляционный пакет Kaspersky Endpoint Agent для Linux из репозитория программ "Лаборатории Касперского" или из файла.

Чтобы создать инсталляционный пакет для программы, выполните следующие действия:

1. Войдите в программу Kaspersky Security Center Web Console.
2. На закладке **Обнаружение устройств и развертывание** выберите **Развертывание и назначение** → **Инсталляционные пакеты**.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На первом шаге мастера вы можете выбрать вариант создания инсталляционного пакета: из репозитория программ "Лаборатории Касперского" или из файла.

   - Если вы выбрали параметр **Создать инсталляционный пакет для программы "Лаборатории Касперского"**, отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Для упрощения поиска необходимого инсталляционного пакета нажмите на кнопку **Фильтр**, в появившемся меню в окне **Свойство** выберите значение **Операционная система** и вариант **Linux**.

   - Если вы выбрали параметр **Создать инсталляционный пакет из файла**, вам будет предложено указать путь к локальной папке, содержащей архив с инсталляционным пакетом программы.

5. Выберите требуемый инсталляционный пакет Kaspersky Endpoint Agent для Linux.

   Откроется окно с информацией об инсталляционном пакете.

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

   Начинается загрузка инсталляционного пакета на Сервер администрирования.

7. Во время процесса загрузки программы отобразится кнопка **Принять**. Выполните следующие действия:

   a. Нажмите на кнопку **Принять**, чтобы прочитать текст Лицензионного соглашения и Политики конфиденциальности.

   b. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

      - **положения и условия настоящего Лицензионного соглашения**;
      - **Политику конфиденциальности, которая описывает обработку данных**.

   c. Нажмите на кнопку **Принять**.

      Загрузка инсталляционного пакета будет продолжена после установки обоих флажков. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.

8. После завершения загрузки нажмите на кнопку **Закрыть**, чтобы закрыть информационное окно инсталляционного пакета.

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

Удаленная установка Kaspersky Endpoint Agent для Linux на выбранные устройства

Kaspersky Security Center Web Console позволяет удаленно устанавливать программы на устройства с помощью задач удаленной установки.

Чтобы создать и запустить задачу удаленной установки Kaspersky Endpoint Agent для Linux на выбранные устройства, выполните следующие действия:

1. Войдите в программу Kaspersky Security Center Web Console.

2. На закладке **Устройства** выберите **Задачи**.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

4. На первом шаге мастера выполните следующие действия:

   a. В окне **Программа** выберите программу **Kaspersky Security Center 12**.

   b. В окне **Тип задачи** выберите тип **Удаленная установка программы**.

   c. При необходимости в окне **Название задачи** введите название для задачи.

   d. В разделе **Выбор устройств, которым будет назначена задача** выберите параметр **Группа устройств**.

5. Нажмите на кнопку **Далее**.

   Откроется следующий шаг мастера создания задачи.

6. Установите флажок напротив группы **Управляемые устройства** или напротив отдельных устройств в этой группе.

7. Нажмите на кнопку **Далее**.

   Откроется следующий шаг мастера создания задачи.

8. В окне **Выбор инсталляционного пакета** выберите ранее созданный пакет Kaspersky Endpoint Agent для Linux.

   Остальные параметры на этом и следующих шагах менять не следует.

9. Нажмите на кнопку **Далее**.

   Откроется завершающий шаг мастера создания задачи.

10. На завершающем шаге мастера установки нажмите на кнопку **Готово**.

11. Установите флажок напротив созданной задачи в списке задач.

12. Нажмите на кнопку **Запустить**.

13. Дождитесь завершения установки Kaspersky Endpoint Agent для Linux на выбранные устройства.

    Статус задачи изменится на **Завершена**.

Локальная установка Kaspersky Endpoint Agent для Linux

В данном разделе содержится информация об установке Kaspersky Endpoint Agent на локальное устройство из инсталляционных пакетов формата DEB или RPM.

Чтобы установить программу или обновить предыдущую версию программы:

1. Скопируйте инсталляционный пакет программы формата DEB или RPM, входящий в комплект поставки, на устройство пользователя.

2. Откройте консоль и выполните команду установки программы из соответствующего пакета:

   - Для установки программы из инсталляционного пакета deb: `sudo apt install имя_пакета.deb`
   - Для установки программы из инсталляционного пакета rpm: `sudo rpm -i имя_пакета.rpm`

   Программа будет установлена на локальное устройство.

Использование программы возможно только после принятия вами условий Лицензионного соглашения и Политики конфиденциальности.

Чтобы ознакомиться с Лицензионным соглашением и Политикой конфиденциальности программы и принять их условия:

1. Откройте консоль и выполните команду `/opt/kaspersky/epagent/sbin/lenactl --eula-pp accept`.
2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского".
3. Нажмите на кнопку **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.
4. Внимательно прочитайте условия Политики конфиденциальности.
5. Нажмите на кнопку **Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности»**.

Программа будет готова к использованию.

Обновление и восстановление Kaspersky Endpoint Agent для Linux

Обновление и восстановление программы выполняется с помощью Kaspersky Security Center или локально.

Для обновления Kaspersky Endpoint Agent для Linux с помощью Kaspersky Security Center требуется создать инсталляционный пакет для новой версии программы и выполнить процедуру установки. Для восстановления программы можно использовать инсталляционный пакет, созданный для текущей версии программы.

Удаление Kaspersky Endpoint Agent для Linux

Удаление программы выполняется с помощью Kaspersky Security Center или локально.

Чтобы удаленно деинсталлировать программу с выбранных устройств с помощью Kaspersky Security Center, выполните следующие действия:

1. Войдите в программу Kaspersky Security Center Web Console.
2. На закладке **Устройства** выберите **Задачи**.
3. Нажмите на кнопку **Добавить**.

   Следуйте далее указаниям мастера создания задачи.
4. На первом шаге мастера выполните следующие действия:
   a. В окне **Программа** выберите программу **Kaspersky Security Center 12**.
   b. В окне **Тип задачи** выберите тип **Удаленная деинсталляция программы**.

c. При необходимости в окне **Название задачи** введите название для задачи.

d. В разделе **Выбор устройств, которым будет назначена задача** выберите параметр **Группа устройств**.

5. Нажмите на кнопку **Далее**.

   Откроется следующий шаг мастера создания задачи.

6. Установите флажок напротив группы **Управляемые устройства** или напротив отдельных устройств в этой группе.

7. Нажмите на кнопку **Далее**.

   Откроется следующий шаг мастера создания задачи.

8. В окне **Программа для деинсталляции** выберите установленную версию Kaspersky Endpoint Agent для Linux.

   Остальные параметры на этом и следующих шагах менять не следует.

9. На последнем шаге мастера нажмите на кнопку **Готово**.

10. Установите флажок напротив созданной задачи в списке задач и нажмите на кнопку **Запустить**.

11. Дождитесь завершения удаления Kaspersky Endpoint Agent для Linux на выбранных устройствах.

    При этом статус задачи изменится на **Завершена**.

В результате выполнения задачи выбранная программа будет удалена с выбранных устройств.

Управление Kaspersky Endpoint Agent для Linux с помощью Консоли администрирования Kaspersky Security Center

Программа Kaspersky Security Center предназначена для централизованного решения основных задач управления и обслуживания системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Kaspersky Security Center позволяет удаленно устанавливать и удалять Kaspersky Endpoint Agent, настраивать параметры работы программы.

Подробную информацию о Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Пользовательский интерфейс для работы с Kaspersky Security Center предоставляется с помощью компонента Консоль администрирования Kaspersky Security Center.

Управление Kaspersky Endpoint Agent в Kaspersky Security Center Web Console осуществляется с помощью *плагина управления Kaspersky Endpoint Agent*.

Далее в разделе приведена основная информация об управлении Kaspersky Endpoint Agent с помощью Консоли администрирования Kaspersky Security Center.

Управление политиками Kaspersky Endpoint Agent для Linux

В этом разделе приведены инструкции по созданию политики Kaspersky Endpoint Agent для Linux и включению параметров политики в Консоли администрирования Kaspersky Security Center.

Инструкции, приведенные в этом разделе, применимы только для Kaspersky Endpoint Agent для Linux. Информацию для Kaspersky Endpoint Agent для Windows см. в отдельном разделе.

Создание политики Kaspersky Endpoint Agent для Linux

Чтобы создать политику Kaspersky Endpoint Agent в Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Нажмите на кнопку **Создать политику**.

   Запустится мастер создания политики.
4. В окне **Ввод названия групповой политики** введите имя, под которым создаваемая политика будет отображаться в списке политик.
5. В окне **Выбрать тип политики** выберите необходимый способ развертывания Kaspersky Endpoint Agent, установив флажок **Endpoint Detection and Response Expert (KATA EDR)**.
6. Нажмите на кнопку **Далее**.
7. Выполните одно из следующих действий во всех последовательно отображающихся окнах с параметрами:

   - Чтобы настроить параметры программы из отображаемых разделов во время создания политики:

     a. Нажмите на кнопку **Настроить** рядом с названием необходимого раздела.

     b. В открывшемся окне настройте необходимые параметры и нажмите на кнопку **OK.**

     c. Нажмите на кнопку **Далее**.

   - Чтобы настроить параметры программы из отображаемых разделов позднее, нажмите на кнопку **Далее**.

   Настройка параметров программы состоит из следующих этапов:

   - Настройка общих параметров прокси-сервера.
   - Настройка интеграции Kaspersky Endpoint Agent с компонентом KATA Central Node.

8. В окне **Целевая группа** выберите группу администрирования Kaspersky Security Center, на которую должна распространяться создаваемая политика, выполнив следующие действия:

   a. Нажмите на кнопку **Обзор**.

