kaspersky

Kaspersky Industrial CyberSecurity for Networks

© 2025 АО "Лаборатория Касперского"

Содержание

О Kaspersky Industrial CyberSecurity for Networks
- Комплект поставки
- Аппаратные и программные требования
- Обзор функциональности Kaspersky Industrial CyberSecurity for Networks
  - Инвентаризация активов
  - Расширенный контроль активов
  - Аудит безопасности
  - Мониторинг промышленной сети
  - Расширенное обнаружение угроз и реагирование
  - Интеграция со сторонними системами
- Рекомендации по обеспечению безопасной работы Kaspersky Industrial CyberSecurity for Networks

Что нового

Архитектура программы

Типовые схемы развертывания
- Установка Сервера без внешних сенсоров
- Установка Сервера и внешних сенсоров
- Подключение Kaspersky Industrial CyberSecurity for Networks к промышленной сети через диод данных
- Получение трафика промышленных сетей от компонентов решения Kaspersky SD-WAN

Установка и удаление программы
- Подготовка к установке программы
  - Подготовка к централизованной установке компонентов
  - Подготовка к локальной установке Сервера или сенсора
- Используемые порты для установки и работы компонентов
- Использование скрипта централизованной установки компонентов программы
  - Централизованная установка компонентов программы
  - Команды меню централизованной установки
  - Изменение параметров и централизованная переустановка компонентов программы
  - Централизованная установка компонентов программы в неинтерактивном режиме
  - Усиление защиты компьютеров с установленными компонентами программы
  - Централизованное удаление компонентов программы
- Использование скрипта локальной установки компонентов программы
- Использование скрипта локального удаления компонентов программы
- Установка плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center
- Обновление с использованием скрипта переноса данных
- Установка обновленной версии программы с патчем
- Подготовка программы к работе
- Начальная настройка программы после установки Сервера

Запуск и остановка программы
- Подключение к Серверу через веб-интерфейс
- Завершение сеанса подключения к Серверу через веб-интерфейс
- Подключение к сенсору через веб-интерфейс

Интерфейс программы
- Веб-интерфейс Сервера Kaspersky Industrial CyberSecurity for Networks

О веб-интерфейсе Сервера в режиме начальной настройки программы
О веб-интерфейсе Сервера в основном режиме работы программы
Раздел Мониторинг
Раздел Активы
Раздел Карта сети
Раздел События
Раздел Отчеты
Раздел Контроль процесса
Раздел Разрешающие правила
Раздел Обнаружение вторжений
Раздел Риски
Раздел Аудит безопасности
Раздел Параметры
Веб-интерфейс сенсора Kaspersky Industrial CyberSecurity for Networks
Лицензирование программы
О Лицензионном соглашении
О Политике конфиденциальности
О лицензии
О лицензионном сертификате
О лицензионном ключе
О файле лицензионного ключа
Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс
Просмотр информации о добавленном лицензионном ключе
Удаление лицензионного ключа
Предоставление данных
Директории для хранения данных программы
О журналах
Администрирование Kaspersky Industrial CyberSecurity for Networks
Развертывание узлов
Добавление и удаление сенсоров
Добавление и подключение сенсора с использованием веб-интерфейса сенсора
Добавление и подключение сенсора с помощью файла свертки
Добавление и подключение сенсора автоматически по сети
Создание нового файла свертки для сенсора
Удаление сенсора
Изменение основных параметров узла
Изменение параметров хранения данных программы на узле
Изменение имени узла с установленным компонентом программы
Подключение и настройка внешнего хранилища для файлов дампа трафика
Управление точками мониторинга на узлах
Добавление точки мониторинга
Включение точек мониторинга
Выключение точек мониторинга
Переименование точки мониторинга
Удаление точки мониторинга
Определение Ethernet-порта, связанного с сетевым интерфейсом
Управление технологиями

Включение и выключение технологий
Настройка режимов работы технологий
Управление наследованием технологий
Загрузка трафика, поступившего на точки мониторинга узлов
Контроль состояния Kaspersky Industrial CyberSecurity for Networks
Контроль состояния программы при подключении через веб-интерфейс
Просмотр сообщений программы
Просмотр записей аудита действий пользователей
Просмотр сведений об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах
Отображаемые сведения об узле в области деталей
Отображаемые сведения о сетевом интерфейсе в области деталей
Просмотр статуса сервисов, обеспечивающих работу компонентов программы
Перезагрузка компьютера с установленными компонентами программы
Проверка регистрации событий с помощью тестового сетевого пакета
Контроль целостности модулей программы
Синхронизация времени на узлах Kaspersky Industrial CyberSecurity for Networks с источником времени для устройств промышленной сети
Обновление сертификатов SSL-соединений
Обновление баз и программных модулей
Запуск обновления вручную
Настройка автоматического обновления
Просмотр сведений об установке обновлений
Перезапуск сервисов на узлах после установки обновления библиотеки OpenSSL
Разделение доступа к функциям программы
Об учетных записях пользователей программы
Функции программы, доступные при подключении к Серверу через веб-интерфейс
Просмотр сведений об учетных записях пользователей программы
Создание учетной записи пользователя программы
Изменение роли учетной записи пользователя программы
Удаление учетной записи пользователя программы
Изменение пароля учетной записи
Настройка контроля активов
Методы и режимы контроля активов
Выбор источников данных об уязвимостях
Добавление устройств вручную
Добавление устройства при работе с таблицей устройств
Добавление устройства при работе с топологической картой
Добавление устройства на основе узла неизвестного устройства на карте сетевых взаимодействий
Добавление устройства на основе неуправляемого коммутатора на топологической карте
Объединение устройств
Объединение устройств при работе с таблицей устройств
Объединение устройств при работе с картой сетевых взаимодействий и топологической картой
Удаление устройств
Удаление устройств при работе с таблицей устройств
Удаление устройств при работе с картой сетевых взаимодействий и топологической картой
Изменение статусов устройств вручную
Изменение статусов устройств при работе с таблицей устройств

Изменение статусов устройств при работе с картой сетевых взаимодействий и топологической картой
О распределении устройств по группам
Автоматическая группировка устройств по заданному критерию
Автоматическая группировка устройств по заданному критерию, начиная с верхнего уровня иерархии в дереве групп
Автоматическая группировка устройств в выбранной группе устройств
Распределение устройств по группам вручную
Включение одного устройства в группу
Включение нескольких устройств в группу
Исключение одного устройства из группы
Исключение нескольких устройств из групп
Перемещение узлов и групп в другие группы на карте сетевых взаимодействий
Формирование дерева групп устройств вручную
Добавление группы
Переименование группы
Удаление групп
Перемещение группы
Поиск групп
Обновление дерева
Установка и удаление меток для устройств
Установка меток для одного устройства
Установка меток для нескольких устройств
Удаление меток для одного устройства
Очистка списков меток для нескольких устройств
Изменение сведений об устройстве
Добавление, изменение и удаление пользовательских полей для устройства
Удаление пользователей устройств
Удаление исполняемых файлов устройств
Настройка адресных пространств
О правилах адресных пространств
О подсетях адресных пространств
Добавление адресного пространства
Формирование списка подсетей для контроля активов
Добавление подсети
Изменение параметров подсети
Удаление подсетей
Просмотр сведений об устройствах с IP-адресами из выбранных подсетей
Изменение адресного пространства
Удаление адресного пространства
Настройка контроля процесса
Поддерживаемые устройства и протоколы
Устройства для контроля процесса
Параметры контроля процесса для устройств
Об автоматическом определении параметров контроля процесса для устройств
Добавление параметров контроля процесса для устройства вручную
Изменение параметров контроля процесса для устройства
Выбор отслеживаемых системных команд

Очистка параметров контроля процесса, заданных для устройства
Импорт конфигураций устройств и тегов из внешних проектов
Поддерживаемые типы проектов для импорта
Теги
Об обнаружении неизвестных тегов
Добавление тега вручную
Изменение параметров тега
Добавление тегов в список избранных
Удаление тегов
Правила контроля процесса
Правила с заданными условиями для значений тегов
Правила с Lua-скриптами
Режим обучения правилам контроля процесса
Просмотр таблицы правил контроля процесса
Создание правила контроля процесса с параметрами условий
Создание правила контроля процесса с Lua-скриптом
Изменение параметров правила контроля процесса
Создание, просмотр и изменение глобального Lua-скрипта
Удаление правил контроля процесса
Настройка контроля взаимодействий
Режим обучения для технологий контроля взаимодействий
Режим наблюдения для технологий контроля взаимодействий
Автоматическое формирование правил контроля взаимодействий в режиме обучения
Автоматическое формирование правил контроля взаимодействий при импорте конфигураций из внешних проектов
Просмотр правил контроля взаимодействий в таблице разрешающих правил
Создание правил контроля взаимодействий вручную
Создание правила контроля взаимодействия с изначально пустыми значениями параметров или со значениями из шаблона
Создание правила контроля взаимодействия на основе имеющегося правила
Создание правила на основе события, зарегистрированного по технологии Контроль целостности сети или Контроль системных команд
Изменение параметров правила контроля взаимодействий
Включение и выключение правил контроля взаимодействий
Удаление правил контроля взаимодействий
Настройка обнаружения вторжений
Правила обнаружения вторжений
Дополнительные методы обнаружения вторжений
Включение и выключение наборов правил обнаружения вторжений
Загрузка и замена пользовательских наборов правил обнаружения вторжений
Удаление пользовательских наборов правил обнаружения вторжений
Управление журналами
Управление параметрами хранения журналов в базе данных Сервера
Управление параметрами сохранения трафика в базе данных Сервера
Управление параметрами сохранения файлов дампа трафика
Включение и выключение аудита действий пользователей
Изменение уровней ведения журналов работы процессов
Настройка совместной работы с EPP-приложениями

Сценарий подготовки к получению данных от EPP-приложений
Добавление сервера интеграции
Создание файла свертки для клиентов сервера интеграции
Таблица серверов интеграции
Включение и выключение сервера интеграции
Изменение параметров сервера интеграции
Удаление сервера интеграции
Управление действиями по реагированию в Kaspersky Industrial CyberSecurity for Networks
Запуск действий по реагированию при работе с событиями
Запуск действий по реагированию при работе с устройствами
Запуск действий по реагированию при работе с зарегистрированными действиями по реагированию
Просмотр таблицы действий по реагированию
Удаление действий по реагированию
Управление коннекторами
Об управляемых и неуправляемых коннекторах
Об отправке событий, сообщений программы и записей аудита в сторонние системы
Об автоматическом управлении сетевым доступом устройств с помощью коннекторов типа Cisco Switch
Добавление коннектора
Просмотр таблицы коннекторов
Включение и выключение коннектора
Изменение параметров коннектора
Создание нового файла свертки для коннектора
Удаление коннектора
Добавление и удаление типов коннекторов
Просмотр таблицы типов коннекторов
Добавление типа коннектора
Удаление типа коннектора
Управление заданиями для аудита безопасности
Задания аудита настроек и уязвимостей
Добавление задания аудита настроек и уязвимостей
Изменение задания аудита настроек и уязвимостей
Просмотр таблицы заданий аудита настроек и уязвимостей
Запуск и остановка заданий аудита настроек и уязвимостей вручную
Просмотр общих сведений о выполнении запусков заданий аудита настроек и уязвимостей
Остановка сканирования устройства в задании аудита настроек и уязвимостей
Удаление заданий аудита настроек и уязвимостей
Управление параметрами хранения для запусков заданий аудита настроек и уязвимостей
Задания контроля конфигураций
Добавление задания контроля конфигураций
Изменение задания контроля конфигураций
Просмотр таблицы заданий контроля конфигураций
Запуск и остановка заданий контроля конфигураций вручную
Просмотр общих сведений о выполнении запусков заданий контроля конфигураций
Назначение эталонной конфигурации устройства
Остановка сканирования устройства в задании контроля конфигураций
Удаление заданий контроля конфигураций
Задания активных опросов устройств

Добавление задания активного опроса
Изменение задания активного опроса
Просмотр таблицы заданий активных опросов
Запуск и остановка заданий активных опросов
Просмотр общих сведений о выполнении запусков заданий активных опросов
Просмотр отчета о выполнении задания активного опроса
Удаление заданий активных опросов
Формирование топологической карты
Узлы на топологической карте
Соединения на топологической карте
Просмотр подробных сведений об объектах топологической карты
Добавление узлов на топологическую карту
Добавление соединений для топологической карты вручную
Добавление соединений для выбранного узла с настройкой дополнительных параметров топологии
Добавление соединений для выбранных узлов без настройки дополнительных параметров топологии
Изменение параметров топологии для узла
Переименование узла неуправляемого коммутатора
Удаление объектов топологической карты
Изменение масштаба топологической карты
Позиционирование топологической карты
Закрепление и открепление узлов на топологической карте
Изменение местоположения узлов на топологической карте вручную
Автоматическое распределение узлов на топологической карте
Фильтрация объектов на топологической карте
Сохранение и загрузка параметров отображения топологической карты
Добавление нового вида с сохранением текущих параметров отображения топологической карты
Обновление вида с сохранением текущих параметров отображения топологической карты
Переименование вида топологической карты
Удаление вида топологической карты
Применение на топологической карте параметров, сохраненных в виде
Поиск узлов на топологической карте
Настройка типов событий
Просмотр таблицы типов событий
Изменение параметров системного типа события
Настройка автоматического сохранения трафика для системных типов событий
Настройка передачи событий через коннекторы
Общие переменные для подстановки значений в Kaspersky Industrial CyberSecurity for Networks
Настройка типов рисков
Просмотр таблицы типов рисков
Изменение базовой оценки для типа риска
Управление параметрами хранения рисков
Управление наборами правил для заданий аудита настроек и уязвимостей
Правила аудита настроек и уязвимостей
Просмотр таблицы наборов правил аудита настроек и уязвимостей
Импорт наборов правил аудита настроек и уязвимостей
Изменение наборов правил аудита настроек и уязвимостей
Удаление наборов правил аудита настроек и уязвимостей

- Управление секретами с учетными данными для удаленных подключений
  - Добавление секрета
  - Просмотр таблицы секретов
  - Защита от компрометации секретов при удаленных подключениях к устройствам
  - Изменение параметров секрета
  - Удаление секретов
- Управление отчетами и шаблонами отчетов
  - Дублирование шаблона отчета
  - Изменение шаблона отчета
  - Удаление шаблона отчета
  - Удаление отчета
  - Отмена формирования отчета
  - Управление параметрами хранения файлов отчетов
- Управление политикой безопасности
  - Экспорт политики безопасности в файл
  - Импорт политики безопасности из файла
  - Очистка текущей политики безопасности
  - Преобразование политики безопасности предыдущей версии программы

Использование Kaspersky Industrial CyberSecurity for Networks API

- Обеспечение безопасного взаимодействия при использовании Kaspersky Industrial CyberSecurity for Networks API
- Создание и использование коннекторов для Kaspersky Industrial CyberSecurity for Networks API
- Подписка на уведомления о значениях тега по протоколу WebSocket