      Откроется окно выбора группы администрирования.

   b. Выберите группу администрирования в списке.

      Например, вы можете выбрать группу **Управляемые устройства**.

   c. Если вы хотите создать подгруппу устройств в группе **Управляемые устройства**, выполните следующие действия:

      1. Нажмите на кнопку **Новая группа**.

      2. В открывшемся окне введите имя подгруппы устройств.

      3. Нажмите на кнопку **ОК**.

   d. Нажмите на кнопку **Далее**.

9. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:

   - **Активная политика**, чтобы политика начала действовать сразу после создания.

   - **Неактивная политика**, чтобы активировать политику позже.

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

11. Нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик.

Включение параметров в политике Kaspersky Endpoint Agent для Linux

При настройке параметров политики Kaspersky Endpoint Agent по умолчанию значения параметров сохраняются, но не применяются до тех пор, пока вы их не включите.

Включение параметров доступно для блоков, в которых находятся эти параметры. В рамках одной политики вы можете включить как часть блоков параметров, так и все блоки параметров.

Чтобы включить блок параметров в политике Kaspersky Endpoint Agent, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли откройте папку **Политики**.

3. Выберите политику для программы Kaspersky Endpoint Agent и откройте окно ее параметров одним из следующих способов:

   - Двойным щелчком мыши по названию политики.

   - В контекстном меню политики выберите пункт **Свойства**.

4. В открывшемся окне выберите раздел **Параметры программы**.

   a. Выберите подраздел **Другие параметры**.

   b. Выберите один из следующих вариантов использования прокси-сервера:

   - **Не использовать прокси-сервер**.
   - **Использовать прокси-сервер с указанными параметрами**.

   Если вы выбрали вариант **Использовать прокси-сервер с указанными параметрами**, в полях **Имя или IP-адрес сервера** и **Порт** введите адрес и порт прокси-сервера, соединение с которым вы хотите установить. По умолчанию используется порт 8080.

   > Kaspersky Endpoint Agent не обеспечивает шифрование соединения с прокси-сервером. Необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Endpoint Agent.

   Если вы хотите использовать NTLM-аутентификацию при подключении к прокси-серверу, выполните следующие действия:

   1. Установите флажок **Использовать NTLM-аутентификацию по имени пользователя и паролю**.
   2. В поле **Имя пользователя** введите имя пользователя, учетная запись которого будет использоваться для авторизации на прокси-сервере.
   3. В поле **Пароль** введите пароль подключения к прокси-серверу.

   Вы можете включить отображение символов пароля, нажав на кнопку **Показать** справа от поля **Пароль**.

   Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.

   c. Нажмите на кнопку **Применить**.

5. Выберите раздел **Интеграция с KATA**.

   a. Перейдите в подраздел **Общие параметры**.

   b. В блоке **Параметры передачи данных** переведите переключатель **Политика применяется** в активное состояние.

   c. В поле **Максимальное время передачи события (сек.)** введите значение 30.

   d. В поле **Максимальное количество событий в одном пакете** введите значение 1024.

   e. В блоке **Регулирование количества запросов** переведите переключатель **Политика применяется** в активное состояние.

   f. Установите флажок **Включить регулирование количества запросов**.

   g. Введите значение для максимального количества событий в час и значение процента превышения лимита событий.

   h. Перейдите в подраздел **Параметры интеграции с KATA**.

i. В блоке **Параметры подключения** переведите переключатель **Принудительно** в активное состояние.

j. Установите флажок **Включить интеграцию с KATA**.

k. Введите адрес и порт сервера KATA в поля **Адрес** и **Порт**.

l. Установите флажок **Использовать закрепленный сертификат для защиты соединения**.

m. Нажмите на кнопку **Добавить новый TLS-сертификат**.

n. В открывшемся окне нажмите на кнопку **Загрузить** и выберите файл сертификата сервера для организации безопасного соединения или введите данные сертификата в поле.

o. Нажмите на кнопку **Добавить**.

p. Нажмите на кнопку **Добавить клиентский сертификат**.

q. В открывшемся окне установите флажок **Защитить соединение при помощи клиентского сертификата**.

r. нажмите на кнопку **Загрузить** и выберите файл клиентского сертификата для организации безопасного соединения.

s. В поле **Пароль криптоконтейнера** введите пароль клиентского сертификата для организации безопасного соединения.

t. Установите флажок **Учитывать период TTL при отправке событий**.

u. В поле **Период TTL (мин.)** введите значение интервала отправления запроса на синхронизацию.

v. Нажмите на кнопку **Применить**.

6. Нажмите на кнопку **OK**.

Необходимые параметры политики для работы Kaspersky Endpoint Agent будут включены.

Управление задачами обновления баз и модулей Kaspersky Endpoint Agent

Вы можете создавать и настраивать параметры задач обновления баз и модулей программы с помощью Консоли администрирования Kaspersky Security Center (см. информацию в разделе справки, описывающем создание и настройку параметров задачи обновления баз и модулей программы в программе Kaspersky Endpoint Agent для Windows).

Вы так же можете настроить обновление баз и модулей программы с помощью командной строки.

Управление Kaspersky Endpoint Agent для Linux с помощью Kaspersky Security Center Web Console

Программа Kaspersky Security Center предназначена для централизованного решения основных задач управления и обслуживания системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Kaspersky Security Center позволяет удаленно устанавливать и удалять Kaspersky Endpoint Agent для Linux, настраивать параметры работы программы.

Подробную информацию о Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Пользовательский интерфейс для работы с Kaspersky Security Center предоставляется с помощью компонента Kaspersky Security Center Web Console.

Управление Kaspersky Endpoint Agent для Linux в Kaspersky Security Center Web Console осуществляется с помощью *веб-плагина управления Kaspersky Endpoint Agent.*

Далее в разделе приведена основная информация об управлении Kaspersky Endpoint Agent для Linux с помощью Kaspersky Security Center Web Console

Управление политиками Kaspersky Endpoint Agent для Linux

В этом разделе приведены инструкции по созданию политики Kaspersky Endpoint Agent для Linux и включению параметров в политике с помощью Kaspersky Security Center Web Console.

Инструкции, приведенные в этом разделе, применимы только для Kaspersky Endpoint Agent для Linux. Информацию для Kaspersky Endpoint Agent для Windows см. в отдельном разделе.

Создание политики Kaspersky Endpoint Agent для Linux

Чтобы создать политику Kaspersky Endpoint Agent для Linux с помощью Kaspersky Security Center Web Console, выполните следующие действия:

1. Войдите в программу Kaspersky Security Center Web Console.
2. На закладке **Устройства** выберите **Политики и профили политик**.
3. Нажмите на кнопку **Добавить**.

   Следуйте далее указаниям мастера создания новой политики.
4. На первом шаге мастера выберите программу **Kaspersky Endpoint Agent**.
5. Нажмите на кнопку **Далее**.

6. Убедитесь, что флажок **Kaspersky Endpoint Detection and Response Expert (KATA EDR)** установлен.

7. Нажмите на кнопку **Далее**.

8. На последнем шаге мастера укажите новое имя политики, измените состояние политики (по умолчанию, политика *Активна*) и настройте наследование параметров.

9. Нажмите на кнопку **Сохранить**.

Созданная политика отобразится в списке политик.

Включение параметров в политике Kaspersky Endpoint Agent для Linux

Чтобы включить параметры в политике Kaspersky Endpoint Agent для Linux с помощью Kaspersky Security Center Web Console, выполните следующие действия:

1. Войдите в программу Kaspersky Security Center Web Console.

2. На закладке **Устройства** выберите **Политики и профили политик**.

3. Нажмите на созданную ранее политику **Kaspersky Endpoint Agent**.

   Откроется окно настроек политики.

4. Выберите раздел **Параметры программы**.

   a. Выберите подраздел **Другие параметры**.

   b. Выберите один из следующих вариантов использования прокси-сервера:

   - **Не использовать прокси-сервер**.
   - **Использовать прокси-сервер с указанными параметрами**.

   Если вы выбрали вариант **Использовать прокси-сервер с указанными параметрами**, в полях **Имя или IP-адрес сервера** и **Порт** введите адрес и порт прокси-сервера, соединение с которым вы хотите установить. По умолчанию используется порт 8080.

   Kaspersky Endpoint Agent для Linux не обеспечивает шифрование соединения с прокси-сервером. Необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Endpoint Agent для Linux.

   Если вы хотите использовать NTLM-аутентификацию при подключении к прокси-серверу, выполните следующие действия:

   1. Установите флажок **Использовать NTLM-аутентификацию по имени пользователя и паролю**.

   2. В поле **Имя пользователя** введите имя пользователя, учетная запись которого будет использоваться для авторизации на прокси-сервере.

   3. В поле **Пароль** введите пароль подключения к прокси-серверу.

   Вы можете включить отображение символов пароля, нажав на кнопку **Показать** справа от поля **Пароль**.

Если вы не хотите использовать прокси-сервер для внутренних адресов вашей организации, установите флажок **Не использовать прокси-сервер для локальных адресов**.

Если вы настраиваете свойства политики, в правом верхнем углу блока параметров измените положение переключателя с **Не определено** на **Принудительно**.

c. Нажмите на кнопку **OK**.

5. В разделе **Интеграция с KATA** выполните следующие действия:

a. Перейдите в подраздел **Общие параметры**.

b. В блоке **Параметры передачи данных** переведите переключатель **Принудительно** в активное состояние.

c. В поле **Максимальное время передачи события (сек.)** введите значение 30.

d. В поле **Максимальное количество событий в одном пакете** введите значение 1024.

e. В блоке **Регулирование количества запросов** установите флажок **Включить регулирование количества запросов**.

f. Введите значение для максимального количества событий в час и значение процента превышения лимита событий.

g. Нажмите на кнопку **OK**.

h. Перейдите в подраздел **Параметры интеграции с KATA**.

i. В блоке **Параметры подключения** переведите переключатель **Принудительно** в активное состояние.

j. Установите флажок **Включить интеграцию с KATA**.

k. Введите адрес и порт сервера KATA в поля **Сервер** и **Порт**.

l. Установите флажок **Использовать закрепленный сертификат для защиты соединения**.

m. Нажмите на кнопку **Добавить TLS-сертификат**.

n. В открывшейся вкладке нажмите на кнопку **Загрузить** и выберите файл сертификата сервера для организации безопасного соединения или введите данные сертификата в поле **Данные TLS-сертификата**.

o. Нажмите на кнопку **OK**.

p. В блоке **Дополнительная защита подключения** установите флажок **Защита подключения с помощью сертификата клиента**.

q. Нажмите на кнопку **Загрузить криптоконтейнер** и выберите файл клиентского сертификата для организации безопасного соединения.

r. В поле **Пароль криптоконтейнера** введите пароль клиентского сертификата для организации безопасного соединения.

s. В блоке **Дополнительно** выполните следующие действия:

a. В поле **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)** введите значение интервала синхронизации в минутах.

b. Установите флажок **Учитывать период TTL при отправке событий**.

c. В поле **Период TTL (мин.)** введите значение интервала отправления запроса на синхронизацию.

t. Нажмите на кнопку **OK**.

6. Нажмите на кнопку **Сохранить**.

Необходимые параметры политики для работы Kaspersky Endpoint Agent для Linux будут включены.

Управление задачами обновления баз и модулей Kaspersky Endpoint Agent

Вы так же можете создавать и настраивать параметры задач обновления баз и модулей программы с помощью Kaspersky Security Center Web Console (см. информацию в разделе справки, описывающем создание и настройку параметров задачи обновления баз и модулей программы в программе Kaspersky Endpoint Agent для Windows).

Вы так же можете настроить обновление баз и модулей программы с помощью командной строки.

Управление Kaspersky Endpoint Agent для Linux с помощью командной строки

Вы можете выполнять отдельные команды Kaspersky Endpoint Agent для Linux через интерфейс командной строки.

Функциональность интерфейса командной строки обеспечивает утилита lenactl. Эта утилита входит в комплект поставки программы и устанавливается на каждую рабочую станцию в директорию /opt/kaspersky/epagent/sbin/.

Для выполнения команд программы через интерфейс командной строки, выполните следующие действия:

1. На устройстве запустите терминал командной строки.
2. Введите команду `export PATH="$PATH:/opt/kaspersky/epagent/sbin/"`.
3. Нажмите на клавишу **ENTER**.

   Теперь вы сможете обращаться к утилите lenactl без указания пути к файлу.
4. Введите нужную команду в формате `lenactl --param1 value`.
5. Нажмите на клавишу **ENTER**.

В результате команда будет выполнена.

Полный список параметров и соответствующих значений приведен ниже.

Основные команды программы

`--product`

Этот параметр используется для запуска, остановки или вывода текущего состояния программы.

Допустимые значения параметра:

- `--product start` – запустить выгруженную программу; после выполнения этой команды остановленная служба программы должна быть запущена;
- `--product stop` – остановить запущенную программу; после выполнения этой команды запущенная служба программы должна быть остановлена;
- `--product state` – вывести в командную консоль текущее состояние программы ("запущена" или "остановлена").

`--update`

Этот параметр используется для однократного обновления баз и модулей программы.

Допустимые значения и дополнительные параметры:

- `--update` – обновить базы программы с серверов "Лаборатории Касперского";
- `--update <источник_обновлений>` – обновить базы программы из указанного источника;
- `--update --app` – обновить базы и модули программы с серверов "Лаборатории Касперского";
- `--update <источник_обновлений> --app` – обновить базы и модули программы из указанного источника.

`--local-update-task`

Этот параметр используется для обновления баз и модулей программы по расписанию с помощью локальной задачи.

> Локальная задача обновления по расписанию создается автоматически при первом запуске программы. По умолчанию, задача находится в неактивном состоянии. После создания задачи обновления при помощи Kaspersky Security Center, локальная задача автоматически удаляется без возможности восстановления.

Допустимые значения и дополнительные параметры:

- `--local-update-task enable-schedule` – включить ежечасное обновление баз программы с серверов "Лаборатории Касперского";
- `--local-update-task --app enable-schedule` – включить ежечасное обновление баз и модулей программы с серверов "Лаборатории Касперского";
- `--local-update-task disable-schedule` – выключить ежечасное обновление баз программы с серверов "Лаборатории Касперского";
- `--local-update-task --app disable-schedule` – выключить ежечасное обновление баз и модулей программы с серверов "Лаборатории Касперского";
- `--local-update-task <источник_обновлений>` – обновлять базы программы из указанного источника.

`--proxy`

Этот параметр используется для применения прокси-сервера.

> Kaspersky Endpoint Agent для Linux не обеспечивает шифрование соединения с прокси-сервером. Необходимо самостоятельно обеспечить безопасное сетевое соединение между вашим прокси-сервером и Kaspersky Endpoint Agent для Linux.

Допустимые значения и дополнительные параметры:

- `--server` – адрес прокси-сервера;
- `--port` – порт прокси-сервера;
- `--user` – имя пользователя прокси-сервера (опционально);
- `--password` – пароль прокси-сервера (если указано имя пользователя);
- `--use-for-local` – использовать прокси-сервер для локальных адресов.

`--traces`

Этот параметр используется для работы с файлами трассировки программы.

> Файлами трассировки считаются все файлы, находящиеся в директории для файлов трассировки.

Допустимые значения и дополнительные параметры:

- `--traces --on` – включить режим получения файлов трассировки;
- `--traces --off` – выключить режим получения файлов трассировки;
- `--traces --clear` – удалить все файлы трассировки в директории;
- `--traces --copyto <путь к директории>` – скопировать файлы трассировки в указанную директорию.

> Системная служба ведения и хранения журналов systemd-journald может быть активна независимо от работы приложения и может записывать свои журналы работы. Это может привести к замедлению работы программы с файлами трассировки и уменьшению свободного дискового пространства.

Чтобы отключить ведение журналов аудита системной службой systemd-journald, выполните следующие команды:

1. `systemctl mask systemd-journald-audit.socket`
2. `systemctl restart systemd-journald`

`--help`

Этот параметр используется для вывода на экран текста справки по параметрам работы с командной строкой.

Команды для настройки взаимодействия программы с сервером EDR

`--servers`

Этот параметр используется для указания адреса и порта сервера EDR.

Аргументы могут быть представлены списком пар server:port, разделенных точкой с запятой. На вход может быть передано несколько пар server:port, при этом программа игнорирует в работе все пары, кроме первой в списке.

Значение по умолчанию отсутствует.

`--timeout`

Этот параметр используется для указания таймаута соединения с сервером EDR в миллисекундах.

Аргумент может быть представлен в виде числа.

Значение по умолчанию: 100000.

`--sync-period`

Этот параметр используется для указания периода синхронизации с сервером EDR в секундах.

Аргумент может быть представлен в виде числа; допустимый диапазон значений: 5-3600.

Значение по умолчанию: 300.

`--send-packet-period`

Этот параметр используется для указания частоты отправки пакетов телеметрии.

Аргумент: число; допустимый диапазон значений: 5-999.

Значение по умолчанию: 30

`--max-events-per-packet`

Этот параметр используется для указания максимального количества событий в пакете телеметрии.

Аргумент: число, допустимый диапазон значений: 5-10000

Значение по умолчанию: 1024.

--compression

Этот параметр используется для применения сжатия.

Аргументы: <yes|no>.

Значение по умолчанию: no.

--tls

Этот параметр используется для применения tls-шифрования.

Аргументы: <yes|no>.

Значение по умолчанию: no.

--pinned-certificate

Этот параметр используется для указания пути к публичной части серверного сертификата.

Аргумент: <path to public part of server pinned certificate>.

Значение по умолчанию отсутствует.

--client-certificate

Этот параметр используется для указания пути к контейнеру с клиентским сертификатом.

Аргумент: <path to client certificate>.

Значение по умолчанию отсутствует.

--client-password

Этот параметр используется для указания пароля от контейнера с клиентским сертификатом.

Аргумент: <password>.

Значение по умолчанию отсутствует.

Проверка целостности компонентов программы Kaspersky Endpoint Agent для Linux

Чтобы избежать подмены манифеста и файлов программы, в Kaspersky Endpoint Agent предусмотрена проверка их целостности. Утилита проверки целостности роверяет целостность файлов и модулей, перечисленных в специальных списках, которые называются файлы манифеста. Файл манифеста компонента программы содержит файлы и модули, целостность которых важна для корректной работы компонента. Целостность самих файлов манифеста также проверяется.

По умолчанию, утилита проверки целостности расположена в директории /opt/kaspersky/epagent/sbin.

Для запуска утилиты проверки целостности, выполните следующие действия:

1. На устройстве запустите терминал командной строки.
2. Введите команду `./integrity_checker --signature-type kds-with-filename [другие параметры] [<путь к манифесту>]`.

   В результате в терминале будет отображена статистика проверки, а также код возврата:

- `0` - целостность манифеста и файлов Kaspersky Endpoint Agent не нарушена;
- `1` - в других случаях.

Список параметров и аргументов приведен ниже.

`<путь к манифесту>`

Этот аргумент используется для проверки целостности манифеста, расположенного по указанному пути. Если этот параметр не указан, утилита использует в качестве манифеста файл с именем integrity_check.xml, расположенный в директории утилиты.