Решение типовых задач

- Мониторинг системы в онлайн-режиме
  - Добавление виджета
  - Настройка отображения виджетов
    - Перемещение виджета
    - Изменение размера виджета
    - Изменение параметров отображения данных в виджете
  - Информация в виджете Устройства
  - Информация в виджете События
  - Удаление виджета
- Контроль активов
  - Таблица устройств
  - Просмотр сведений об устройстве
  - Автоматическое добавление и обновление устройств
  - Автоматическое присвоение статусов устройств
  - Дерево групп устройств
  - Контроль чтения и записи проектов ПЛК
  - Контроль оборудования на промышленных устройствах
  - Контроль оборудования на Windows- и Linux-устройствах
  - Контроль пользователей на устройствах
  - Контроль приложений и патчей на устройствах
  - Контроль запусков исполняемых файлов на устройствах
  - Контроль конфигураций устройств
  - Сравнение сохраненных конфигураций устройства
- Работа с картой сетевых взаимодействий

- Узлы на карте сетевых взаимодействий
- Группы устройств на карте сетевых взаимодействий
- Соединения на карте сетевых взаимодействий
- Просмотр подробных сведений об объектах
- Изменение масштаба карты сетевых взаимодействий
- Позиционирование карты сетевых взаимодействий
- Закрепление и открепление узлов и групп
- Изменение местоположения узлов и групп вручную
- Автоматическое распределение узлов и групп
- Поиск узлов на карте сетевых взаимодействий
- Фильтрация объектов на карте сетевых взаимодействий
  - Комплексная фильтрация узлов и соединений
    - Фильтрация с помощью периода на временной шкале
    - Фильтрация по зарегистрированным событиям
  - Фильтрация узлов
    - Фильтрация узлов по статусам устройств
    - Фильтрация узлов по состояниям безопасности устройств
    - Фильтрация узлов по категориям устройств
    - Включение и выключение отображения узлов, связанных с отфильтрованными узлами
  - Фильтрация соединений
    - Фильтрация соединений по значениям оценок критичности соединений
    - Фильтрация соединений по протоколам взаимодействий
    - Фильтрация соединений по уровням модели OSI
  - Сброс параметров фильтрации
- Сохранение и загрузка параметров отображения карты сетевых взаимодействий
  - Добавление нового вида с сохранением текущих параметров отображения карты сетевых взаимодействий
  - Обновление вида с сохранением текущих параметров отображения карты сетевых взаимодействий
  - Переименование вида карты сетевых взаимодействий
  - Удаление вида карты сетевых взаимодействий
  - Применение на карте сетевых взаимодействий параметров, сохраненных в виде
- Загрузка трафика при работе с картой сетевых взаимодействий

Мониторинг сетевых сеансов

- Таблица сетевых сеансов
- Просмотр сведений о сетевом сеансе
- Загрузка трафика сетевых сеансов

Мониторинг событий и инцидентов

- Оценки и уровни критичности событий
- Технологии регистрации событий
- Статусы событий
- Таблица зарегистрированных событий
- Просмотр событий, включенных в инцидент
- Просмотр подробных данных о событии
- Изменение статусов событий
- Просмотр сведений об инцидентах EDR
- Создание разрешающих правил для событий
  - Создание разрешающего правила с изначально пустыми значениями параметров или со значениями из шаблона
  - Создание разрешающего правила на основе имеющегося правила

Создание разрешающего правила на основе зарегистрированного события
Установка меток
Копирование событий в текстовый редактор
Загрузка трафика для событий
Экспорт данных о событиях активности в файл индикаторов компрометации
Создание директории для экспорта событий на сетевой ресурс
Контроль рисков
О рисках категории Уязвимость
Сценарий реализации для процесса непрерывного управления рисками
Просмотр таблицы рисков
Просмотр сведений о риске
Изменение статусов рисков вручную
Просмотр сведений о рисках при работе с таблицей устройств
Контроль технологического процесса
Мониторинг значений параметров технологического процесса
Параметры тегов
Просмотр таблицы тегов
Обнаружение паролей по умолчанию при подключении к устройствам
Получение отчетов
Просмотр таблицы отчетов
Экспорт отчета в файл
Отчеты по шаблонам
Просмотр таблицы шаблонов отчетов
Просмотр сведений о шаблоне отчета
Формирование отчета по шаблону вручную
Отчеты по заданиям аудита настроек и уязвимостей
Формирование отчета о запуске задания вручную
Формирование отчета о сканировании устройства вручную
Обнаружение проблем безопасности в протоколах шифрования
Типовые действия при работе с таблицами данных
Просмотр таблицы данных
Настройка отображения и порядка столбцов
Фильтрация по стандартным периодам времени
Фильтрация по заданному периоду времени
Фильтрация по столбцам
Поиск в таблице
Сброс заданных параметров фильтрации и поиска
Сортировка таблицы
Выбор элементов в таблице данных
Переходы к связанным элементам в других разделах веб-интерфейса
Экспорт данных из таблицы в файл
Обновление таблицы данных
Управление программой через Kaspersky Security Center
Включение и настройка функциональности взаимодействия с Kaspersky Security Center
Добавление лицензионного ключа в Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center
Получение обновлений с Сервера администрирования Kaspersky Security Center
Мониторинг событий через Kaspersky Security Center

Типы событий в Kaspersky Security Center для событий Kaspersky Industrial CyberSecurity for Networks
Соответствие уровней важности событий в Kaspersky Security Center
Контроль состояния безопасности АСУ ТП: Kaspersky Security Center и SCADA
Подключение к компьютеру Сервера из Kaspersky Security Center
Централизованный контроль систем с Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console
О веб-плагине управления Kaspersky Industrial CyberSecurity for Networks
Сценарий подготовки к использованию технологии единого входа (SSO)
Предоставление пользователям Kaspersky Security Center прав доступа, соответствующих ролям пользователей в Kaspersky Industrial CyberSecurity for Networks
Веб-виджеты для мониторинга систем и Серверов Kaspersky Industrial CyberSecurity for Networks
Веб-виджет Статусы KICS for Networks
Веб-виджет Критические события KICS for Networks
Веб-виджет Устройства, требующие внимания в KICS for Networks
Веб-виджет Актуальные события KICS for Networks
Веб-виджет Карта размещения KICS for Networks
Веб-виджет Информация о Серверах KICS for Networks
Поиск устройств и событий по базам данных Серверов Kaspersky Industrial CyberSecurity for Networks
Настройка параметров для поиска устройств
Настройка параметров для поиска событий
Просмотр таблицы с результатами поискового запроса
Размещение компонентов Kaspersky Industrial CyberSecurity for Networks на картах
Формирование списка подразделений для общей карты
Добавление подразделения
Переименование подразделения
Удаление подразделения
Замена фонового изображения для карты
Формирование списков Серверов в подразделениях
Добавление Сервера в подразделение
Удаление Сервера из подразделения
Управление размещением объектов на картах
Исключение Сервера из мониторинга в Web Console
Просмотр информации о Серверах на картах
Устранение неисправностей
Не выполняется установка программы из-за недоступного репозитория для DNF
Не выполняется установка компонента программы на выбранном узле
Обнаружены проблемы в работе программы
Новое сообщение программы
Закончилось свободное пространство на жестком диске
При включении точки мониторинга возникает ошибка
Отсутствует трафик на точке мониторинга
Не загружается трафик для событий или инцидентов
Профилактические и пусконаладочные работы на АСУ ТП
Непредвиденная перезагрузка системы
Недоступна функциональность коннекторов и удаленных подключений после изменения или добавления IP-адреса Сервера
Не выполняется загрузка обновлений с Сервера администрирования Kaspersky Security Center

После переустановки Сервера администрирования Kaspersky Security Center не выполняется синхронизация Агента администрирования
Не выполняется подключение к Серверу через веб-интерфейс
При подключении к Серверу браузер выводит предупреждение о сертификате
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Получение информации для технической поддержки
Источники информации о программе
Приложения
Настройка синхронизации времени по протоколам NTP и PTP
Настройка синхронизации времени по протоколу NTP в CentOS
Настройка синхронизации времени по протоколу PTP в CentOS
Поддерживаемые типы кадров ASDU в протоколах стандартов IEC 60870-5-104 и IEC 60870-5-101
Загрузка, обработка и контроль конфигураций устройств и тегов с поддержкой протоколов стандарта IEC 61850
Отправка событий Kaspersky Industrial CyberSecurity for Networks в SIEM-системы
Проверка передачи событий на примере системы HP ArcSight
Формат сообщений, посылаемых в SIEM-систему
Особенности подключения узлов Kaspersky Industrial CyberSecurity for Networks в качестве шлюзов соединений в Kaspersky Security Center
Файлы для импорта проекта универсального формата
Файл описания устройств: devices.csv
Файл описания соединений: connections.csv
Файл описания переменных и тегов: variables.csv
Файл описания перечислений: enums.csv
Файл описания наборов данных (группы тегов): datasets.csv
Файл описания отчетов протокола MMS: iec61850_mms_reports.csv
Системные типы событий в Kaspersky Industrial CyberSecurity for Networks
Системные типы событий по технологии Контроль технологического процесса
Системные типы событий по технологии Контроль системных команд
Системные типы событий по технологии Контроль целостности сети
Системные типы событий по технологии Обнаружение вторжений
Системные типы событий по технологии Контроль активов
Системные типы событий по технологии Внешние системы
Системные типы событий по технологии Защита конечных устройств
Категории системных команд в Kaspersky Industrial CyberSecurity for Networks
Примеры использования адресных пространств в Kaspersky Industrial CyberSecurity for Networks
Поддерживаемые протоколы общего применения
Особенности получения типов конфигураций устройств с помощью заданий контроля конфигураций
Конфигурации устройств под управлением операционных систем семейства Windows
Конфигурации устройств под управлением операционных систем семейства Linux
Конфигурации устройств, относящихся к сетевому оборудованию
Конфигурации ПЛК и других устройств, получаемые с использованием коннекторов типа Active poll
Используемые команды для сканирований Linux-устройств в заданиях аудита безопасности
Операционные системы устройств, поддерживаемые для проведения активных опросов устройств
Обнаружение атрибутов и типовых взаимодействий устройств в Kaspersky Industrial CyberSecurity for Networks
Настройка зеркалирования портов для Kaspersky Industrial CyberSecurity for Networks

Настройка зеркалирования портов для коммутаторов серий Cisco Access и Distribution
Настройка зеркалирования портов для коммутаторов серии Cisco Small Business™
Настройка зеркалирования портов для промышленных Ethernet-коммутаторов Hirschmann
Настройка зеркалирования портов для коммутаторов Siemens серии SCALANCE
Настройка зеркалирования портов для коммутаторов Siemens серии RUGGEDCOM i800, i801, i802, i803
Настройка узла Kaspersky Industrial CyberSecurity for Networks для получения трафика по технологии ERSPAN
Глоссарий
ARP-спуфинг
CVE
Endpoint Protection Platform (EPP)
EPP-приложение
IOC
IOC-файл
SCADA
SIEM
Адресное пространство (АП)
АСУ ТП
Внешние системы
Выделенная сеть Kaspersky Industrial CyberSecurity
Защита конечных устройств
Интеллектуальное электронное устройство (IED)
Инцидент
Карта сетевых взаимодействий
Контроль активов
Контроль системных команд
Контроль технологического процесса
Контроль целостности сети
Неуправляемый коммутатор
Неуправляемый коннектор
Обнаружение вторжений
Политика безопасности
Правило контроля взаимодействий
Правило контроля процесса
Правило корреляции событий
Правило обнаружения вторжений
Программируемый логический контроллер (ПЛК)
Проект ПЛК
Промышленная сеть
Риск
Роль учетной записи
Сенсор Kaspersky Industrial CyberSecurity for Networks
Сервер Kaspersky Industrial CyberSecurity for Networks
Системная команда
Событие
Соединение на карте сети
Тег
Технология единого входа (SSO)

- Тип риска
- Тип события
- Топологическая карта
- Точка мониторинга
- Узел
- Управляемый коннектор
- Устройство
- Уязвимость устройства

Информация о стороннем коде

Уведомления о товарных знаках

О Kaspersky Industrial CyberSecurity for Networks

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

Kaspersky Industrial CyberSecurity for Networks выполняет следующие функции:

- Контролирует активы предприятия, представленные устройствами промышленной сети. Обнаруживает активность устройств и сведения об устройствах на основании данных, полученных при анализе сетевых пакетов и/или от приложений "Лаборатории Касперского", которые выполняют функции защиты рабочих станций и серверов.

- Контролирует устройства и их взаимодействия с учетом принадлежности их MAC- или IP-адресов к адресным пространствам.

- Проверяет взаимодействия между устройствами промышленной сети на соответствие заданным правилам контроля взаимодействий. Формирование правил контроля взаимодействий может выполняться автоматически в режиме обучения.

- Отображает взаимодействия между устройствами промышленной сети в виде карты сетевых взаимодействий. При отображении объекты визуально выделяются по различным признакам (например, объекты, требующие внимания).

- Отображает схему физических подключений устройств в промышленной сети в виде топологической карты. При отображении объекты визуально выделяются по различным признакам (например, по статусу объектов).

- Обнаруживает риски по результатам анализа трафика и по полученным сведениям об устройствах.

- Позволяет проводить аудит безопасности устройств с использованием заданий аудита настроек и уязвимостей, заданий контроля конфигураций и заданий активных опросов.

- Извлекает из сетевых пакетов значения параметров технологического процесса, управляемого автоматизированной системой управления технологическим процессом (далее также "АСУ ТП"), и проверяет допустимость этих значений по заданным правилам контроля процесса. Формирование правил контроля процесса может выполняться автоматически в режиме обучения.

- Обнаруживает в трафике системные команды, переданные или полученные устройствами, которые участвуют в автоматизации технологического процесса. Оповещает об обнаруженных неразрешенных системных командах и ситуациях, которые могут быть признаками нарушения безопасности промышленной сети.

- Контролирует операции чтения и записи проектов для программируемых логических контроллеров по данным из трафика промышленной сети.

- Анализирует трафик промышленной сети на наличие признаков атак, не оказывая влияния на промышленную сеть и не привлекая внимания потенциального нарушителя. Обнаруживает признаки атак с помощью заданных правил обнаружения вторжений и встроенных алгоритмов проверки аномалий в сетевых пакетах.

- Регистрирует сетевые сеансы, создаваемые устройствами для соединений с другими устройствами.

- Регистрирует события и передает сведения о них в сторонние системы, а также в Kaspersky Security Center.

- Анализирует зарегистрированные события и при обнаружении определенных последовательностей событий регистрирует инциденты по встроенным правилам корреляции. Инциденты группируют события, имеющие некоторые общие признаки или относящиеся к одному процессу.