`--verbose`

Этот параметр используется для вывода результата проверки целостности для каждого файла и подробное описание ошибок проверки целостности, если таковые произошли.

`--trace <путь к файлу>`

Этот параметр используется для указания файла для сохранения данных трассировки уровня DEBUG.

Если этот параметр не используется, данные трассировки не сохраняются.

`--crl <путь к списку отозванных сертификатов>`

Этот параметр используется для проверки подписи манифеста с использованием списка отозванных сертификатов, расположенного по указанному пути.

Создание резервной копии и восстановление программы

Если вы используете неотказоустойчивую версию Kaspersky Anti Targeted Attack Platform, вы можете создать резервную копию программы, а затем восстановить ее из резервной копии.

Для отдельного сервера Central Node вы можете создать резервную копию данных этого сервера Central Node.

Если вы используете режим распределенного решения и мультитенантности, вы можете:

- Создать резервную копию данных PCN.
- 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 нужно 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.
- Объектов в Хранилище.
- Файлов из обнаружений, выполненных при повторной проверке (rescan).
- Артефактов Sandbox.
- Конфигурационных файлов.
- Данных о лицензиях KATA и KEDR.

- Параметров Central Node или PCN:
  - Если вы используете отдельный сервер Central Node, создается резервная копия параметров Central Node.
  - Если вы используете режим распределенного решения и мультитенантности и работаете на сервере PCN, создается резервная копия параметров PCN.
  - Если вы используете режим распределенного решения и мультитенантности и работаете на сервере SCN, вы можете создать резервную копию SCN, но при восстановлении данных из резервной копии роль сервера изменится с SCN на отдельный сервер Central Node.

Вы можете очистить директорию перед созданием резервной копии программы.

Перед восстановлением программы из резервной копии на сервере Central Node или PCN, на котором вы выполняете восстановление программы, происходит очистка:

- Базы данных программы.
- Объектов в Хранилище.
- Файлов из обнаружений, выполненных при повторной проверке (rescan).
- Артефактов Sandbox.
- Конфигурационных файлов.
- Данных о лицензиях KATA и KEDR.
- Параметров Central Node или PCN.

Состав и объем данных, экспортируемых для создания резервной копии программы

Максимальный объем данных	Тип данных	Экспортируемые данные	Режим работы с программой
4 ГБ	• Параметры Central Node. • Базы данных программы на Central Node: • обнаружения и наличие у обнаружений статуса VIP; • задачи и результаты их выполнения; • политики; • пользовательские правила TAA (IOA) и исключения; • пользовательские правила IDS и исключения; • IOC-файлы; • правила исключений из проверки; • информация о файлах в Хранилище; • информация об объектах на карантине; • список компьютеров с Endpoint Agent; • отчеты и шаблоны отчетов; • данные учетных записей пользователей; • 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 мультитенантности.
4 ГБ	Параметры SCN.	По выбору. Как для отдельного сервера Central Node.	Режим распределенного решения и мультитенантности.
4 ГБ	Базы данных программы на PCN: • обнаружения и наличие у обнаружений статуса VIP; • результаты выполнения задач; • политики; • пользовательские правила TAA (IOA) и исключения; • пользовательские правила IDS и исключения; • IOC-файлы; • список данных, исключенных из проверки; • информация о файлах в Хранилище; • информация об объектах на карантине; • список хостов Kaspersky Endpoint Agent; • отчеты и шаблоны отчетов; • данные учетных записей пользователей; • уведомления.	По умолчанию.	Режим распределенного решения и мультитенантности.
Нет	Конфигурационные файлы.	Да	Все режимы.
Нет	Лицензии KATA и KEDR.	Да	Все режимы.
300 ГБ	Хранилище.	По выбору.	Все режимы.

Максимальный объем данных	Тип данных	Экспортируемые данные	Режим работы с программой
300 ГБ	Артефакты Sandbox.	По выбору.	Все режимы.
300 ГБ	Файлы из обнаружений, выполненных при повторной проверке (rescan).	По выбору.	Все режимы.
Нет	База событий.	Нет.	Все режимы.

Файлы, которые в момент создания резервной копии программы находились в очереди на проверку, не экспортируются.

Версии восстанавливаемой и установленной на сервер программ должны совпадать. Если версии программ не совпадают, при запуске восстановления программы отобразится сообщение об ошибке и процесс восстановления будет прерван.

Создание резервной копии параметров сервера Central Node из меню администратора программы

Чтобы создать резервную копию параметров Central Node (PCN или SCN в режиме распределенного решения и мультитенантности), выполните следующие действия в меню администратора сервера:

1. В списке разделов меню администратора программы выберите раздел **System administration**.
2. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
3. В списке действий выберите **Backup/Restore settings**.
4. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup/Restore settings**.
5. В списке действий выберите **New**.
6. Нажмите на клавишу **ENTER**.

   Откроется окно **Backup settings**.
7. Нажмите на кнопку **Back up**.

Резервная копия параметров сервера будет создана.

Загрузка файла с резервной копией параметров сервера с сервера Central Node или PCN на жесткий диск компьютера

Рекомендуется сохранять файлы с резервной копией параметров сервера Central Node на жесткий диск вашего компьютера.

Чтобы загрузить файл с резервной копией параметров сервера Central Node 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 параметров сервера, созданной на сервере Central Node с IP-адресом 10.0.0.10 под учетной записью admin 10 апреля 2020 года в 10 часов 00 минут 00 секунд:

```
scp admin@10.0.0.10:settings-20200410-100000.tar.gz
```

Файл с резервной копией параметров сервера будет сохранен на жесткий диск вашего компьютера в текущую директорию.

Загрузка файла с резервной копией параметров сервера с вашего компьютера на сервер Central Node

Чтобы загрузить файл с резервной копией параметров сервера Central Node с жесткого диска вашего компьютера на сервер, выполните следующую команду в режиме Technical Support Mode:

```
scp <имя файла с резервной копией параметров сервера 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 параметров сервера, созданной 10 апреля 2020 года в 10 часов 00 минут 00 секунд, на сервер Central Node с IP-адресом 10.0.0.10 под учетной записью admin:

```
scp settings-20200410-100000.tar.gz admin@10.0.0.10:
```

Файл с резервной копией параметров сервера будет загружен на сервер Central Node в текущую директорию.

Восстановление параметров сервера из резервной копии через меню администратора программы

Для восстановления параметров сервера Central Node из резервной копии нужно предварительно создать резервную копию текущих параметров сервера. В случае сбоя при восстановлении параметров сервера вы сможете воспользоваться сохраненной копией параметров сервера.

Чтобы восстановить параметры сервера из уже созданной ранее резервной копии, выполните следующие действия в меню администратора 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 параметры сервера.

   Если нужного файла нет в списке, вам нужно загрузить файл с резервной копией параметров на сервер.
6. Нажмите на клавишу **ENTER**.

   Откроется окно выбора действий.
7. В списке действий выберите **Restore <имя файла с резервной копией параметров сервера>**.
8. Нажмите на клавишу **ENTER**.

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

Параметры сервера будут восстановлены из выбранного файла.

Если аппаратная конфигурация сервера Central Node, на котором была создана резервная копия, отличается от аппаратной конфигурации сервера, на котором вы планируете восстановить параметры сервера, после восстановления вам нужно заново настроить параметры масштабирования 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 сервера:

```
kata-backup-restore backup
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

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	`-c`	Очистить директорию перед сохранением файла с резервной копией программы.
Нет	`-d <number of stored files>`	Указать максимальное количество файлов с резервной копией программы, хранимых в директории, где <number> – количество файлов.
Нет	`-e`	Сохранить файлы в Хранилище.

Нет	`-q`	Сохранить файлы на карантине.
Нет	`-a`	Сохранить файлы, ожидающие повторной проверки (rescan).
Нет	`-s`	Сохранить артефакты Sandbox.
Нет	`-n`	Сохранить параметры Central Node или PCN.
Нет	`-l <filepath>`	Сохранить результат выполнения команды в файл, где <filepath> – имя файла журнала событий, включая абсолютный или относительный путь к файлу.

Если дополнительные параметры не указаны, резервная копия Kaspersky Anti Targeted Attack Platform будет содержать только базы данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, 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 – KATA5.0.sql для резервной копии программы версии 5.0.

Пример:

Команда для создания резервной копии программы:

```
kata-backup-restore backup -b <path> -c -d <number of stored files> -e -q -a -s -n -l <filepath>
```

Восстановление программы из резервной копии в режиме Technical Support Mode

Для восстановления Kaspersky Anti Targeted Attack Platform из резервной копии нужно предварительно создать резервную копию текущего состояния программы и загрузить ее на жесткий диск вашего компьютера. В случае сбоя при восстановлении программы или при необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией программы.

Версии восстанавливаемой и установленной на сервер программ должны совпадать. Если версии программ не совпадают, при запуске восстановления программы отобразится сообщение об ошибке и процесс восстановления будет прерван.

Чтобы восстановить Kaspersky Anti Targeted Attack Platform из резервной копии, выполните следующую команду в режиме Technical Support Mode сервера:

```
kata-backup-restore restore
```

Вы также можете указать один или несколько параметров к этой команде (см. таблицу ниже).

Подсказка по использованию параметров доступна по команде `-h`.

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> – полный путь к файлу с резервной копией программы.
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:

```
kata-backup-restore restore -r <path> -l <filepath>
```

Обновление Kaspersky Anti Targeted Attack Platform

Вы можете обновить программу Kaspersky Anti Targeted Attack Platform с версии 4.1 до версии 5.0. При обновлении устанавливается неотказоустойчивая версия программы.

Если для настройки даты и времени сервера Central Node вы использовали один NTP-сервер, перед обновлением Kaspersky Anti Targeted Attack Platform рекомендуется удалить этот NTP-сервер или настроить интеграцию с еще одним NTP-сервером. Иначе при обновлении может возникнуть ошибка.

В качестве дополнительного NTP-сервера допускается использовать недоступный или нерабочий сервер.

Обновление программы включает в себя следующие этапы:

1. Обновление компонента Sandbox.

   В программе не предусмотрена стандартная процедура обновления. Вам требуется установить компонент версии 5.0.

   После установки компонента вам нужно указать максимальное количество одновременно запускаемых виртуальных машин. По умолчанию используется значение 48.

   При установке компонента на виртуальную машину VMware ESXi вам требуется задать для нее конфигурацию, описанную в разделе *Расчеты для компонента Sandbox*.

2. Обновление компонента Central Node.

   Обновление компонента до версии 5.0 возможно только с версии 4.1. Если вы используете более раннюю версию, требуется последовательно обновить версии компонента до версии 4.1: 3.7 → 3.7.1, 3.7.1 → 3.7.2, 3.7.2 → 4.0, 4.0 → 4.1.

   Для обновления компонента Central Node на сервере с этим компонентом требуется предварительно запустить скрипт kata-upgrade-preparation. Скрипт входит в комплект поставки программы.

   Если вы не используете режим распределенного решения и мультитенантности и используете отдельный сервер Central Node, вы можете обновить программу на сервере Central Node.

   Если вы используете режим распределенного решения и мультитенантности:

   a. Вы можете обновить программу на сервере PCN. После обновления программы сервер PCN будет относиться к тому же тенанту, к которому он относился до обновления.

   b. 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 тенант, к которому относится сервер SCN.

c. 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.

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. Для этого выполните следующие действия в веб-интерфейсе сервера PCN:

a. Добавьте необходимые тенанты.

b. Настройте доступ учетных записей пользователей с ролью **Старший сотрудник службы безопасности** и **Сотрудник службы безопасности** к этим тенантам и серверам.

c. Удалите все SCN, временно отключенные от PCN при обновлении.

d. Повторно подключите к PCN все необходимые SCN.

При этом программа предложит вам выбрать тенант 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.

3. Обновление компонента Sensor, установленного на отдельный сервер.

   В программе не предусмотрено стандартной процедуры обновления. Вам требуется установить компонент версии 5.0.

4. Обновление компонента Kaspersky Endpoint Agent:

   - Kaspersky Endpoint Agent для Windows.

     Если вы используете решение совместно с Kaspersky Security для Windows Server, вы можете выполнить миграцию с Kaspersky Security для Windows Server на Kaspersky Endpoint Security для Windows версии 12.1 и выше, которая содержит встроенный агент. Подробнее о миграции см. в справке приложения Kaspersky Endpoint Security для Windows.

   - Kaspersky Endpoint Agent для Linux.

   - Kaspersky Endpoint Security для Windows.

Особенности обновления Kaspersky Anti Targeted Attack Platform с версии 4.1 до версии 5.0

1. После обновления Kaspersky Anti Targeted Attack Platform до версии 5.0 вам нужно будет заново добавить лицензионные ключи программы.
2. **Не** сохраняются пользовательские схемы расположения виджетов в разделе **Мониторинг** после обновления программы.
3. **Не** сохраняются параметры сетевых интерфейсов. Если вы хотите использовать сетевые интерфейсы для получения зеркалированного SPAN-трафика, после обновления вам требуется настроить захват трафика.
4. Данные компонентов Sensor и Sandbox **не** сохраняются.
5. Совместимость сервера Central Node 5.0 с компонентами Sensor и Sandbox более ранней версии **не** поддерживается.

Обновление компонента Central Node

Обновление компонента до версии 5.0 возможно только с версии 4.1. Если вы используете более раннюю версию, требуется последовательно обновить версии компонента до версии 4.1: 3.7 → 3.7.1, 3.7.1 → 3.7.2, 3.7.2 → 4.0, 4.0 → 4.1.

Для обновления компонента Central Node на сервере с этим компонентом требуется предварительно запустить скрипт kata-upgrade-preparation. Скрипт входит в комплект поставки программы.

Чтобы обновить компонент Central Node:

1. Поместите пакет скрипта на сервер с компонентом Central Node.
2. Войдите в консоль управления сервера Central Node, на котором вы хотите обновить компонент, по протоколу SSH или через терминал.
3. Установите пакет, выполнив команду `sudo pip3 install /tmp/upgrade_preparation-1.0-py3-none-any.whl`.
4. Запустите скрипт, выполнив команду `sudo /usr/local/bin/kata-upgrade-preparation`.
5. Запустите образ диска с компонентами Central Node и Sensor.
6. Выполните шаги по развертыванию компонента.
7. Задайте параметры масштабирования программы в веб-интерфейсе по управлению масштабированием.

Компонент Central Node будет обновлен.

Состав и объем данных, сохраняемых при обновлении программы Kaspersky Anti Targeted Attack Platform

Состав и объем данных, сохраняемых при обновлении программы Kaspersky Anti Targeted Attack Platform с версии 4.1 до версии 5.0 представлен в таблице ниже.

Состав и объем данных, сохраняемых при обновлении программы с версии 4.1 до версии 5.0

Тип данных	Данные, сохраняемые при обновлении
Параметры Central Node или PCN.	Все данные, кроме: • лицензионных ключей; • параметров интеграции с компонентом Sandbox; • параметров интеграции с компонентом Sensor.
Базы данных программы на Central Node или PCN (база обнаружений, данные мониторинга работы программы, база пользовательских правил, задачи, политики, правила, добавленные в исключения).	Все данные, кроме: • файлов, которые в момент обновления Kaspersky Anti Targeted Attack Platform до версии 5.0 находились в очереди на проверку; • файлов, которые в момент обновления Kaspersky Anti Targeted Attack Platform до версии 5.0 находились в очереди на повторную проверку (rescan); • данных отчетов.
База событий.	Все данные.
Хранилище и карантин.	Все данные.
Артефакты Sandbox.	Все данные.

Взаимодействие с внешними системами по API

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с внешними системами, чтобы управлять действиями по реагированию на угрозы, а также для проверки хранящихся в них файлов и предоставления внешним системам доступа к информации обо всех обнаружениях программы.

Взаимодействие внешних систем с Kaspersky Anti Targeted Attack Platform осуществляется с помощью интерфейса API. Вызовы методов API доступны только для авторизованных внешних систем. Для авторизации администратору программы необходимо создать запрос на интеграцию внешней системы с программой. После этого администратор должен обработать запрос в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Если вы развернули компоненты Central Node и Sensor в виде кластера, вы можете настроить отказоустойчивую интеграцию с внешней системой одним из следующих способов:

- Использовать функцию Round Robin.
- Настроить параметры внешней системы, чтобы при возникновении таймаута внешняя система переключалась между IP-адресами серверов кластера.

Чтобы настроить отказоустойчивую интеграцию с внешней системой:

1. Настройте на сервере DNS функцию Round Robin для доменного имени, соответствующего кластеру Central Node.
2. В параметрах почтового сервера укажите это доменное имя.

   Интеграция с почтовым сервером будет настроена по доменному имени. Почтовый сервер обратится к случайному серверу кластера. При отказе этого сервера почтовый сервер будет обращаться к другому работоспособному серверу кластера.

Интеграция внешней системы с Kaspersky Anti Targeted Attack Platform

Для начала работы с API необходимо выполнить интеграцию внешней системы с Kaspersky Anti Targeted Attack Platform. Внешняя система должна пройти авторизацию на сервере Kaspersky Anti Targeted Attack Platform.

Чтобы выполнить интеграцию внешней системы с Kaspersky Anti Targeted Attack Platform:

1. Сгенерируйте уникальный идентификатор внешней системы для авторизации в Kaspersky Anti Targeted Attack Platform – `sensorId`.

2. Сгенерируйте сертификат сервера внешней системы.

3. Создайте любой запрос от внешней системы в Kaspersky Anti Targeted Attack Platform, содержащий идентификатор `sensorId`. Например, вы можете создать запрос на проверку объекта из внешней системы в Kaspersky Anti Targeted Attack Platform.

В веб-интерфейсе Kaspersky Anti Targeted Attack Platform отобразится запрос на авторизацию от внешней системы. Обратитесь к администратору программы для обработки запроса.

Если вам нужно сменить сертификат сервера внешней системы, выполните действия по интеграции внешней системы в Kaspersky Anti Targeted Attack Platform повторно.

API для проверки объектов внешних систем

Kaspersky Anti Targeted Attack Platform предоставляет HTTPS REST интерфейс проверки объектов, хранящихся во внешних системах.

Для проверки объектов, хранящихся во внешних системах, рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. **Создание запроса на проверку объектов HTTP-методом `POST`**

2. **Создание запроса на получение результатов проверки HTTP-методом `GET`**

   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 HTTP-методом `GET`. Рекомендуемая периодичность отправки запроса 1 раз в минуту.

   Вы также можете настроить отправку уведомлений об обнаруженных объектах в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

3. **Создание запроса на удаление результатов проверки HTTP-методом `DELETE`**

   Вы можете удалить результаты проверки указанного объекта или всех объектов.

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 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 создании запроса HTTP-методом `POST` выдается код возврата 413. Вы можете узнать максимально допустимый размер объекта, просмотрев список ограничений программы на проверку объектов с помощью метода `GET`.

Запрос на проверку объектов

Для создания запроса на проверку объектов используется HTTP-метод `POST`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Вы можете задавать параметры выполнения команды cURL с помощью дополнительных ключей (см. таблицу ниже).