- Сохраняет в базе данных трафик, относящийся к зарегистрированным событиям. Трафик может сохраняться автоматически (если для событий включено автоматическое сохранение трафика) или по запросу на загрузку трафика.

- Получает, обрабатывает и предоставляет данные от приложений, входящих в состав системы защиты конечных устройств (англ. Endpoint Protection Platform, EPP). С помощью EPP-приложений предоставляет возможность запуска действий по реагированию на устройствах.

- По данным, поступающим из различных источников, контролирует на устройствах списки оборудования, пользователей, приложений, патчей, исполняемых файлов и других компонентов конфигураций. При изменении этих списков Kaspersky Industrial CyberSecurity for Networks регистрирует соответствующие события.

- Предоставляет отчеты со сведениями о состоянии устройств и безопасности системы, а также о результатах аудита безопасности.

- Предоставляет возможность загрузки трафика из хранилищ с файлами дампа трафика. Для загрузки может использоваться как внутреннее хранилище узла (созданное автоматически), так и внешнее хранилище, если оно подключено на узле.

- Предоставляет возможности работы через графический интерфейс пользователя и через интерфейс прикладного программирования (API).

- Предоставляет данные для централизованного контроля систем с Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console.

Комплект поставки

В комплект поставки Kaspersky Industrial CyberSecurity for Networks 4.2 входят следующие файлы:

- Архив, содержащий все файлы комплекта поставки программы: kics4net-release_<номер версии программы>.tar.gz. В архиве упакованы следующие файлы:
  - ZIP-архивы с описаниями типов коннекторов, встроенных в программу (размещены в упакованной директории connector-types);
  - скрипты и пакеты для установки, проверки и удаления компонентов программы (размещены в упакованной директории linux-centos);
  - пакеты для установки плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center и веб-плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center Web Console (размещены в упакованной директории sc_plugin);
  - архивы с документацией с описаниями запросов и спецификациями для Kaspersky Industrial CyberSecurity for Networks API (размещены в упакованной директории sdk);
  - файлы с текстом Лицензионного соглашения на поддерживаемых языках локализации: русский, английский;
  - файлы с текстом Политики конфиденциальности на поддерживаемых языках локализации: русский, английский;
  - файлы с информацией о версии (Release Notes) на поддерживаемых языках локализации: русский, английский.
- Копии файлов, содержащихся в архиве kics4net-release_<номер версии программы>.tar.gz:
  - пакеты для установки плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center и веб-плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center Web Console;
  - файлы с текстом Лицензионного соглашения на поддерживаемых языках локализации: русский, английский;
  - файлы с текстом Политики конфиденциальности на поддерживаемых языках локализации: русский, английский;
  - файлы с информацией о версии (Release Notes) на поддерживаемых языках локализации: русский, английский.

В комплект поставки Kaspersky Industrial CyberSecurity for Networks 4.2.1 входят следующие файлы:

- Архив, содержащий все файлы комплекта поставки программы: kics4net-release_<номер версии программы>.tar.gz. В архиве упакованы следующие файлы:
  - ZIP-архивы с описаниями типов коннекторов, встроенных в программу (размещены в упакованной директории connector-types);
  - скрипты и пакеты для установки, проверки и удаления компонентов программы (размещены в упакованной директории linux-centos);
  - пакеты для установки плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center и веб-плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center Web Console (размещены в упакованной директории sc_plugin);
  - архивы с документацией с описаниями запросов и спецификациями для Kaspersky Industrial CyberSecurity for Networks API (размещены в упакованной директории sdk);
  - файлы с текстом Лицензионного соглашения на поддерживаемых языках локализации: русский, английский, упрощенный китайский;
  - файлы с текстом Политики конфиденциальности на поддерживаемых языках локализации: русский, английский, упрощенный китайский;
  - файлы с информацией о версии (Release Notes) на поддерживаемых языках локализации: русский, английский, упрощенный китайский.
- Копии файлов, содержащихся в архиве kics4net-release_<номер версии программы>.tar.gz:
  - пакеты для установки плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center и веб-плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center Web Console;
  - файлы с текстом Лицензионного соглашения на поддерживаемых языках локализации: русский, английский, упрощенный китайский;
  - файлы с текстом Политики конфиденциальности на поддерживаемых языках локализации: русский, английский, упрощенный китайский;
  - файлы с информацией о версии (Release Notes) на поддерживаемых языках локализации: русский, английский, упрощенный китайский.
- Дополнительные файлы, указанные в формуляре на программу.

Аппаратные и программные требования

Аппаратные требования

Kaspersky Industrial CyberSecurity for Networks имеет следующие минимальные требования к аппаратному обеспечению компьютеров для установки компонентов программы:

- Компьютер, который будет выполнять функции Сервера:
  - центральный процессор: Intel® Core™ i7 или аналог (рекомендуются конфигурации с максимальной частотой для одного ядра);
  - объем оперативной памяти: 32 ГБ;
  - объем свободного пространства на жестком диске: 500 ГБ (рекомендуется использовать SSD).
- Компьютер, который будет выполнять функции сенсора:
  - центральный процессор: Intel Core i5 / i7 или аналог (рекомендуются конфигурации с максимальным количеством ядер);
  - объем оперативной памяти: 8 ГБ и дополнительно 4 ГБ при использовании точек мониторинга на этом компьютере (для любого количества точек мониторинга);
  - объем свободного пространства на жестком диске: 250 ГБ (рекомендуется использовать SSD).

Рекомендуется использовать распределенную схему развертывания с Сервером и внешними сенсорами, причем настраивать поступление трафика промышленной сети рекомендуется на точки мониторинга сенсоров. Сенсоры обеспечивают снижение нагрузки на Сервер программы за счет предварительной обработки трафика и хранения данных.

Для обеспечения стабильной производительности весь объём трафика промышленной сети необходимо распределять между узлами Сервера и сенсоров. Рекомендуемые предельные значения скорости входящего трафика составляют 500 Мбит/с для узла Сервера и 250 Мбит/с для узла сенсора.

Избегайте подачи дублированного трафика на узел Сервера или сенсора и правильно настраивайте сетевое оборудование для передачи копии трафика (примеры настройки зеркалирования портов для некоторых моделей коммутаторов см. в Приложении). При обнаружении дублированного трафика программа автоматически отбрасывает дублированные сетевые пакеты, что приводит к повышению нагрузки на аппаратные ресурсы компьютера и в некоторых случаях может приводить к замедлению обработки трафика.

При использовании сенсоров пропускная способность выделенной сети Kaspersky Industrial CyberSecurity между Сервером и каждым сенсором должна быть не менее 1 Мбит/с без учета скорости входящего трафика на точки мониторинга сенсора. С учетом скорости входящего трафика на точки мониторинга, пропускная способность канала между сенсором и Сервером должна быть увеличена на величину не менее 50% от суммарного входящего трафика на сенсор (по всем точкам мониторинга сенсора).

Пример:
На сенсоре используются две точки мониторинга, на одну из которых поступает трафик 100 Мбит/с, на другую 200 Мбит/с. В этом случае пропускная способность канала между сенсором и Сервером должна быть не менее 151 Мбит/с (1+(200+100)/2=151).

Программные требования

Kaspersky Industrial CyberSecurity for Networks имеет следующие требования к программному обеспечению компьютеров для установки компонентов программы:

- Операционная система CentOS Stream 9.

  При установке операционной системы рекомендуется выделить под системный (корневой) раздел все место на жестком диске за вычетом минимально необходимого места для boot- и swap-разделов. Также для повышения производительности работы программного обеспечения вы можете монтировать директорию /var/ на высокоскоростной жесткий диск (при наличии дополнительного дискового устройства, например SSD-диска). При этом монтировать директорию /var/ на другой диск требуется полностью. Не допускается монтировать на разные диски поддиректории, вложенные в директорию /var/ (в частности, директорию /var/opt/).

- Операционная система одной и той же версии должна быть установлена на всех компьютерах, на которых устанавливаются компоненты программы.

- Для установки компонентов программы в операционной системе CentOS должны быть выполнены следующие условия:

  - Установлен пакет для синхронизации времени chrony версии 3.1 и выше.

    Вы можете установить пакет для синхронизации времени chrony, используя следующие команды в консоли операционной системы:

    ```
    sudo dnf install chrony
    sudo systemctl enable chronyd
    sudo systemctl start chronyd
    ```

  - Выключена система принудительного контроля доступа SELinux. Для этого:

    1. Откройте файл конфигурации системы. Для этого введите команду:

       ```
       sudo mcedit /etc/selinux/config
       ```

    2. Задайте значение параметра:

       ```
       SELINUX=disabled
       ```

    3. Сохраните и закройте файл конфигурации.

    4. Перезагрузите компьютер.

  - Установлен пакет dnf-utils.

    Вы можете установить пакет dnf-utils, используя следующую команду в консоли операционной системы:

    ```
    sudo dnf install dnf-utils
    ```

  - Установлен пакет compat-openssl.

    Вы можете установить пакет compat-openssl, используя следующую команду в консоли операционной системы:

    ```
    sudo dnf install compat-openssl11
    ```

  - Установлен пакет lttng-ust с библиотекой LTTng версии не выше 2.12.

    В операционной системе CentOS Stream 9 вы можете установить пакет lttng-ust с библиотекой LTTng нужной версии, используя следующую команду в консоли операционной системы:

    ```
    sudo dnf install lttng-ust.x86_64
    ```

- Для работы компонентов программы на компьютере, который будет выполнять функции Сервера, в операционной системе CentOS дополнительно должны быть выполнены следующие условия:

  - Установлен интерпретатор языка Python версии 3.9 и выше, а также пакеты для работы коннекторов и скриптов преобразования данных (если коннекторы будут работать на других компьютерах, пакеты также требуется установить на эти компьютеры).

    Вы можете установить пакеты для работы коннекторов и скриптов преобразования данных, используя следующие команды в консоли операционной системы:

    ```
    sudo dnf install epel-release
    sudo dnf install python3-psycopg2 python3-cryptography python3-paramiko
    ```

  - Установлен почтовый сервер (Mail Transfer Agent – MTA) для отправки сообщений электронной почты через коннектор электронной почты, а также для отправки отчетов по электронной почте (например, Postfix).

Вы можете установить почтовый сервер Postfix, используя следующие команды в консоли операционной системы:

```
sudo dnf -y install postfix
sudo systemctl start postfix
sudo systemctl enable postfix
```

- Установлен интерпретатор языка Perl версии 5.10 и выше (если устанавливается Агент администрирования Kaspersky Security Center).

Для установки компонентов программы рекомендуется использовать отдельные компьютеры, на которых установлено только программное обеспечение из состава операционной системы. Если на компьютерах установлено прикладное программное обеспечение сторонних производителей, производительность компонентов Kaspersky Industrial CyberSecurity for Networks может быть снижена.

Для подключения через веб-интерфейс могут использоваться следующие браузеры:

- Google™ Chrome™ версии 115 и выше.
- Mozilla™ Firefox™ версии 115 и выше.
- Microsoft® Edge® версии 115 и выше.

Поддерживаемые версии Kaspersky Security Center

Программа Kaspersky Industrial CyberSecurity for Networks совместима с Kaspersky Security Center 14.2 и Kaspersky Security Center Linux версий 15 и 15.1.

Интеграция с EPP-приложениями

В программе Kaspersky Industrial CyberSecurity for Networks поддерживается работа в режиме интеграции со следующими приложениями, выполняющими функции защиты рабочих станций и серверов (EPP-приложения):

- Kaspersky Industrial CyberSecurity for Nodes версий 3.1, 3.2 и 4.0.

  Взаимодействие Kaspersky Industrial CyberSecurity for Networks с этим приложением обеспечивает программа Kaspersky Endpoint Agent, установленная на устройствах. Поддерживаемые версии программы Kaspersky Endpoint Agent: 3.15, 3.16 и 4.0.

- Kaspersky Industrial CyberSecurity for Linux Nodes версий 1.3 и 1.5.

  Взаимодействие Kaspersky Industrial CyberSecurity for Networks с этим приложением обеспечивают программные модули, встроенные в Kaspersky Industrial CyberSecurity for Linux Nodes.

Все возможности режима интеграции доступны при использовании Kaspersky Industrial CyberSecurity for Nodes версии 4.0 с программой Kaspersky Endpoint Agent версии 4.0. При использовании других версий указанного программного обеспечения недоступны возможности получения данных от EPP-приложений для следующей функциональности Kaspersky Industrial CyberSecurity for Networks:

- Получение сведений о цепочках развития угроз для инцидентов EDR – если используется Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.3 или 1.5.
- Управление действиями по реагированию – если используется Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.3 или 1.5.
- Контроль оборудования на Linux®-устройствах – если используется Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.3.
- Контроль конфигураций устройств – если используется Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.3 либо программа Kaspersky Endpoint Agent версии 3.15 или 3.16.
- Контроль пользователей на устройствах – если используется Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.3 либо программа Kaspersky Endpoint Agent версии 3.15 или 3.16.
- Контроль приложений на устройствах – если используется Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.3 либо программа Kaspersky Endpoint Agent версии 3.15 или 3.16.
- Контроль патчей на устройствах – если используется Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.3 или 1.5 либо программа Kaspersky Endpoint Agent версии 3.15 или 3.16.
- Контроль запуска исполняемых файлов на устройствах – если используется Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.3 либо программа Kaspersky Endpoint Agent версии 3.15 или 3.16.

Интеграция с решением Kaspersky SD-WAN

В программе Kaspersky Industrial CyberSecurity for Networks поддерживается работа в режиме интеграции с решением Kaspersky SD-WAN версии 2.2 и выше.

Обзор функциональности Kaspersky Industrial CyberSecurity for Networks

Выполнение функций программы обеспечивают соответствующие части функциональности Kaspersky Industrial CyberSecurity for Networks. Вы можете использовать функциональность выборочно, в зависимости от конкретных условий и оснащенности вашей системы. Однако наиболее эффективная защита с помощью Kaspersky Industrial CyberSecurity for Networks достигается при использовании и правильной настройке всей предусмотренной функциональности.

Части функциональности Kaspersky Industrial CyberSecurity for Networks условно можно разделить на группы, обеспечивающие целевое применение функций программы.

Инвентаризация активов

Инвентаризацию активов промышленной сети обеспечивают следующие части функциональности Kaspersky Industrial CyberSecurity for Networks:

- Контроль активов с формированием таблицы устройств по сведениям об устройствах из трафика, поступающего через точки мониторинга.
- Контроль рисков по данным из трафика (в том числе обнаружение уязвимостей устройств по сведениям об устройствах).
- Проведение активных опросов устройств для получения наиболее точной и полной информации об устройствах и их конфигурациях с помощью методов активных опросов устройств как по протоколам прикладного уровня, так и по протоколам общего применения.
- Мониторинг в онлайн-режиме с отображением данных о текущем состоянии системы в различных виджетах.
- Карта сетевых взаимодействий по данным из трафика, поступающего через точки мониторинга, с возможностью просматривать сведения о взаимодействиях устройств в различные периоды времени.
- Топологическая карта, на которой представлены устройства из таблицы устройств и соединения, добавленные по результатам активных опросов или вручную.
- Мониторинг сетевых сеансов с формированием таблицы сетевых сеансов.
- Сохранение файлов дампа трафика с возможностью последующей загрузки трафика в файлы (например, можно загружать трафик сетевых сеансов).