Подробную информацию о ключах команд cURL см. в документации cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/scans?sensorInstanceId=
<идентификатор sensorInstanceId>" -F "content=<путь к файлу, который вы хотите
проверить>" -F scanId=<идентификатор запроса на проверку> -F "objectType=file"
```

При успешной обработке запроса отобразится статус `"OK"`.

Параметры

Параметр	Тип	Описание
`sensorId`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`content`	file	Содержимое проверяемого объекта.

Параметр	Тип	Описание
`scanId`	string	Уникальный идентификатор запроса на проверку. Должен быть сформирован на стороне внешней системы. Не может содержать пробелы и специальные символы. Не используйте имена файлов в качестве идентификатора запроса на проверку. Если этот параметр не указан, просмотр результатов проверки недоступен.
`objectType`	string	Тип проверяемого объекта. Возможное значения параметра: `file`.
`sensorInstanceId`	string	Уникальный идентификатор экземпляра внешней системы. Экземплярами внешней системы считаются также серверы, объединенные в кластер. Параметр не является обязательным.

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.

Пример ввода команды с параметрами

```
curl --cert /root/cert.pem --key /root/server.key -
X POST "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans?
sensorInstanceId=instance1" -F "content=@/tmp/test" -F scanId=1 -F "objectType=file"
```

Запрос на получение результатов проверки

Для создания запроса на получение результатов проверки используется HTTP-метод `GET`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Вы можете задавать параметры выполнения команды cURL с помощью дополнительных ключей (см. таблицу ниже).

Подробную информацию о ключах команд cURL см. в документации cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X
GET<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/scans/state?sensorInstanceId=
<идентификатор sensorInstanceId>&state=<один или несколько статусов проверки, которые вы
хотите отобразить в результатах проверки>"
```

При успешной отправке запроса отобразится список запросов на проверку объектов и результаты проверки этих объектов. Результаты проверки будут отфильтрованы по статусам, которые вы указали в параметре `state`. Например, если в запросе на получение результатов проверки вы указали статусы `state=processing,detect`, отобразятся только запросы на проверку объектов, которые находятся в обработке или в которых программа обнаружила угрозу.

Параметры

Параметр	Тип	Описание
`sensorId`	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`state`	array (тип элементов string)	Статус проверки объекта. При указании этого параметра результаты проверки будут отфильтрованы по статусу. Указывайте один или несколько статусов через запятую. Возможны следующие значения параметра: • `detect`; • `not detected`; • `processing`; • `timeout`; • `error`.
`sensorInstanceId`	string	Уникальный идентификатор экземпляра внешней системы. Экземплярами внешней системы считаются также серверы, объединенные в кластер. Параметр не является обязательным.

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.

Пример ввода команды с параметрами, если вы хотите отобразить все статусы проверки объектов в результатах проверки

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/state?sensorInstanceId=instance1&state=detect,not%20detected,processing,error,timeout"
```

Запрос на удаление результатов проверки

Для создания запроса на удаление результатов проверки одного или нескольких объектов используется метод `DELETE`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X DELETE
"<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/scans/<идентификатор scanId>"
```

При успешной обработке запроса результаты проверки объекта будут удалены. Отобразится статус `"OK"`.

Параметры

Параметр	Тип	Описание
`sensorId`	string	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`scanId`	string	Уникальный идентификатор запроса на проверку объекта. 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.

Пример ввода команды

```
curl --cert /root/cert.pem --key /root/server.key -
X DELETE "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/1"
```

Запрос на вывод ограничений программы на проверку объектов

Для создания запроса на вывод ограничений программы на проверку объектов (например, по размеру) используется HTTP-метод `GET`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/scans/filters"
```

При успешной обработке запроса отобразятся ограничения программы на проверку объектов. Например, ограничение `maxObjectSize` – максимально допустимый размер объекта, который вы можете отправить на проверку.

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.

Пример ввода команды

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-
a00b-111c-b11a-11001b1f1111/scans/filters"
```

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 на вывод информации об обнаружениях

Для создания запроса на вывод информации об обнаружениях Kaspersky Anti Targeted Attack Platform используется HTTP-метод `GET`. Создать запрос можно, например, с помощью утилиты командной строки cURL.

Синтаксис команды

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/scanner/v1/sensors/<идентификатор sensorId>/detects?detect_type=<одна или
несколько технологий, с помощью которых выполнено обнаружение>&limit=<количество
обнаружений в ответе на запрос>&token=<идентификатор запроса>"
```

При успешной обработке запроса отобразится список обнаружений, выполненных программой Kaspersky Anti Targeted Attack Platform на сервере внешней системы.

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; 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.

Пример ввода команды с параметрами

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/detects?detect_type=am,sb&limit=100&token=7b226f6666736574223a20307d"
```

Состав передаваемых данных

Информация, передаваемая о каждом обнаружении, представлена в таблице ниже.

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.
`detection`	Зависит от технологии, с помощью которой обнаружен объект.	Данные о найденных угрозах.
`details`	Зависит от источника обнаруженного объекта.	Данные об окружении обнаруженных объектов.

Данные об обнаруженных объектах

Состав передаваемых данных об обнаруженных объектах в зависимости от типа объекта приведен в таблице ниже.

	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.	7bbfc1d690079b0c591e146c4294305da1cee857e12db401
	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
	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
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.

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`
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.

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
	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/
	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'

Источник объекта	Параметр	Описание	Тип данных	Пример
	`messageId`	ID сообщения электронной почты.	String	`1745028736.156014.1542897410859.JavaMail.svc_jira_poc`
• `endpoint` • `external`	`hostName`	Имя компьютера, на котором выполнено обнаружение.	String	`computername.example.com`
	`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`
	`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`

API для управления действиями по реагированию на угрозы

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для осуществления действий по реагированию на угрозы. Команды на выполнение операций поступают на сервер Central Node, после чего программа передает их Kaspersky Endpoint Agent.

С помощью внешних систем вы можете выполнить следующие операции на хостах с Kaspersky Endpoint Agent:

- Управлять сетевой изоляцией хостов.
- Управлять правилами запрета.
- Запускать программы.

Все перечисленные операции доступны на хостах с Kaspersky Endpoint Agent для Windows. На хостах с Kaspersky Endpoint Agent для Linux доступна только функция запуска программы.

Запрос на получение списка хостов Kaspersky Endpoint Agent

Для создания запроса на вывод информации о хостах с Kaspersky Endpoint Agent используется HTTP-метод GET.

Синтаксис команды

```
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/sensors"
```

При успешной обработке запроса отобразится список хостов с Kaspersky Endpoint Agent.

Вы можете создать запрос на вывод информации о хостах с указанными параметрами: IP-адресом, именем или идентификатором хоста. Вы можете указать один, несколько или все параметры.

> При указании имени хоста вам нужно учитывать, что фильтр чувствителен к регистру символов.

```
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/sensors?ip=<IP-адрес
хоста>&host=<имя хоста>&sensor_id=<идентификатор sensor_id>"
```

При успешной обработке запроса отобразится информация о выбранном хосте с Kaspersky Endpoint Agent.

Параметры

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Уникальный идентификатор хоста Kaspersky Endpoint Agent.
`ip`	string	IP-адрес хоста Kaspersky Endpoint Agent.
`host`	string	Имя хоста Kaspersky Endpoint Agent.

Пример ввода команд с параметрами

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors"
```

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors?
ip=10.16.40.243&host=host4&sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0"
```

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Требуется авторизация.
401	Ошибка ввода параметров.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на получение информации о сетевой изоляции и наличии правил запрета для хостов Kaspersky Endpoint Agent

Для создания запроса на вывод информации о сетевой изоляции и наличии правил запрета для хостов Kaspersky Endpoint Agent используется HTTP-метод GET.

Синтаксис команды

```
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id>&settings_type=<network_isolation или prevention>"
```

При успешной обработке запроса отобразится список хостов Kaspersky Endpoint Agent, для которых на момент выполнения запроса применены правила запрета или сетевой изоляции.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста Kaspersky Endpoint Agent.
settings_type	enum	Тип правила - network_isolation или prevention.

Пример ввода команды с параметрами

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&settings_type=network_izolation"
```

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Требуется авторизация.
401	Ошибка ввода параметров.
404	Не найден указанный хост Kaspersky Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка. Повторите запрос позднее.

Управление сетевой изоляцией хостов

Для изоляции хоста Kaspersky Endpoint Agent с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. **Создание запроса на получение списка хостов Kaspersky Endpoint Agent**
2. **Создание запроса на получение информации о хостах, для которых уже включена сетевая изоляция**
3. **Создание запроса на одну из следующих операций с хостами Kaspersky Endpoint Agent:**
   - включение сетевой изоляции;
   - отключение сетевой изоляции;
   - добавление исключения в уже существующее правило сетевой изоляции.

Вы можете управлять созданными правилами сетевой изоляции в веб-интерфейсе программы.

Запрос на включение сетевой изоляции

Чтобы включить сетевую изоляцию для выбранного хоста, вам требуется добавить правило сетевой изоляции. Для создания запроса используется HTTP-метод POST.

Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id>&settings_type=network_isolation" -H 'Content-Type:
application/json' -d '

{

"settings": {

"autoTurnoffTimeoutInSec": <время действия сетевой изоляции>}

}

'
```

При успешной обработке запроса правило сетевой изоляции будет добавлено. Сетевая изоляция для выбранного хоста действует с момента добавления правила.

По истечении времени, указанного при создании запроса, сетевая изоляция перестанет действовать. Правило сетевой изоляции при этом не удаляется. При необходимости вы можете удалить выбранное правило.

Для отключения сетевой изоляции вам требуется создать запрос на отключение выбранного правила.