Расширенный контроль активов

Расширенный контроль активов выполняется по данным, запрос и получение которых обеспечивают следующие части функциональности Kaspersky Industrial CyberSecurity for Networks:

- Контроль активов с обогащением сведений об устройствах и с добавлением новых устройств по данным, поступающим от EPP-приложений.
- Контроль пользователей на устройствах по полученным сведениям об учетных записях, зарегистрированных в операционных системах устройств.
- Контроль приложений и патчей на устройствах по полученным сведениям о программном обеспечении, установленном и зарегистрированном в операционных системах устройств.
- Контроль исполняемых файлов на устройствах по полученным сведениям о запусках исполняемых файлов на устройствах.
- Совместная работа с EPP-приложениями для регистрации событий защиты рабочих станций и серверов, для отображения взаимодействий устройств с установленными EPP-приложениями и для получения других сведений о сетевой активности.

Аудит безопасности

Аудит безопасности устройств выполняется по данным, запрос и получение которых обеспечивают следующие части функциональности Kaspersky Industrial CyberSecurity for Networks:

- Проведение аудита настроек и уязвимостей для оценки соответствия параметров устройств стандартам безопасности и для поиска уязвимостей.
- Контроль конфигураций для получения и сохранения детальной информации о конфигурациях устройств, а также для сравнения изменений в конфигурациях.
- Проведение активных опросов устройств для целей аудита безопасности (в том числе для получения сведений о рисках на устройствах).
- Контроль рисков по результатам выполнения заданий аудита настроек и уязвимостей и заданий активных опросов.

Мониторинг промышленной сети

Мониторинг промышленной сети обеспечивают следующие части функциональности Kaspersky Industrial CyberSecurity for Networks:

- Обнаружение вторжений с использованием правил обнаружения вторжений, встроенных алгоритмов проверки сетевых пакетов для обнаружения аномалий, а также правил анализа статистики для обнаружения атак и нежелательной сетевой активности.
- Контроль взаимодействий для обнаружения неразрешенных сетевых взаимодействий, не удовлетворяющих правилам по технологии Контроль целостности сети.
- Контроль технологического процесса (далее также "контроль процесса") для отслеживания в трафике значений параметров технологического процесса по правилам контроля процесса, а также для отслеживания передаваемых системных команд (системные команды, разрешенные для передачи, можно указать в правилах контроля взаимодействий по технологии Контроль системных команд).
- Мониторинг событий, регистрируемых по различным технологиям (в том числе на основе описаний техник атак из базы знаний MITRE ATT&CK), с последующей регистрацией инцидентов по правилам корреляции и инцидентов Endpoint Detection and Response.

Для углубленного анализа трафика промышленной сети и раннего обнаружения аномальных ситуаций вы можете использовать функциональность коннекторов для совместной работы с программным продуктом Kaspersky Machine Learning for Anomaly Detection.

Расширенное обнаружение угроз и реагирование

Расширенное обнаружение угроз и реагирование обеспечивают следующие части функциональности Kaspersky Industrial CyberSecurity for Networks:

- Отображение сведений об инцидентах EDR при мониторинге событий для определения статуса обработки обнаружений и анализа развития угроз (сведения отображаются в виде графа событий активности и в табличном виде).
- Обогащение событий сведениями о приложениях, при работе которых возникли условия для регистрации событий, сведениями о пользователях, запускавших приложения, и другими сведениями.
- Управление действиями по реагированию на устройствах с установленным программным компонентом Endpoint Agent – в зависимости от условий запуска действий вы можете включать сетевую изоляцию устройства, запрещать запуск исполняемых файлов и скриптов, помещать файлы на карантин.
- Автоматическая блокировка сетевого доступа неразрешенных устройств с помощью коннекторов для сетевых коммутаторов.

Интеграция со сторонними системами

Вы можете настроить Kaspersky Industrial CyberSecurity for Networks для совместной работы со следующими программами и решениями "Лаборатории Касперского":

- Kaspersky Security Center.
- EPP-приложения, представленные Kaspersky Industrial CyberSecurity for Nodes или Kaspersky Industrial CyberSecurity for Linux Nodes.
- Kaspersky SD-WAN.

Кроме того, с использованием функциональности коннекторов и Kaspersky Industrial CyberSecurity for Networks API вы можете реализовать совместную работу с многими другими программами и решениями, в том числе со сторонними продуктами. Например, совместная работа поддерживается со следующими программными продуктами:

- Kaspersky Unified Monitoring and Analysis Platform.
- Kaspersky Machine Learning for Anomaly Detection.
- Сетевые коммутаторы Cisco™.

Если вы хотите реализовать совместную работу Kaspersky Industrial CyberSecurity for Networks с программными продуктами, взаимодействие с которыми не поддерживается функциональностью коннекторов встроенных типов, вы можете добавлять типы коннекторов в программу.

Рекомендации по обеспечению безопасной работы Kaspersky Industrial CyberSecurity for Networks

Чтобы обеспечить безопасную работу программы на предприятии, рекомендуется усилить защиту компьютеров, на которых установлены Сервер и сенсоры Kaspersky Industrial CyberSecurity for Networks, после установки Kaspersky Industrial CyberSecurity for Networks. Требуемый уровень защиты для безопасной работы программы реализуется операционной системой и ее средствами защиты. Для поддержания безопасного состояния рекомендуется регулярно устанавливать обновления баз и программных модулей Kaspersky Industrial CyberSecurity for Networks и обновления безопасности операционной системы.

К оборудованию, на котором работает программа, рекомендуется ограничить физический доступ, чтобы предотвратить следующие возможные последствия:

- несанкционированное выключение оборудования (или его отключение от сети);
- подключение технических средств для перехвата передаваемых данных;
- кража жестких дисков с данными;
- уничтожение или подмена данных на жестких дисках с использованием другого оборудования.

При внедрении Kaspersky Industrial CyberSecurity for Networks рекомендуются следующие меры:

- Ограничение удаленного и локального доступа к компьютерам с установленными компонентами Kaspersky Industrial CyberSecurity for Networks.

  После каждого использования скрипта централизованной установки компонентов программы (в том числе для централизованного удаления или для усиления защиты компьютеров) в целях безопасности требуется закрыть доступ к компьютерам по протоколу SSH. Вы можете закрыть доступ, используя команду в консоли операционной системы компьютера `sudo systemctl disable --now sshd`. Для последующего возобновления доступа по протоколу SSH (если возникнет необходимость в повторном использовании скрипта централизованной установки компонентов программы) вы можете использовать команду `sudo systemctl enable --now sshd`.

- Регулярная проверка и обновление парольных политик для действующих учетных записей в операционных системах на компьютерах с установленными компонентами программы. Парольные политики должны соответствовать рекомендациям по обеспечению требуемого уровня безопасности операционной системы.

- Обеспечение доступа к интерфейсам программы исключительно для персонала, обладающего полномочиями для установки и настройки программы, а также для пользователей, которые решают типовые задачи с помощью программы (операторы).

- Контроль физического доступа к оборудованию, на котором работает программа, и к используемому сетевому оборудованию с помощью технических средств или службы охраны.
- Мониторинг контролируемых помещений с помощью средств охранной сигнализации и видеонаблюдения.

При передаче событий программы в сторонние системы (кроме Kaspersky Security Center), безопасность передачи данных не обеспечивается программой. Рекомендуется обеспечить безопасность передачи данных другими средствами.

Для использования средств управления работой программы дополнительно рекомендуются следующие меры по обеспечению информационной безопасности интранет-системы:

- Обеспечение защиты трафика внутри интранет-системы.
- Обеспечение защиты подключений к внешним сетям.
- Использование цифровых сертификатов, изданных доверенными центрами сертификации.
- Использование учетных данных, удовлетворяющих требованиям к именам и паролям учетных записей пользователей программы.
- Обеспечение конфиденциальности и уникальности паролей.

  При угрозе компрометации пароля пользователь программы должен своевременно изменить свой пароль.
- Настроенная синхронизация времени на узлах Kaspersky Industrial CyberSecurity for Networks.
- Завершение сеанса подключения через веб-интерфейс перед окончанием работы с браузером.

  Для принудительного завершения сеанса подключения нужно использовать пункт **Выход** в меню пользователя.

Что нового

В Kaspersky Industrial CyberSecurity for Networks 4.2 появились следующие возможности и доработки:

- Добавлена функциональность контроля конфигураций устройств – по результатам выполнения заданий контроля конфигураций вы можете просматривать сведения о конфигурациях и сравнивать сохраненные конфигурации. Для контроля поддерживаются типы конфигураций операционных систем Windows и Linux, устройств категории ПЛК и сетевых устройств. Типы конфигураций предусматривают получение соответствующих компонентов конфигурации устройств (например, для сетевых устройств предусмотрено получение таблиц маршрутизации и других компонентов). Обработка полученных конфигураций в программе выполняется в соответствии с выбранным режимом в задании: программа может только обновлять конфигурации, архивировать все уникальные конфигурации или сравнивать полученные конфигурации с эталонными.

- Функциональность проведения активных опросов доработана для более удобного использования – настройка проведения активных опросов устройств выполняется с помощью заданий для аудита безопасности (задания активных опросов или задания контроля конфигураций), предоставляются возможности запуска заданий вручную и автоматически по расписанию.

- Расширена функциональность контроля активов в части контроля оборудования на промышленных устройствах – с помощью коннекторов типа **Active poll**, используемых в заданиях контроля конфигураций или в заданиях активных опросов, вы можете получать сведения об оборудовании и конфигурациях устройств Siemens SIMATIC серий S7-300, S7-400 и Schneider Electric серии Modicon: M580, M340 (в том числе сведения о модулях в слотах, о проектах ПЛК, содержимое журналов и другие сведения).

- Расширена функциональность контроля активов в части получения сведений об объектах в операционных системах устройств – вы можете использовать части функциональности, которые обеспечивают контроль пользователей, контроль приложений и патчей, контроль запусков исполняемых файлов на устройствах.

- Добавлена поддержка событий срабатывания Sigma-правил от программных компонентов Endpoint Agent – при срабатывании Sigma-правил в EPP-приложениях сведения об этом регистрируются в Kaspersky Industrial CyberSecurity for Networks в виде событий по технологии Защита конечных устройств и инцидентов EDR.

- Расширены возможности импорта конфигураций устройств и тегов из проектов для устройств IEC 61850 – теги импортируются в программу в исходном структурном виде, а также по результатам импорта программа автоматически формирует правила контроля взаимодействий.

- Расширены возможности получения данных от Kaspersky Industrial CyberSecurity for Linux Nodes – при работе в режиме интеграции с этим приложением Kaspersky Industrial CyberSecurity for Networks получает больше сведений о Linux-устройствах по результатам выполнения заданий для аудита безопасности.

- Реализована поддержка работы в режиме интеграции с решением Kaspersky SD-WAN – в этом режиме Kaspersky Industrial CyberSecurity for Networks получает трафик промышленных сетей с удаленных технологических площадок от компонентов решения Kaspersky SD-WAN.

- В программу добавлен новый тип коннектора **Cisco Switch** – с помощью коннекторов этого типа вы можете настроить автоматическое управление сетевым доступом устройств с использованием сетевых коммутаторов Cisco.

- Расширены списки обнаруживаемых уязвимостей промышленного оборудования и программного обеспечения — с использованием функциональности контроля рисков и функциональности аудита безопасности программа может обнаруживать уязвимости устройств Прософт-Системы ARIS, ABB, Rockwell Automation, сетевых устройств Cisco, Hirschmann и Moxa, а также уязвимости в программном обеспечении Rockwell Automation FactoryTalk и Siemens WinCC OA.

- В наборы правил для заданий аудита настроек и уязвимостей добавлены правила для проверки соответствия приказу ФСТЭК №239 (для Windows- и Linux-устройств) и стандарту NIST Special Publication 800-53.

В версии Kaspersky Industrial CyberSecurity for Networks 4.2.1 появились следующие возможности и доработки:

- Добавлена поддержка получения расширенных сведений и контроля конфигураций для устройств Emerson DeltaV (с версией системы 14) и Rockwell Automation Allen-Bradley.

- Добавлена поддержка базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, выделенной для работы с Linux-устройствами – вместе с обновлениями баз и программных модулей поставляется и обновляется набор правил **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП (Linux)**, который является системным набором правил аудита настроек и уязвимостей.

- Добавлена поддержка протокола ВНИИА для контроля процесса.

- Добавлена функциональность контроля команд управления сетевым оборудованием по протоколу Telnet.

- Добавлена поддержка упрощенного китайского языка локализации.

- Выбор языка локализации компонентов Kaspersky Industrial CyberSecurity for Networks выполняется при установке Сервера программы, а не во время начальной настройки на странице веб-интерфейса Сервера (при начальной настройке в разделе **Начальная настройка** программа предлагает выбрать язык веб-интерфейса программы, который в дальнейшем вы можете изменять с помощью меню).

Архитектура программы

Kaspersky Industrial CyberSecurity for Networks включает в себя следующие компоненты:

- *Сервер* – основной компонент, который принимает данные, обрабатывает и предоставляет их пользователям программы. Полученная информация (например, события и сведения об устройствах) сохраняется на Сервере в базе данных. В каждой схеме развертывания Kaspersky Industrial CyberSecurity for Networks может использоваться только один Сервер.

- *Сенсор* – компонент, который под управлением Сервера получает и анализирует данные из вычислительных сетей, подключенных к сетевым интерфейсам компьютера. Результаты анализа данных сенсор передает на Сервер. По запросам Сервера сенсор может отправлять на Сервер полученные данные в том виде, в котором они поступили для анализа (например, трафик, относящийся к зарегистрированным событиям). Сенсоры устанавливаются на отдельных компьютерах. Если компьютер выполняет функции Сервера, на этот компьютер невозможно установить сенсор. В программе может использоваться до 50 сенсоров.

Безопасность соединений Сервера и сенсоров обеспечивается с использованием сертификатов. С помощью сертификатов также обеспечивается безопасность и других соединений с компонентами программы (например, подключение к компоненту через веб-интерфейс или подключение сторонних систем через специальные программные модули – *коннекторы*).

Если на компьютерах контролируемой сети установлены приложения "Лаборатории Касперского", выполняющие функции защиты рабочих станций и серверов (EPP-приложения), в Kaspersky Industrial CyberSecurity for Networks можно настроить интеграцию с этими приложениями. После настройки интеграции Сервер и/или сенсоры получают данные от EPP-приложений и могут взаимодействовать с ними.

При использовании заданий аудита безопасности Сервер и/или сенсоры могут удаленно подключаться к устройствам для сканирования устройств и получения результатов.

Сервер Kaspersky Industrial CyberSecurity for Networks выполняет следующие функции:

- управляет сенсорами и принимает от них результаты анализа полученных данных;

- обрабатывает и сохраняет полученные сведения об устройствах и их взаимодействиях;

- регистрирует и сохраняет события;

- выполняет дополнительный анализ накопленной информации для обнаружения угроз и инцидентов (например, по правилам корреляции событий);

- контролирует работоспособность программы;

- контролирует действия пользователей программы;

- обрабатывает поступающие запросы через веб-интерфейс и коннекторы и предоставляет запрашиваемые данные.

Сенсор Kaspersky Industrial CyberSecurity for Networks выполняет следующие функции:

- анализирует поступающий трафик промышленной сети:
  - выделяет из трафика данные о взаимодействиях устройств и о технологических параметрах;
  - выявляет признаки атак в трафике;
- регистрирует события по результатам анализа данных;
- передает события, информацию о трафике, об устройствах и о технологических параметрах на Сервер Kaspersky Industrial CyberSecurity for Networks.

Компоненты программы получают копию трафика промышленной сети от *точек мониторинга*. Точки мониторинга могут использоваться как на сенсорах, так и на Сервере. Вы можете добавить точки мониторинга на сетевые интерфейсы, обнаруженные на узлах с установленными компонентами программы. Точки мониторинга требуется добавить на сетевые интерфейсы, через которые поступает трафик из промышленной сети.

Все сетевые интерфейсы, на которые добавлены точки мониторинга, должны быть подключены к промышленной сети таким образом, чтобы исключить возможность влияния на промышленную сеть. Например, для подключения можно использовать порты сетевых коммутаторов промышленной сети, настроенные на передачу зеркалированного трафика (Switched Port Analyzer, SPAN).

На узлах с установленными компонентами программы вы можете настроить операционную систему для приема зеркалированного трафика с использованием технологии ERSPAN (Encapsulated Remote SPAN). После настройки для технологии ERSPAN в операционной системе узла появляется виртуальный сетевой интерфейс, на который вы можете добавить точку мониторинга.

В программе действуют следующие ограничения на количество точек мониторинга:

- суммарное количество точек мониторинга – не более 50;
- количество точек мониторинга на Сервере – не более 4;
- количество точек мониторинга на сенсоре – не более 8.

При работе в режиме интеграции с решением Kaspersky SD-WAN вы можете использовать не более 100 точек мониторинга как на одном узле, так и суммарно на всех узлах с установленными компонентами программы.

Для соединения с Сервером сенсоров и других компонентов решения Kaspersky Industrial CyberSecurity (Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes, Kaspersky Security Center) рекомендуется использовать *выделенную сеть* Kaspersky Industrial CyberSecurity. Сетевое оборудование для взаимодействия компонентов в выделенной сети должно быть установлено отдельно от промышленной сети. В общем случае к выделенной сети следует подключить следующие компьютеры и устройства:

- узел Сервера Kaspersky Industrial CyberSecurity for Networks;
- узлы сенсоров Kaspersky Industrial CyberSecurity for Networks;
- компьютеры для подключения к Серверу и сенсорам через веб-интерфейс;

- компьютеры с Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes и программными компонентами Endpoint Agent;
- устройства, к которым выполняются удаленные подключения для сканирования в рамках заданий аудита безопасности;
- компьютеры с программными модулями коннекторов;
- компьютер с Kaspersky Security Center;
- сетевой коммутатор.

Типовые схемы развертывания

В Kaspersky Industrial CyberSecurity for Networks предусмотрены следующие способы установки компонентов:

- установка Сервера без внешних сенсоров;
- установка Сервера и внешних сенсоров.

При необходимости для подключения Сервера и/или сенсоров к промышленной сети может использоваться диод данных.

При любом способе установки рекомендуется использовать специальную выделенную сеть для соединения компонентов решения Kaspersky Industrial CyberSecurity (Kaspersky Industrial CyberSecurity for Networks, Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes, Kaspersky Security Center). Минимальное требование к пропускной способности выделенной сети при установке Сервера и сенсоров Kaspersky Industrial CyberSecurity for Networks см. в статье Аппаратные и программные требования.

Установка Сервера без внешних сенсоров

При установке Сервера без внешних сенсоров все данные для обработки и анализа поступают только на компьютер, выполняющий функции Сервера. Вы можете применить этот способ установки, если компьютер имеет достаточное количество сетевых интерфейсов для получения данных из различных источников.

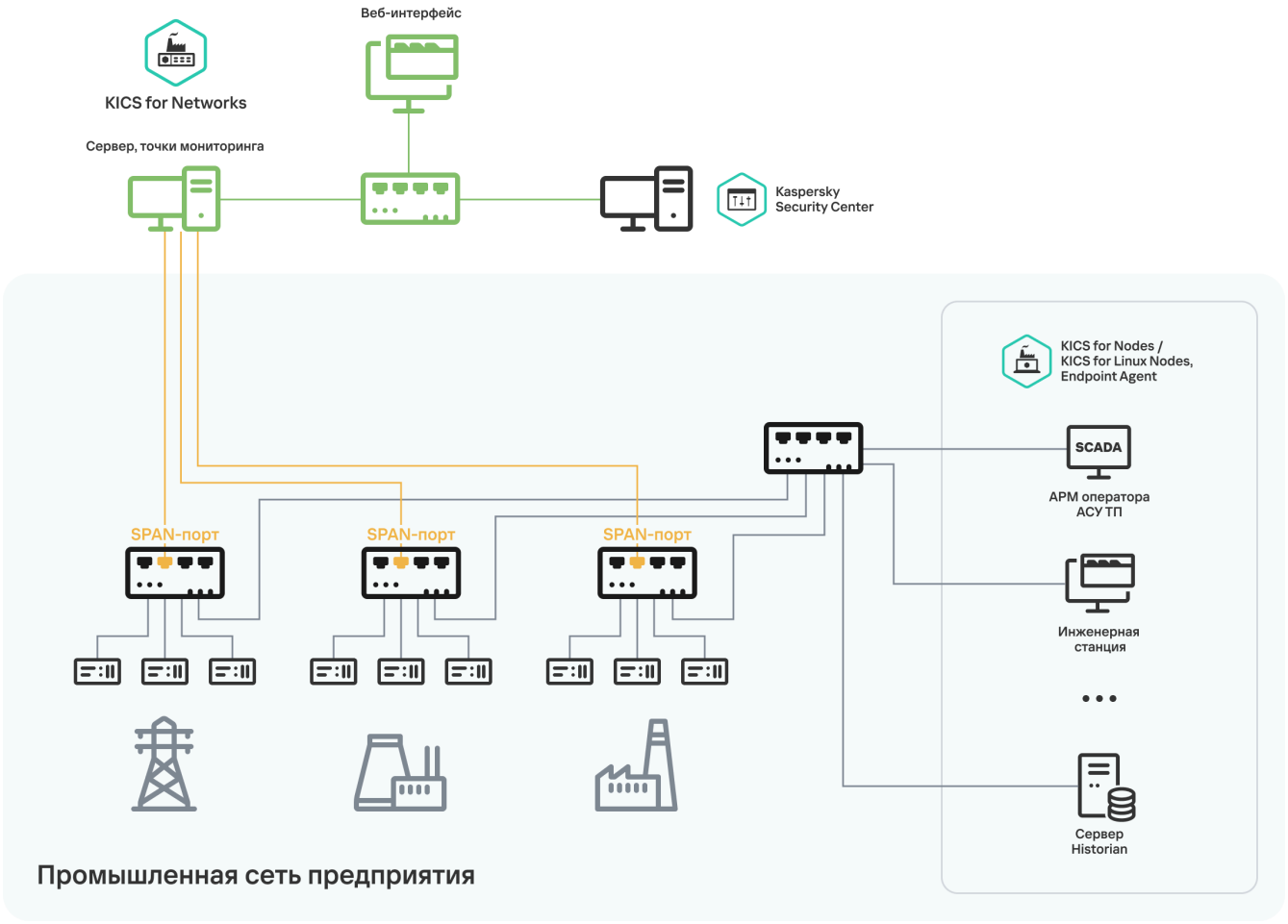
Схему развертывания Сервера без внешних сенсоров рекомендуется выбирать для мониторинга одной площадки с небольшим количеством источников трафика. В случае распределенной сетевой архитектуры рекомендуется выбирать схему развертывания Сервера и внешних сенсоров.

Если для передачи трафика на Сервер в распределенной сетевой архитектуре используются средства агрегации трафика (такие, как коммутаторы агрегации или брокеры сетевых пакетов), это может привести к потере контекста об источниках возникновения событий информационной безопасности. Кроме того, если в различных сегментах сети используются одинаковые адреса устройств, эти адреса будут неправильно сопоставляться с устройствами без дополнительной настройки средств агрегации трафика и программы. Также в программе могут быть недоступны для контроля отдельные сегменты сети и устройства, могут возникать ошибки при использовании некоторых функций программы (в частности, в функциональности аудита и активных опросов, реагирования на угрозы).

На компьютере должны быть сетевые интерфейсы для поступления трафика на точки мониторинга из всех сегментов промышленной сети. Всего таких сетевых интерфейсов должно быть не более четырех, в связи с ограничением на количество точек мониторинга на Сервере.

Также компьютер должен иметь еще один сетевой интерфейс для подключения к Серверу с других компьютеров через веб-интерфейс. На этом сетевом интерфейсе не должно быть точки мониторинга. Если на компьютере больше нет свободных сетевых интерфейсов, этот же сетевой интерфейс может использоваться и для других подключений из выделенной сети Kaspersky Industrial CyberSecurity.

На рисунке ниже показан пример схемы развертывания Сервера без сенсоров. Сетевые интерфейсы компьютера, выполняющего функции Сервера, подключаются к SPAN-портам сетевых коммутаторов (SPAN-порты и соединения обозначены желтым цветом) и получают копию трафика из трех сегментов промышленной сети. Выделенная сеть Kaspersky Industrial CyberSecurity обозначена линиями зеленого цвета.



Пример схемы развертывания Сервера без сенсоров

Установка Сервера и внешних сенсоров

Способ установки Сервера и внешних сенсоров предполагает использование нескольких компьютеров для установки компонентов программы. На одном из компьютеров устанавливается Сервер. На остальных компьютерах устанавливаются сенсоры, которые будут получать данные из вычислительных сетей. В программе может использоваться до 50 сенсоров.

Для получения трафика из промышленной сети требуется добавить точки мониторинга на компьютеры:

- не более 8 точек мониторинга на сенсоре;
- не более 4 точек мониторинга на Сервере;
- всего в программе не более 50 точек мониторинга.

Точки мониторинга требуется добавить на те сетевые интерфейсы, на которые будет поступать трафик из сегментов промышленной сети. Компьютер должен иметь по одному сетевому интерфейсу на каждую точку мониторинга.

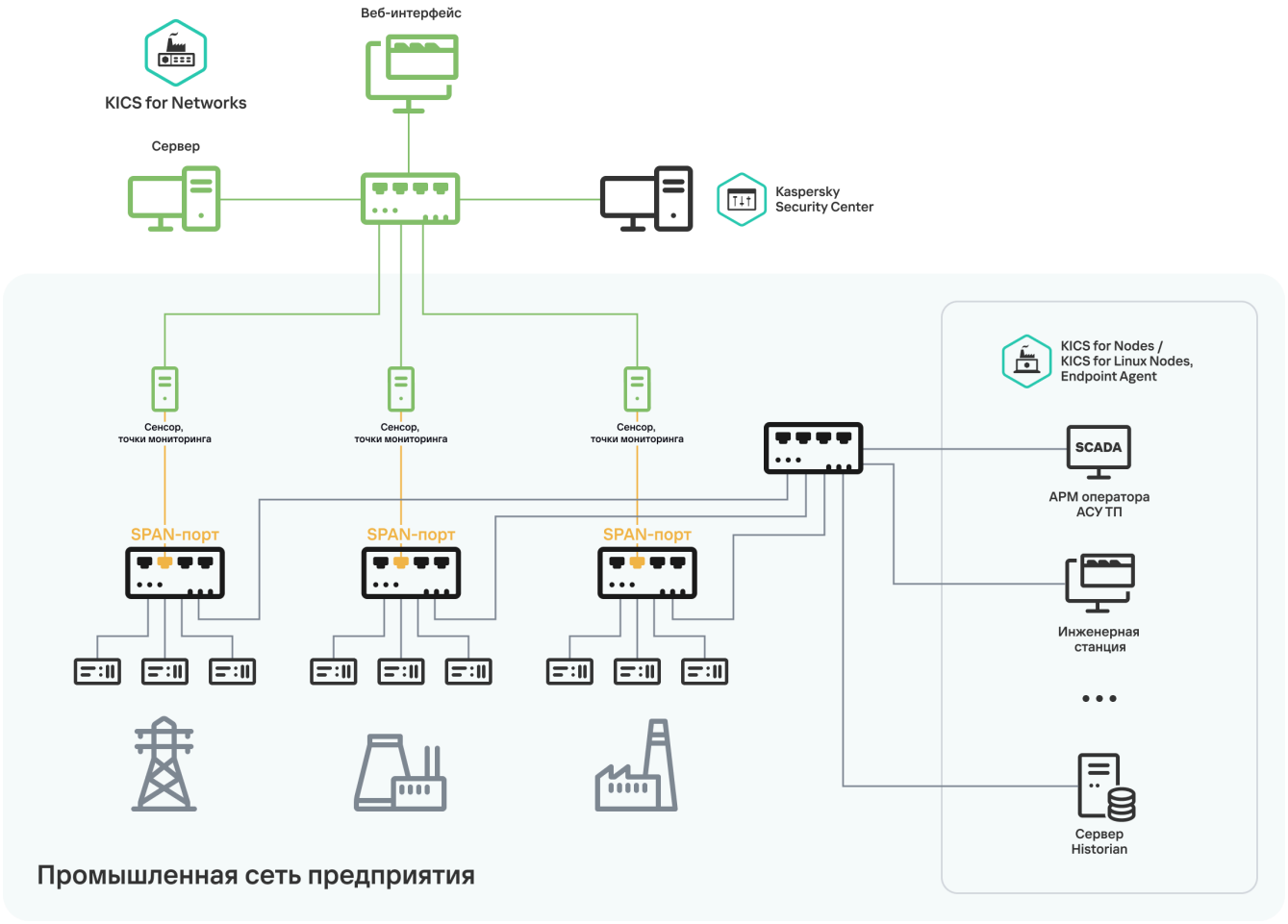
Также компьютеры должны иметь отдельные сетевые интерфейсы, которые будут использоваться в следующих целях:

- соединение с Сервером (на компьютерах, которые выполняют функции сенсоров);
- подключение с других компьютеров через веб-интерфейс;
- другие подключения из выделенной сети Kaspersky Industrial CyberSecurity.