Параметры

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Уникальный идентификатор хоста Kaspersky Endpoint Agent.
`autoTurnoffTimeoutInSec`	integer	Время, в течение которого будет действовать сетевая изоляция хоста. Допустимый диапазон – от 1 до 9999 часов. Время сетевой изоляции указывается в секундах. Например, если вы хотите включить сетевую изоляцию хоста на два часа, вам требуется указать 7200 секунд.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X POST "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings": {
"autoTurnoffTimeoutInSec": 7200}
}
'
```

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост Kaspersky Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданного правила сетевой изоляции, вам требуется создать новый запрос на добавление правила с нужными параметрами.

Запрос на отключение сетевой изоляции

Чтобы отключить сетевую изоляцию для выбранного хоста, вам требуется создать запрос на отключение правила сетевой изоляции. Для создания запроса используется HTTP-метод DELETE.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X DELETE "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=<идентификатор sensor_id>&settings_type=network_isolation"
```

При успешной обработке запроса правило сетевой изоляции будет отключено.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста Kaspersky Endpoint Agent.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X DELETE "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&settings _type=network_isolation"
```

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост Kaspersky Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на добавление исключения в правило сетевой изоляции

Чтобы добавить исключение для ранее созданного правила сетевой изоляции, вам требуется создать запрос на добавление исключения. Для создания запроса используется HTTP-метод POST.

Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=<идентификатор sensor_id>&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
```

```
{
"settings":
{"excludedRules": [
{
"direction": "<outbound, inbound или both>",
"protocol": <номер IP-протокола>,
"remoteIpv4Address": "<IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик
которого не должен быть заблокирован>",
"localPortRange":
{
"fromPort": <номер порта>,
"toPort": <номер порта>
}
}
,
{
"direction": "<outbound, inbound или both>",
"protocol": <номер IP-протокола>,
"remoteIpv4Address": "<IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик
которого не должен быть заблокирован>",
"remotePortRange":
{
"fromPort": <номер порта>,
"toPort": <номер порта>
}
}
,
{
"direction": "<outbound, inbound или both>",
"protocol": <номер IP-протокола>,
"remoteIpv4Address": "<IP-адрес хоста с компонентом Endpoint Agent, сетевой трафик
которого не должен быть заблокирован>"
}
]
,
"autoTurnoffTimeoutInSec": <время действия сетевой изоляции>
}
}
'
```

При успешной обработке запроса исключение из правила сетевой изоляции будет добавлено.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста Kaspersky Endpoint Agent.

`direction`	`array`	Направление сетевого трафика, которое не должно быть заблокировано. Может иметь следующие значения: • inbound; • outbound; • both. Если вы не указали значение параметра, по умолчанию будет применено значение both и приложение будет передавать трафик в обоих направлениях.
`protocol`	`integer`	Номер IP-протокола, назначенный Internet Assigned Numbers Authority (IANA). Если вы не указали значение параметра, по умолчанию сетевая изоляция будет распространена на все протоколы.
`remoteIpv4Address`	`string`	IP-адрес хоста Kaspersky Endpoint Agent, сетевой трафик которого не должен быть заблокирован.
`remotePortRange`	`string`	Порт назначения. Вы можете указать порт, только если вы выбрали входящее или исходящее направление сетевого трафика. Для двунаправленного трафика нельзя задавать диапазон портов.
`localPortRange`	`string`	Порт, с которого устанавливается соединение. Вы можете указать порт, только если вы выбрали входящее или исходящее направление сетевого трафика. Для двунаправленного трафика нельзя задавать диапазон портов.
`autoTurnoffTimeoutInSec`	`integer`	Время, в течение которого будет действовать сетевая изоляция хоста. Допустимый диапазон – от 1 до 9999 часов. Время сетевой изоляции указывается в секундах. Например, если вы хотите включить сетевую изоляцию хоста на два часа, вам требуется указать 7200 секунд.

Пример ввода команды с параметрами

```
curl -k --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings":
{"excludedRules": [
{
"direction": "inbound",
"protocol": 6,
"remoteIpv4Address": "10.16.41.0",
"localPortRange":
{
"fromPort": 3389,
"toPort": 3389
}
}
,
{
"direction": "outbound",
"remoteIpv4Address": "10.16.41.1",
"remotePortRange":
{
"fromPort": 13957,
"toPort": 55409
}
}
,
{
"direction": "both",
"protocol": 6,
"remoteIpv4Address": "10.16.41.2"
}
]
,
"autoTurnoffTimeoutInSec": 7200
}
}
'
```

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост Kaspersky Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданного исключения, вам требуется создать новый запрос на добавление исключения с нужными параметрами.

Управление правилами запрета

С помощью правил запрета вы можете заблокировать запуск файлов или процессов на выбранном хосте или всех хостах с Kaspersky Endpoint Agent. Например, вы можете запретить запуск программ, использование которых считаете небезопасным. Программа идентифицирует файлы по их хешу с помощью алгоритмов хеширования MD5 и SHA256. Правило запрета, созданное через внешние системы, может содержать несколько хешей файлов.

Через внешние системы вы можете управлять всеми правилами запрета, созданными для одного хоста или всех хостов, одновременно. При создании правила запрета для выбранного хоста через внешние системы Kaspersky Anti Targeted Attack Platform заменяет все правила запрета, назначенные на этот хост, правилом с новыми параметрами. Например, если ранее вы добавили несколько правил запрета для выбранного хоста через веб-интерфейс программы, а потом добавили правило запрета через внешние системы, все правила запрета, добавленные в веб-интерфейсе, будут заменены добавленным через внешние системы правилом.

При изменении параметров правила запрета, созданного через внешние системы, программа сохраняет только новые параметры. Например, если вы создали правило запрета, которое содержит хеши для нескольких файлов, и хотите добавить в это правило еще один хеш, вам требуется создать запрос на добавление правила запрета и указать в нем все хеши, для которых вы создавали запрет ранее, и новый хеш.

Описанный сценарий также актуален для правил запрета, назначенных на все хосты.

Для создания правила запрета с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. Создание запроса на получение списка хостов Kaspersky Endpoint Agent
2. Создание запроса на получение информации о хостах, для которых существуют правила запрета
3. **Создание запроса на одну из следующих операций с правилами запрета:**
   - создание правила;
   - удаление правила.

Добавленные правила запрета отображаются в веб-интерфейсе программы в разделе **Политики**, подразделе **Правила запрета**.

Если вы создаете через внешнюю систему правило запрета для всех хостов, вам требуется предварительно убедиться, что на сервере отсутствует и не применяется к одному или нескольким хостам правило запрета для этого же файла. Это условие также справедливо, если вы хотите создать через внешнюю систему правило запрета для выбранного хоста: вам требуется убедиться, что на сервере отсутствует и не применяется ко всем хостам правило запрета для этого же файла. В противном случае сервер вернет внешней системе ошибку со списком хостов, к которым уже применяется правило запрета.

Если правило запрета, создаваемое через внешнюю систему, содержит несколько хешей файлов, в информации об ошибке указывается только первый файл, вызвавший ошибку. Сведения о других дублирующихся правилах запрета не отображаются.

Для изменения уже созданного через веб-интерфейс или внешние системы правила запрета вам нужно создать запрос на добавление правила запрета с обновленными параметрами.

Запрос на создание правила запрета

Для создания запроса используется HTTP-метод POST. Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id или all, если вы хотите создать правило запрета для всех
хостов>&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": [

{

"file": {

"<sha256 или md5>": "<SHA256- или MD5-хеш файла, запуск которого вы хотите запретить>"

}

},

{

"file": {

"<sha256 или md5>": "<SHA256- или MD5-хеш файла, запуск которого вы хотите запретить>"

}

'
```

При успешной обработке запроса правило запрета будет добавлено. Правило запрета действует с момента добавления.

При необходимости вы можете удалить правило запрета.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста Kaspersky Endpoint Agent.
objects	string	Тип объекта, запуск которого вы хотите запретить. Возможное значения параметра: file.
sha256 или md5	string	SHA256- или MD5-хеш объекта, запуск которого вы хотите запретить.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X POST "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '
{
"settings": {
"objects": [
{
"file": {
"sha256": "830195824b742ee59390bc5b9302688c778fc95a64e7d597e28a74c03a04dd63"
}
"file": {

"md5": "d8e577bf078c45954f4531885478d5a9"

}
'
```

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост Kaspersky Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на удаление правила запрета

Вы можете удалить правило запрета с помощью нового запроса с пустыми значениями или запроса с параметром DELETE. Для создания запросов используются HTTP-методы POST и DELETE.

Синтаксис команды для нового запроса

Параметры команды передаются в теле запроса в формате JSON.

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id или all, если вы хотите удалить правило запрета для всех
хостов>&settings_type=prevention" -H 'Content-Type: application/json' -d '

{

"settings": {

"objects": []

}

}

'
```

Синтаксис команды с параметром DELETE

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X DELETE "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=
<идентификатор sensor_id или all, если вы хотите удалить правило запрета для всех
хостов>&settings_type=prevention"
```

Параметры

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Уникальный идентификатор хоста Kaspersky Endpoint Agent.

Пример ввода команды для нового запроса

```
curl -k --example.cert --example.key -X POST "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=all&settings_type=prevention"-H 'Content-Type: application/json' -d '
{

"settings": {

"objects": []

}

}

'
```

Пример ввода команды с параметром DELETE

```
curl -k --example.cert --example.key -X DELETE "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=all&settings_type=prevention"
```

При успешной обработке запроса правило запрета будет удалено.

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Не найден указанный хост Kaspersky Endpoint Agent.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Управление задачей запуска программы

Для управления задачей запуска программы с помощью интерфейса API рекомендуется использовать следующий сценарий взаимодействия с Kaspersky Anti Targeted Attack Platform:

1. Создание запроса на получение информации о параметрах, времени создания и статусе выполнения задачи
2. **Создание запроса на одну из следующих операций с задачей:**
   - создание задачи;
   - удаление задачи.

Добавленные задачи отображаются в веб-интерфейсе программы в разделе **Задачи**.

Получение информации о задаче

Для создания запроса на получение информации о задаче используется HTTP-метод GET.

Синтаксис команды

```
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/tasks/<идентификатор
task_id>?settings=<true или false>"
```

При успешной обработке запроса отобразится информация о параметрах, времени создания и статусе выполнения задачи.

Параметры

Параметры	Тип	Описание
`external_system_id`	`UUID`	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`sensor_id`	`UUID`	Уникальный идентификатор хоста Kaspersky Endpoint Agent.
`task_id`	`UUID`	Уникальный идентификатор задачи.
`settings`	`boolean`	Может иметь следующие значения: • true. При указании этого значения отображается информация о параметрах, времени создания и статусе выполнения задачи. • false. При указании этого значения отображается информация о времени создания и статусе выполнения задачи.

Пример ввода команды с параметрами

```
GET https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-
BE0A-72A75CDB0BE8?settings=<true или false>
```

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Ошибка ввода параметров.
401	Требуется авторизация.
409	Задача с указанным идентификатором уже существует.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Запрос на создание задачи

Для создания запроса на запуск программы Kaspersky Anti Targeted Attack Platform используется HTTP-метод POST. Параметры команды передаются в теле запроса в формате JSON.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/tasks/<идентификатор
task_id>?sensor_id=<идентификатор sensor_id>&task_type=run_process" -H 'Content-Type:
application/json' -d '

{

"task": {

"shedule": {"startNow": <true или false>},

"execCommand": "<название программы, которую вы хотите запустить>",

"cmdLineParameters": "<дополнительные параметры запуска файла или выполнения команды>",

"workingDirectory": "<рабочая директория>"

}

}

'
```

При успешной обработке запроса задача на запуск программы будет создана.

Параметры

Параметр	Тип	Описание
external_system_id	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Уникальный идентификатор хоста Kaspersky Endpoint Agent.
task_id	UUID	Уникальный идентификатор задачи.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X POST "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&task_type=run_process" -H 'Content-Type: application/json' -d '
{

"task": {

"schedule": {"startNow": true},

"execCommand": "Example.exe",

"cmdLineParameters": "C:\Windows\System32\",

"workingDirectory": "/all"

}

}

'
```

Возвращаемое значение

Код возврата	Описание
200	Операция выполнена успешно.
400	Ошибка ввода параметров.
401	Требуется авторизация.
404	Задача с указанным идентификатором не найдена.
500, 502, 503, 504	Внутренняя ошибка сервера. Повторите запрос позднее.

Если вы хотите изменить параметры созданной задачи, вам требуется создать новый запрос на добавление задачи с нужными параметрами.

Запрос на удаление задачи

Для создания запроса на удаление задачи Kaspersky Anti Targeted Attack Platform используется HTTP-метод DELETE.

Синтаксис команды

```
curl -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X DELETE "
<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию
443>/kata/response_api/v1/<идентификатор external_system_id>/tasks/<идентификатор
task_id>"
```

При успешной обработке запроса задача на запуск программы будет удалена.

Параметры

Параметр	Тип	Описание
`external_system_id`	UUID	Уникальный идентификатор внешней системы, используемый для авторизации в Kaspersky Anti Targeted Attack Platform.
`task_id`	UUID	Уникальный идентификатор задачи.

Пример ввода команды с параметрами

```
curl -k --example.cert --example.key -X DELETE "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-
81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8"
```

Возвращаемое значение

Код возврата	Описание
`200`	Операция выполнена успешно.
`400`	Ошибка ввода параметров.
`401`	Требуется авторизация.
`404`	Задача с указанным идентификатором не найдена.
`500, 502, 503, 504`	Внутренняя ошибка сервера. Повторите запрос позднее.

Источники информации о программе

Страница Kaspersky Anti Targeted Attack Platform на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Anti Targeted Attack Platform вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Anti Targeted Attack Platform содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Anti Targeted Attack Platform в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Anti Targeted Attack Platform в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Anti Targeted Attack Platform, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Получение информации о Kaspersky Endpoint Agent для Linux для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией об операционной системе и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

Kaspersky Endpoint Agent включает аудит системных событий с помощью Linux Audit Daemon и настраивает правила аудита для своей работы. При деинсталляции программы удаляются правила аудита, настроенные программой. При этом работа Linux Audit Daemon не прекращается.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить настройки программы. Для этого может потребоваться выполнение следующих действий:

- Получить расширенную диагностическую информацию.
- Выполнить более тонкую настройку программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить настройки 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 настройки, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав получаемых в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных 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 настроек работы программы способами, не описанными в справке 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.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Anti Targeted Attack Platform, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Anti Targeted Attack Platform.

Kaspersky предоставляет поддержку Kaspersky Anti Targeted Attack Platform в течение жизненного цикла (см. страницу жизненного цикла программ). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;

- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Глоссарий

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.

Backdoor-программа

Программа, которую злоумышленники устанавливают на взломанном компьютере для того, чтобы повторно получать доступ к этому компьютеру.

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.

End User License Agreement

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

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.

IOC

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

Файл, содержащий набор индикаторов IOC, при совпадении с которыми программа считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

Kaspersky Anti Targeted Attack Platform

Решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "*APT*").

Kaspersky Endpoint Agent

Компонент программы. Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации и работающие под управлением операционных систем Microsoft Windows и Linux. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами.

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.

Kaspersky Threat Intelligence Portal

Информационная система "Лаборатории Касперского". Содержит и отображает информацию о репутации файлов и URL-адресов.

KATA

Kaspersky Anti Targeted Attack. Функциональный блок программы Kaspersky Anti Targeted Attack Platform, обнаруживающий угрозы по периметру IT-инфраструктуры предприятия.

KEDR

Kaspersky Endpoint Detection and Response. Функциональный блок программы Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту компьютеров локальной сети организации.

Kerberos-аутентификация

Механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, позволяющий передавать данные через незащищенные сети. Механизм основан на использовании билета (ticket), который выдается пользователю доверенным центром аутентификации.

Keytab-файл

Файл, содержащий пары уникальных имен (principals) для клиентов, которым разрешается Kerberos-аутентификация, и зашифрованные ключи, полученные из пароля пользователя. Keytab-файлы используются в системах, поддерживающих Kerberos, для аутентификации пользователей без ввода пароля.

MIB (Management Information Base)

Виртуальная база данных, используемая для управления объектами, которые передаются по протоколу SNMP.

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.

NTP-сервер

Сервер точного времени, использующий протокол Network Time Protocol.

OpenIOC

Открытый стандарт описания индикаторов компрометации (Indicator of Compromise, IOC), созданный на базе XML и содержащий свыше 500 различных индикаторов компрометации.

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.

Targeted Attack Analyzer

Модуль программы. Выполняет анализ и проверку сетевой активности программного обеспечения, установленного на компьютеры локальной сети организации, на основе правил TAA (IOA). 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.

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.

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.

Вредоносные веб-адреса

Веб-адреса ресурсов, распространяющих вредоносное программное обеспечение.

Дамп

Содержимое рабочей памяти процесса или всей оперативной памяти системы в определенный момент времени.

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.

Имя субъекта-службы (SPN)

Уникальный идентификатор службы в сети для проверки подлинности по протоколу Kerberos.

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.

Мультитенантность

Режим работы, при котором Kaspersky Anti Targeted Attack Platform используется для защиты инфраструктуры нескольких организаций или филиалов одной организации одновременно.

Правила YARA

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.

Правило TAA (IOA)

Один признак подозрительного поведения объекта в IT-инфраструктуре организации, при совпадении с которым Kaspersky Anti Targeted Attack Platform считает событие обнаружением. Правило TAA (IOA) содержит описание признака атаки и рекомендации по противодействию.

Пропускная способность канала связи

Наибольшая возможная в данном канале связи скорость передачи информации.

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)*.

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**.

Тенант

Отдельная организация или филиал организации, которому предоставляется решение Kaspersky Anti Targeted Attack Platform.

Техника MITRE

База знаний MITRE ATT&CK (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.

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.

Фишинговые URL-адреса

URL-адреса ресурсов, занимающихся получением неправомерного доступа к конфиденциальным данным пользователей. Как правило, целью фишинга является кража различных финансовых данных.

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apple, Mac, Macintosh и Safari – товарные знаки Apple Inc.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

Snort является зарегистрированным товарным знаком или товарным знаком Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix – товарный знак Citrix Systems, Inc. и/или дочерних компаний, зарегистрированный в патентном офисе США и других стран.

ESET и ESET NOD32 являются товарными знаками или зарегистрированными товарными знаками ESET spol. s r.o. или соответствующей компании ESET.

Google и Google Chrome – товарные знаки Google LLC.

Intel, Xeon и Core – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

McAfee является товарным знаком или зарегистрированным товарным знаком McAfee LLC или ее дочерних компаний в США и других странах.

Microsoft, Active Directory, Excel, Internet Explorer, Microsoft Edge, PowerPoint, PowerShell, Win32, Windows и Windows Server, Windows Vista, Windows XP являются товарными знаками группы компаний Microsoft.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

Oracle – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

Red Hat, CentOS и Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

Trend Micro является товарным знаком или зарегистрированным товарным знаком Trend Micro Incorporated.

VMware ESXi – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.