Для этих целей на каждом компьютере могут использоваться как несколько отдельных сетевых интерфейсов, так и один общий сетевой интерфейс. На этих сетевых интерфейсах не должно быть точек мониторинга.

Сенсоры Kaspersky Industrial CyberSecurity for Networks рекомендуется устанавливать вблизи источников трафика и/или в тех же сегментах сети, в которых установлены Kaspersky Industrial CyberSecurity for Nodes и/или Kaspersky Industrial CyberSecurity for Linux Nodes. Такой подход позволит упростить настройку интеграции между программами, не потребует дополнительных действий по настройке доступа к устройствам и конфигурированию сетевого оборудования, а также минимизирует сетевые соединения между различными сегментами.

На рисунке ниже показан пример схемы развертывания Сервера и трех сенсоров. Сетевые интерфейсы компьютеров, выполняющих функции сенсоров, подключаются к SPAN-портам сетевых коммутаторов (SPAN-порты и соединения обозначены желтым цветом) и получают копию трафика из соответствующих сегментов промышленной сети. Выделенная сеть Kaspersky Industrial CyberSecurity обозначена линиями зеленого цвета.



Пример схемы развертывания Сервера и трех сенсоров

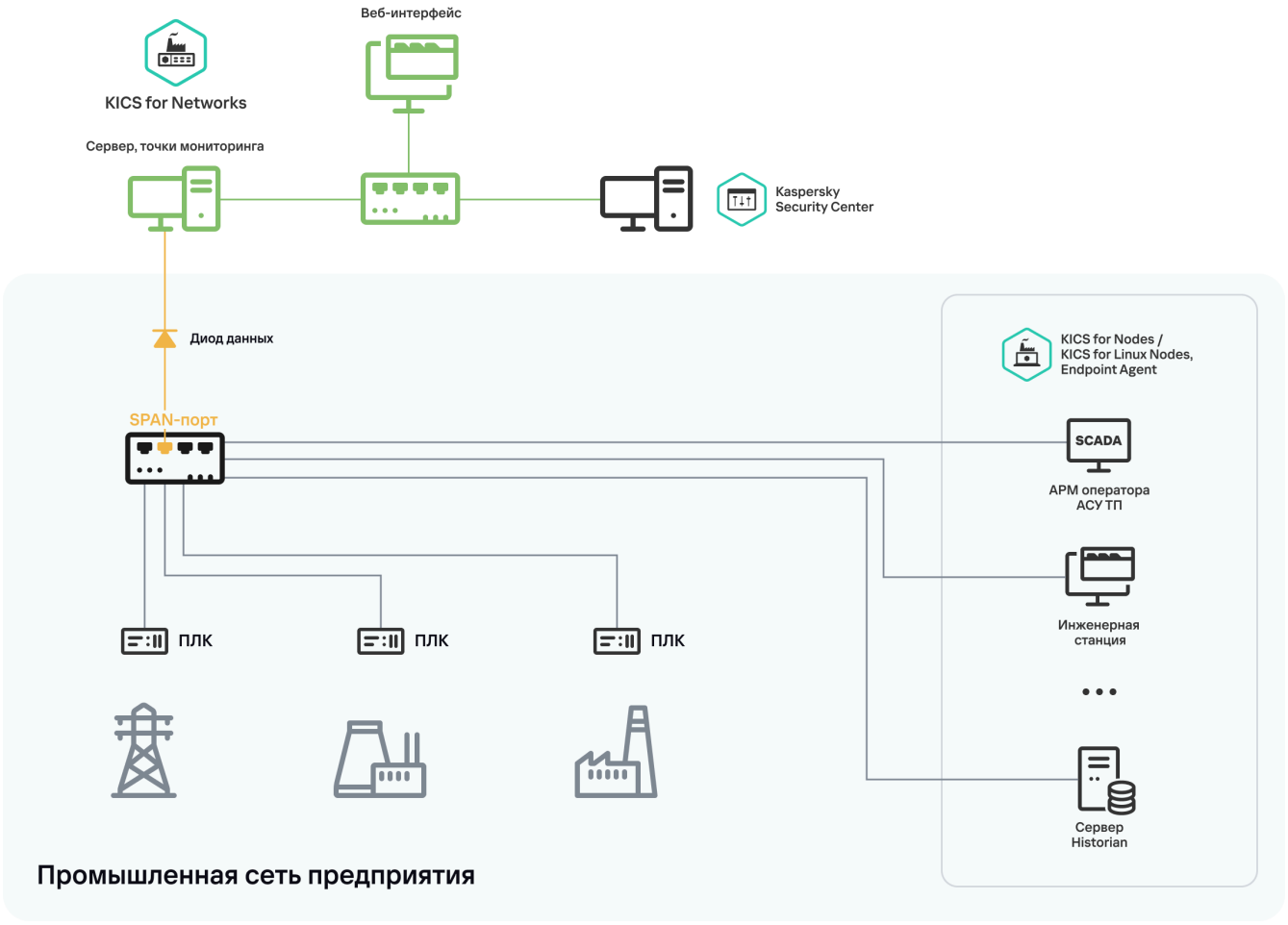
Подключение Kaspersky Industrial CyberSecurity for Networks к промышленной сети через диод данных

Для подключения Kaspersky Industrial CyberSecurity for Networks к промышленной сети вы можете дополнительно использовать специальные устройства, обеспечивающие одностороннюю передачу данных из промышленной сети. Такие устройства называются *диодами данных*.

Получение трафика промышленной сети через диоды данных

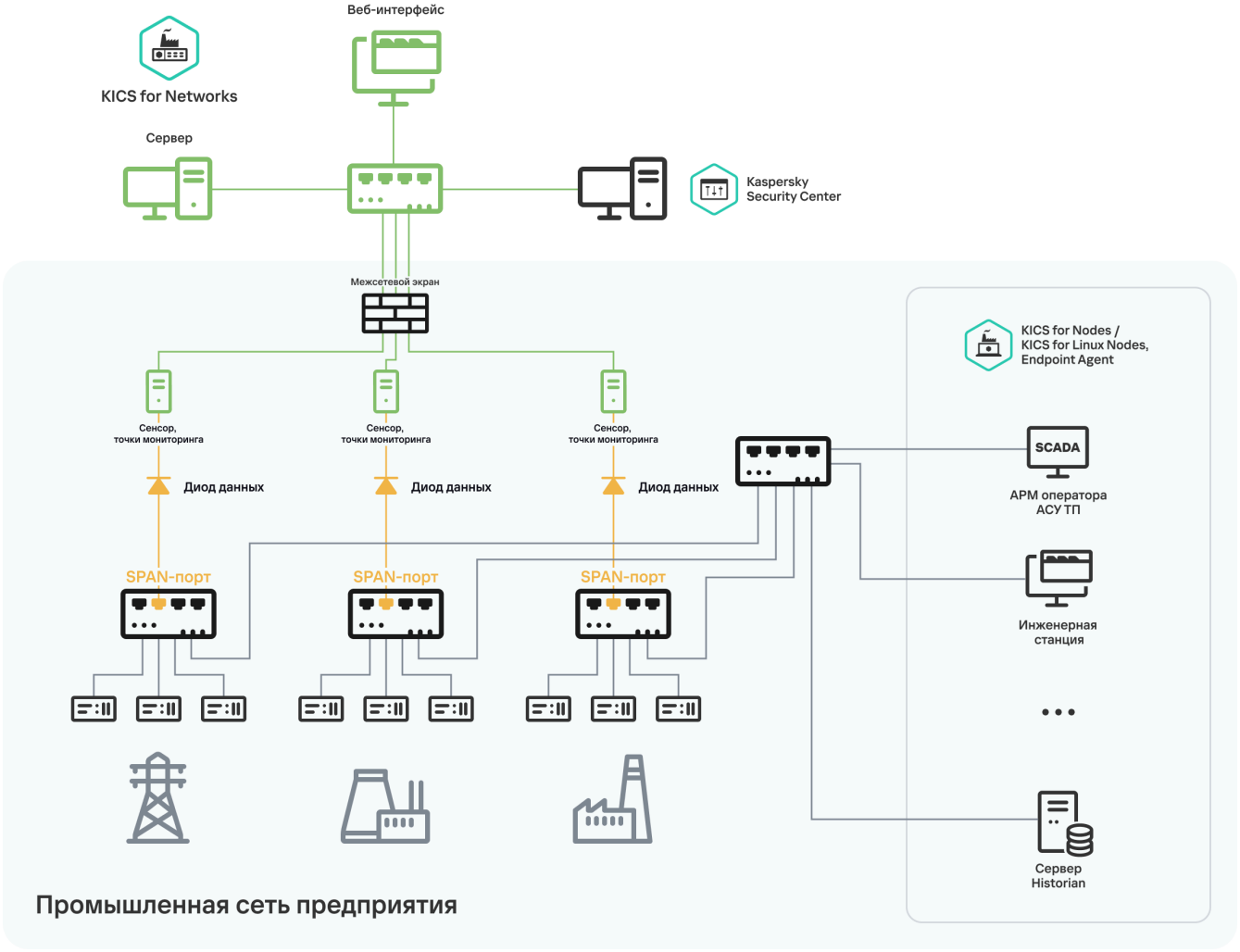
Для передачи трафика промышленной сети в Kaspersky Industrial CyberSecurity for Networks диоды данных должны поддерживать передачу сетевых пакетов без фильтрации для всех протоколов канального уровня, включая служебные протоколы. Диоды данных устанавливаются на линиях соединений точек мониторинга Kaspersky Industrial CyberSecurity for Networks и SPAN-портов сетевых коммутаторов.

На рисунке ниже показана схема развертывания с подключением через диод данных к точке мониторинга на Сервере. Через диод данных поступает трафик от SPAN-порта сетевого коммутатора в промышленной сети. В этой схеме применяется способ установки Сервера без внешних сенсоров.



Типовая схема с подключением Сервера через диод данных

На рисунке ниже показана схема развертывания с подключением нескольких сенсоров Kaspersky Industrial CyberSecurity for Networks через диоды данных. Через диоды данных поступает трафик от SPAN-портов сетевых коммутаторов в промышленной сети. В этой схеме применяется способ установки Сервера и трех сенсоров.



Типовая схема с подключением сенсоров через диоды данных

Если вы хотите дополнительно разграничить сегменты промышленной сети, в которых установлены сенсоры, и сегмент выделенной сети Kaspersky Industrial CyberSecurity, в котором установлен Сервер, вы можете использовать межсетевой экран на линиях соединений сенсоров и Сервера.

Получение трафика промышленной сети и работа в режиме интеграции с EPP-приложениями через диоды данных

При работе в режиме интеграции с EPP-приложениями возможности передачи данных через диоды должны поддерживаться как на стороне диодов данных, так и на стороне EPP-приложений.

На рисунке ниже показана схема развертывания для случая, когда на сенсоры Kaspersky Industrial CyberSecurity for Networks поступает трафик от SPAN-портов сетевых коммутаторов и данные телеметрии от EPP-приложений из нескольких технологических площадок.

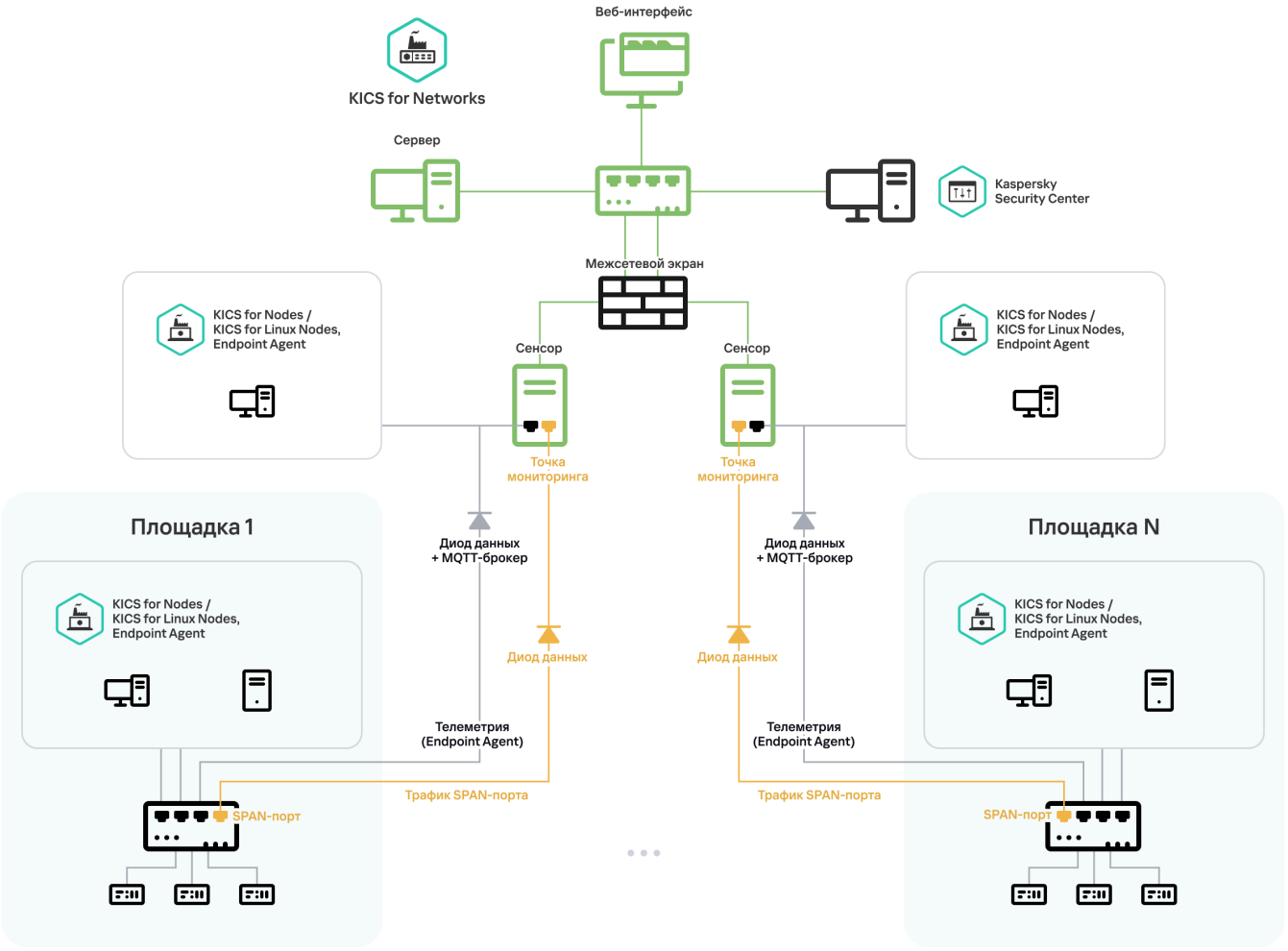


Схема получения трафика и данных от EPP-приложений на сенсоры

Трафик от SPAN-портов сетевых коммутаторов поступает на точки мониторинга сенсоров Kaspersky Industrial CyberSecurity for Networks через диоды данных, которые поддерживают передачу сетевых пакетов без фильтрации для всех протоколов канального уровня, включая служебные протоколы.

Данные телеметрии от EPP-приложений поступают на сенсоры через сетевые интерфейсы, которые не используются в качестве точек мониторинга. Эти данные передаются в виде сообщений по протоколу MQTT, поэтому для их передачи диоды данных должны поддерживать функциональность MQTT-брокера. Для приема и обработки поступающих MQTT-сообщений используются компьютеры-подписчики с установленными EPP-приложениями.

Отправку и прием MQTT-сообщений с данными телеметрии выполняют программные компоненты Endpoint Agent. Для получения дополнительных сведений о настройке EPP-приложений при такой схеме передачи данных телеметрии вы можете обратиться к вашему персональному техническому менеджеру (TAM).

Для разграничения сегментов технологических площадок и сегмента сети демилитаризованной зоны используется межсетевой экран.

Получение трафика промышленных сетей от компонентов решения Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity for Networks может работать в режиме интеграции с решением Kaspersky SD-WAN. При работе в этом режиме Kaspersky Industrial CyberSecurity for Networks получает зеркалированный трафик, который проходит через сетевые коммутаторы на удаленных технологических площадках, если на этих площадках установлен компонент решения Kaspersky SD-WAN устройство Customer Premise Equipment (далее "устройство CPE"). С помощью устройств CPE вы можете частично реализовать функции сенсоров Kaspersky Industrial CyberSecurity for Networks, обеспечив получение программой трафика промышленных сетей с географически разнесенных площадок. При этом данные передаются в программу по защищенным каналам.

Устройства CPE, получающие зеркалированный трафик непосредственно на удаленных площадках, шифруют этот трафик для его передачи на другие (принимающие) устройства CPE, расположенные в одной сети с узлами Kaspersky Industrial CyberSecurity for Networks. Принимающим устройствам CPE должна быть назначена роль шлюза SD-WAN, если связь между устройствами, передающими зеркалированный трафик, возможна только через шлюз. Рекомендуется размещать принимающие устройства CPE в выделенной сети Kaspersky Industrial CyberSecurity. Эти устройства передают зеркалированный трафик на сетевые интерфейсы узлов Kaspersky Industrial CyberSecurity for Networks.

Идентификация трафика, поступающего на сетевой интерфейс узла Kaspersky Industrial CyberSecurity for Networks от разных устройств CPE, выполняется за счет добавления в сетевые пакеты идентификаторов виртуальных локальных сетей (VLAN) в соответствии со стандартом IEEE 802.1q. При настройке интеграции Kaspersky Industrial CyberSecurity for Networks с решением Kaspersky SD-WAN требуется обеспечить соответствие используемых идентификаторов VLAN на стороне компонентов Kaspersky SD-WAN и на стороне компьютера с установленным компонентом Kaspersky Industrial CyberSecurity for Networks (каждый сетевой интерфейс, на который поступает трафик с определенным идентификатором VLAN, должен быть VLAN-интерфейсом с совпадающим идентификатором).

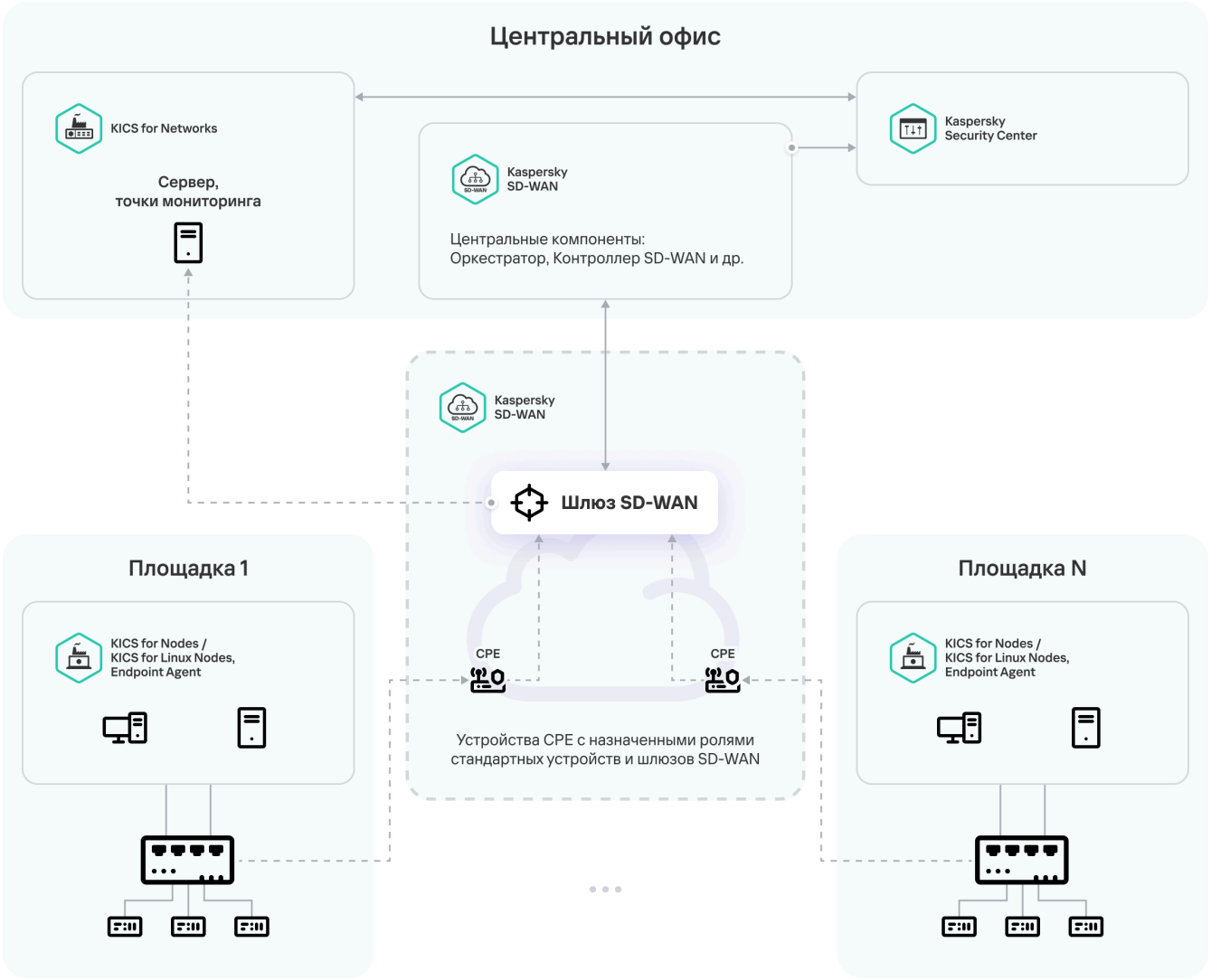
Для эффективного использования режима интеграции в программе можно расширить ограничения на количество точек мониторинга путем дополнительной настройки программных компонентов. Максимально возможные ограничения для режима интеграции с решением Kaspersky SD-WAN:

- не более 100 точек мониторинга на узле;
- всего в программе не более 100 точек мониторинга.

Остальные требования к развертыванию компонентов Kaspersky Industrial CyberSecurity for Networks аналогичны другим типовым схемам развертывания (например, для схемы установки Сервера без внешних сенсоров).

Для получения дополнительных сведений о настройке программных компонентов для работы в режиме интеграции вы можете обратиться к вашему персональному техническому менеджеру (TAM).

На рисунке ниже показан пример схемы развертывания Kaspersky Industrial CyberSecurity for Networks и решения Kaspersky SD-WAN для случая, когда зеркалированный трафик из нескольких технологических площадок поступает на Сервер Kaspersky Industrial CyberSecurity for Networks через один шлюз SD-WAN. Компьютеры, подключенные к выделенной сети Kaspersky Industrial CyberSecurity, и компьютеры с центральными компонентами SD-WAN находятся в центральном офисе организации. Пунктирными линиями обозначен путь передачи зеркалированного трафика от сетевых коммутаторов на удаленных технологических площадках.



Пример схемы развертывания совместно с решением Kaspersky SD-WAN

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Industrial CyberSecurity for Networks.

Подготовка к установке программы

Перед началом установки Kaspersky Industrial CyberSecurity for Networks убедитесь, что компьютеры удовлетворяют аппаратным и программным требованиям. Также убедитесь, что соблюдаются рекомендации по обеспечению безопасной работы в отношении оборудования, аппаратного и программного обеспечения компьютеров.

Для работы компонентов программы рекомендуется использовать отдельные компьютеры, на которых установлено только программное обеспечение из состава операционной системы. Если на компьютерах установлено прикладное программное обеспечение сторонних производителей, производительность компонентов Kaspersky Industrial CyberSecurity for Networks может быть снижена.

Для установки компонентов программы на каждом компьютере должна быть учетная запись пользователя с root-правами, от имени которого будет выполняться установка. Вы можете добавить нужные учетные записи с помощью стандартных средств операционной системы.

В зависимости от используемого скрипта установки компонентов программы из состава комплекта поставки, а также от типа устанавливаемых компонентов программы, вам нужно выполнить действия для подготовки к централизованной установке компонентов или локальной установке Сервера или сенсора.

Подготовка к централизованной установке компонентов

На компьютерах для централизованной установки компонентов проверьте выполнение следующих условий:

- К компьютерам есть сетевой доступ, настроен и открыт доступ по протоколу SSH.
- На компьютерах есть учетные записи пользователей с root-правами (от имени этих пользователей будет выполняться установка компонентов программы).
- На компьютерах отсутствуют учетные записи пользователей и групп со следующими именами, зарезервированными для взаимодействия компонентов программы (если такие учетные записи существуют, после установки программы они могут получить повышенные права доступа вплоть до root-прав):
  - kics4net;
  - kics4net-apm;
  - kics4net-asset-config-repo;
  - kics4net-asset-inventory;
  - kics4net-blob-storage;
  - kics4net-config-control-orch;
  - kics4net-connectors;
  - kics4net-connectors-launcher;
  - kics4net-email-gateway;
  - kics4net-epp-proxy;
  - kics4net-fts;
  - kics4net-nats;
  - kics4net-nats-server;
  - kics4net-oval-facade;
  - kics4net-postgresql;
  - kics4net-report-builder;
  - kics4net-report-data-source;
  - kics4net-report-renderer;
  - kics4net-report-tc;

- kics4net-report-tcv;
- kics4net-responses-manager;
- kics4net-risk-oval-detector;
- kics4net-scap-manager;
- kics4net-scap-manager-view;
- kics4net-scan-oval-manager;
- kics4net-scheduler;
- kics4net-secrets;
- kics4net-task-m;
- kics4net-task-mv;
- kics4net-vault;
- kics4net-websensor;
- kics4net-webserver.

Чтобы подготовить компьютеры к установке компонентов программы:

1. На всех компьютерах, на которых будут установлены компоненты программы, назначьте одинаковый пароль для учетной записи пользователя с root-правами (от имени которого будет выполняться установка компонентов программы). По умолчанию в качестве учетной записи пользователя, от имени которого выполняется установка, используется учетная запись root. Запомните имена пользователей и пароль. Эти данные потребуется указать при работе скрипта установки программы.

   После установки компонентов программы рекомендуется изменить пароли для этих пользователей.

2. Выясните и сохраните следующие данные о компьютерах:

   - Имя и IP-адрес компьютера, который будет выполнять функции Сервера.
   - IP-адреса компьютеров, которые будут выполнять функции сенсоров.
   - Имя или IP-адрес и SSL-порт компьютера с Kaspersky Security Center.

   Для вывода имени компьютера вы можете ввести в командной строке команду `hostname`. Для вывода сведений об IP-адресах и сетевых интерфейсах вы можете ввести в командной строке команду `sudo ifconfig` (в операционной системе Windows® используйте команду `ipconfig`).

3. На компьютере, с которого будет выполняться централизованная установка, подключитесь по протоколу SSH к каждому компьютеру, на который будут устанавливаться компоненты программы. Подключение нужно выполнить для проверки доступа по протоколу SSH.

   Для подключения выполните следующие действия:

   a. Введите в командной строке команду:

      `ssh <имя пользователя>@<IP-адрес компьютера>`

   b. После ввода команды выполните необходимые действия по запросам операционной системы.

   c. Для завершения сеанса подключения используйте команду:

      `exit`

4. Скопируйте архив kics4net-release_<номер версии программы>.tar.gz из комплекта поставки на компьютер, с которого будет выполняться установка.

5. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки архива:

   `tar -zxvf kics4net-release_<номер версии программы>.tar.gz`

   Распакованные директории и файлы появятся во вложенной директории kics4net-release_<номер версии программы>.

6. При подготовке к установке компонентов версии Kaspersky Industrial CyberSecurity for Networks 4.2.1: если вы хотите использовать функциональность взаимодействия с Kaspersky Security Center и на компьютере, на котором будет установлен Сервер, не устанавливался Агент администрирования Kaspersky Security Center, то скопируйте пакет для установки Агента администрирования klnagent64-<номер версии Агента администрирования>.x86_64.rpm в директорию kics4net-release_<номер версии программы>/linux-centos.

   Для получения пакета для установки Агента администрирования Kaspersky Security Center вы можете обратиться к вашему персональному техническому менеджеру (TAM).

Подготовка к локальной установке Сервера или сенсора

На компьютере для установки Сервера или сенсора проверьте выполнение следующих условий:

- К компьютеру есть сетевой доступ.
- На компьютере есть учетная запись пользователя с root-правами (от имени этого пользователя будет запущен скрипт локальной установки).
- На компьютере отсутствуют учетные записи пользователей и групп со следующими именами, зарезервированными для взаимодействия компонентов программы (если такие учетные записи существуют, после установки программы они могут получить повышенные права доступа вплоть до root-прав):
  - Если на компьютере будет установлен Сервер:
    - kics4net;
    - kics4net-apm;
    - kics4net-asset-config-repo;
    - kics4net-asset-inventory;
    - kics4net-blob-storage;
    - kics4net-config-control-orch;
    - kics4net-connectors;
    - kics4net-connectors-launcher;
    - kics4net-email-gateway;
    - kics4net-epp-proxy;
    - kics4net-fts;
    - kics4net-nats;
    - kics4net-nats-server;
    - kics4net-oval-facade;
    - kics4net-postgresql;
    - kics4net-report-builder;
    - kics4net-report-data-source;
    - kics4net-report-renderer;

- kics4net-report-tc;
- kics4net-report-tcv;
- kics4net-responses-manager;
- kics4net-risk-oval-detector;
- kics4net-scap-manager;
- kics4net-scap-manager-view;
- kics4net-scan-oval-manager;
- kics4net-scheduler;
- kics4net-secrets;
- kics4net-task-m;
- kics4net-task-mv;
- kics4net-vault;
- kics4net-webserver.

- Если на компьютере будет установлен сенсор:
  - kics4net;
  - kics4net-apm;
  - kics4net-connectors;
  - kics4net-connectors-launcher;
  - kics4net-epp-proxy;
  - kics4net-nats;
  - kics4net-nats-server;
  - kics4net-oval-facade;
  - kics4net-websensor.

Чтобы подготовить компьютер к локальной установке Сервера или сенсора:

1. Выясните и сохраните следующие данные о компьютере:

   - Учетные данные пользователя с root-правами, от имени которого будет выполнен запуск скрипта локальной установки.
   - Имя и IP-адрес компьютера (для последующего подключения к этому компьютеру).

   Для вывода имени компьютера вы можете ввести в командной строке команду `hostname`. Для вывода сведений об IP-адресах и сетевых интерфейсах вы можете ввести в командной строке команду `sudo ifconfig`.

2. Скопируйте архив kics4net-release_<номер версии программы>.tar.gz из комплекта поставки на компьютер.

3. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки архива:

   `tar -zxvf kics4net-release_<номер версии программы>.tar.gz`

   Распакованные директории и файлы появятся во вложенной директории kics4net-release_<номер версии программы>.

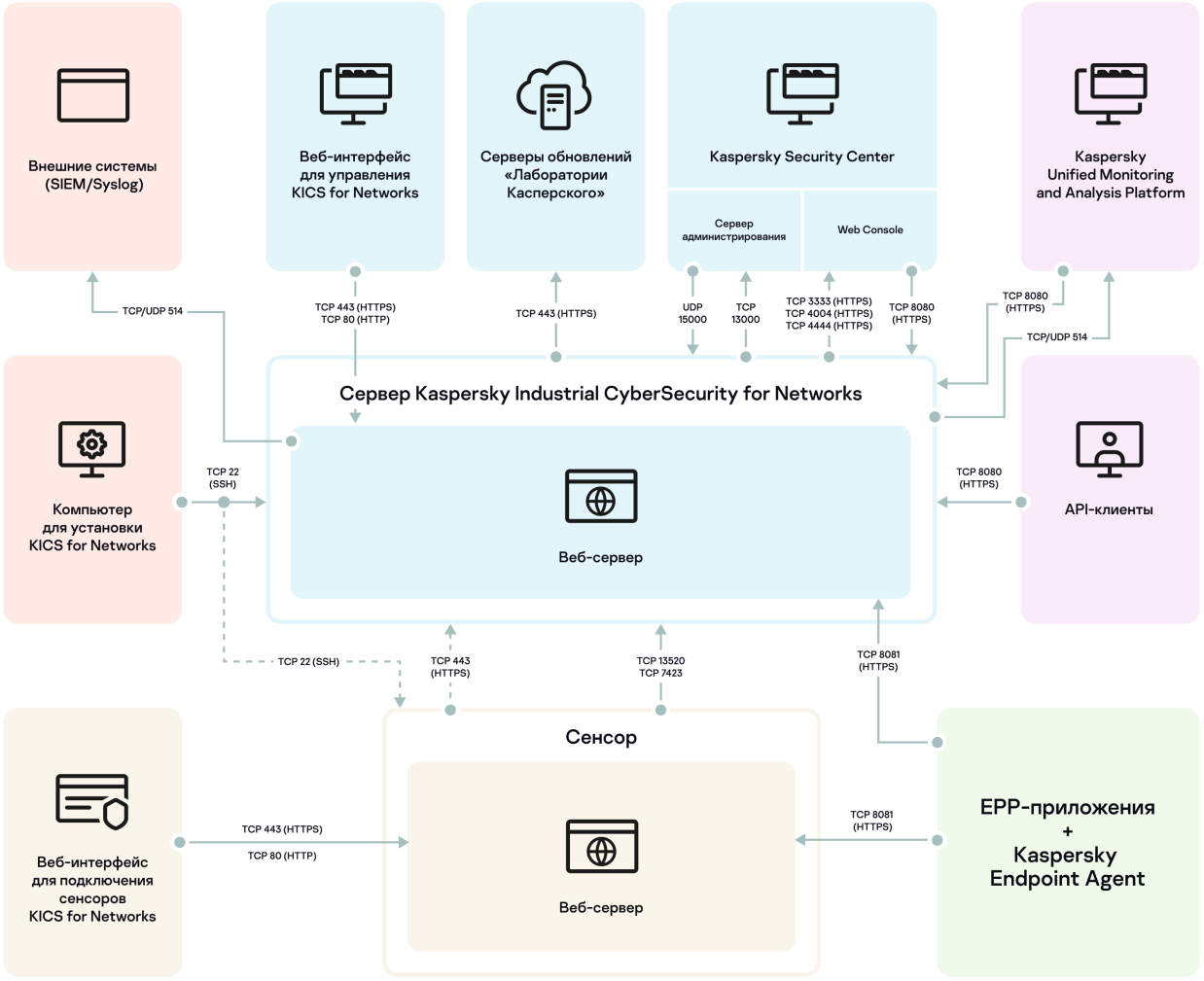
4. При подготовке к установке Сервера версии Kaspersky Industrial CyberSecurity for Networks 4.2.1: если вы хотите использовать функциональность взаимодействия с Kaspersky Security Center и на компьютере, на котором будет установлен Сервер, не устанавливался Агент администрирования Kaspersky Security Center, то скопируйте пакет для установки Агента администрирования klnagent64-<номер версии Агента администрирования>.x86_64.rpm в директорию kics4net-release_<номер версии программы>/linux-centos.

   Для получения пакета для установки Агента администрирования Kaspersky Security Center вы можете обратиться к вашему персональному техническому менеджеру (TAM).

Используемые порты для установки и работы компонентов

Для установки и работы компонентов Kaspersky Industrial CyberSecurity for Networks должны быть доступны определенные порты и протоколы, которые будут использоваться для передачи данных. Вам нужно настроить доступность портов и протоколов в параметрах сетевого оборудования или программного обеспечения, с помощью которого контролируется сетевой трафик.

На рисунке ниже показаны порты и протоколы, используемые компонентами программы.



Используемые порты и протоколы

Назначение используемых портов описано в таблице ниже.

Назначение используемых портов

Порт	Протокол	Описание
Компьютер для установки компонентов программы		
22	TCP (SSH)	Используется для подключения к узлам и установки компонентов Сервера и сенсоров.
Компьютер, выполняющий функции Сервера		
22	TCP (SSH)	Используется для взаимодействия с компьютером для установки компонентов программы.
80	TCP (HTTP)	Используется для подключения через веб-интерфейс.
443	TCP (HTTPS)	Используется для следующих целей: • подключение через веб-интерфейс; • подключение к серверам обновлений "Лаборатории Касперского"; • подключение сенсора через веб-интерфейс автоматически по сети.
514	TCP/UDP	Используется для отправки данных через коннекторы SIEM и Syslog.

Порт	Протокол	Описание
3333 4004 4444	TCP (HTTPS)	Используются для взаимодействия с компонентом Identity and Access Manager в Kaspersky Security Center Web Console при использовании технологии единого входа (SSO).
7423	TCP	Используется для подключений сенсоров.
8080	TCP (HTTPS)	Используется для следующих целей: • подключение через Kaspersky Industrial CyberSecurity for Networks API (в том числе через коннектор KUMA); • подключение Kaspersky Security Center Web Console.
8081	TCP (HTTPS)	Используется для получения данных от EPP-приложений (если на узел Сервера добавлен сервер интеграции).
13000	TCP	Используется для подключения Агента администрирования к Серверу администрирования Kaspersky Security Center.
13520	TCP	Используется для подключений сенсоров.
15000	UDP	Используется для отправки сигналов управления Агенту администрирования от Сервера администрирования Kaspersky Security Center.
Компьютер, выполняющий функции сенсора		
22	TCP (SSH)	Используется для взаимодействия с компьютером для установки компонентов программы.
80	TCP (HTTP)	Используется для подключения через веб-интерфейс.
8081	TCP (HTTPS)	Используется для получения данных от EPP-приложений (если на узел сенсора добавлен сервер интеграции).

Использование скрипта централизованной установки компонентов программы

В этом разделе приведены сведения о возможностях использования скрипта централизованной установки компонентов программы kics4net-deploy-<номер версии программы>.bundle.sh. Вы можете использовать этот скрипт для централизованной установки и удаления Сервера и сенсоров Kaspersky Industrial CyberSecurity for Networks.

Если установка или удаление компонентов программы выполняются с помощью скрипта kics4net-deploy-<номер версии программы>.bundle.sh, применять скрипты локальной установки или локального удаления, входящие в комплект поставки программы, не обязательно.

Централизованная установка компонентов программы

В этой статье описана процедура централизованной установки компонентов программы с помощью скрипта kics4net-deploy-<номер версии программы>.bundle.sh.

Перед централизованной установкой компонентов требуется выполнить действия для подготовки к установке программы.

Скрипт централизованной установки компонентов программы использует данные, сохраненные в файле параметров установки. Для запуска скрипта не требуются root-права для текущей учетной записи на компьютере, с которого будет выполняться установка.

Чтобы централизованно установить компоненты Kaspersky Industrial CyberSecurity for Networks на компьютеры:

1. На компьютере, с которого будет выполняться установка, перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.

2. Введите команду запуска скрипта централизованной установки компонентов программы:

   `bash kics4net-deploy-<номер версии программы>.bundle.sh`

   На экране отобразится меню выбора языка локализации.

3. Выберите язык локализации. В зависимости от версии программы выбранный язык будет использоваться:

   - В версии Kaspersky Industrial CyberSecurity for Networks 4.2 – только для локализации меню централизованной установки программы. Для локализации компонентов Kaspersky Industrial CyberSecurity for Networks вы можете выбрать другой язык после установки Сервера при начальной настройке программы.

   - В версии Kaspersky Industrial CyberSecurity for Networks 4.2.1 – для локализации меню централизованной установки программы и для локализации компонентов Kaspersky Industrial CyberSecurity for Networks. После установки Сервера компоненты программы будут использовать язык локализации, выбранный на этом этапе.

4. В меню выбора варианта установки выберите пункт **Выполнить новую установку**.

   На экране отобразится главное меню централизованной установки.

5. Выполните следующие действия:

   a. С помощью пункта меню **Добавить Сервер** добавьте узел Сервера и настройте основные параметры для этого узла.

   b. Если вы хотите настроить дополнительные параметры для узла Сервера, выберите пункт **Изменить параметры Сервера** и настройте нужные параметры.

   c. При установке Сервера с сенсорами добавьте узлы сенсоров с помощью пункта меню **Добавить сенсор**.

   d. Если вы хотите настроить дополнительные параметры для добавленных узлов сенсоров, выберите пункт **Изменить параметры сенсора** и последовательно настройте нужные параметры для каждого добавленного узла.

   e. С помощью пункта меню **Изменить пользователя, от имени которого выполняется установка** укажите учетную запись пользователя с root-правами, от имени которого будет выполняться централизованная установка компонентов программы. Эта учетная запись будет использоваться на тех узлах, для которых не указана дополнительная учетная запись при настройке дополнительных параметров.

6. По окончании настройки параметров выберите пункт **Сохранить параметры и начать установку**.

   На экране отобразится приглашение для ввода пароля пользователя, от имени которого выполняется установка.

7. Введите пароль пользователя, от имени которого выполняется установка. Пароль требуется ввести дважды: сначала в приглашении `SSH password` и затем в приглашении `BECOME password`.

   Скрипт установки начнет установку компонентов. Во время установки на экране выводятся служебные сообщения о выполняемых операциях.

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh.

После завершения установки компонентов Kaspersky Industrial CyberSecurity for Networks программа не выполняет функции по контролю промышленной сети. Чтобы использовать программу, вам нужно выполнить действия для подготовки программы к работе.

Команды меню централизованной установки

В этой статье приведены сведения об основных командах меню централизованной установки. Меню выводится на экран при запуске скрипта централизованной установки компонентов программы kics4net-deploy-<номер версии программы>.bundle.sh. Этот файл требуется запускать в директории, созданной при подготовке к установке программы.

С помощью меню централизованной установки вы можете создать или изменить конфигурацию параметров установки программы и запустить процедуру установки или удаления компонентов.

Меню установки имеет иерархическую структуру пунктов. На первом уровне представлены пункты главного меню. Для выбора нужного пункта требуется ввести его номер и нажать на клавишу **ENTER**. Если выбранный пункт выполняет переход к другой группе пунктов, на экране появляется вложенное меню.

Пункты меню, которые задают значения параметров, могут иметь значения по умолчанию или ранее заданные значения. Такие значения отображаются в квадратных скобках в конце названия пункта.

Команды в главном меню распределены по группам.

Команды управления установкой Сервера

Для управления установкой Сервера вы можете использовать следующие команды в меню установки:

- **Добавить Сервер** – добавляет новый узел, которому будут назначены функции Сервера. Пункт присутствует, если Сервер еще не добавлен. При выборе этого пункта вам нужно указать основные параметры Сервера при появлении следующих запросов:

  - **Введите IP-адрес узла для установки** – задает IP-адрес, который будет использоваться для подключения к компьютеру по протоколу SSH и установки Сервера.

  - **Добавить функциональность взаимодействия программы с Kaspersky Security Center** – добавляет функциональность, которая позволит использовать Сервер администрирования Kaspersky Security Center для получения лицензионного ключа и загрузки обновлений, а также передавать в Kaspersky Security Center события и состояние программы. Для передачи событий в другие сторонние системы не требуется добавлять эту функциональность.

    Если добавлена функциональность взаимодействия программы с Kaspersky Security Center, при установке программы устанавливается компонент Агент администрирования Kaspersky Security Center. Для этого пакет для установки Агента администрирования должен присутствовать в директории kics4net-release_<номер версии программы>/linux-centos, созданной при подготовке к централизованной установке компонентов.

    > Установка Агента администрирования не выполняется при обнаружении этого компонента, используемого другой программой "Лаборатории Касперского" (чтобы не нарушить взаимодействие этой программы с Сервером администрирования Kaspersky Security Center). При этом функциональность взаимодействия Kaspersky Industrial CyberSecurity for Networks с Kaspersky Security Center может быть доступна не в полном объеме, если версия установленного Агента администрирования отличается от версии этого компонента в комплекте поставки Kaspersky Industrial CyberSecurity for Networks.

  - **Включить синхронизацию времени между Сервером и сенсорами** – включает автоматическую синхронизацию времени Сервера с узлами, на которых установлены сенсоры.

- **Изменить параметры Сервера** – изменяет параметры добавленного Сервера. С помощью этого пункта меню вы можете изменить доступные для изменения основные параметры компонента и настроить дополнительные параметры. После выбора этого пункта появляется вложенное меню, в котором вы можете изменить следующие параметры:

  - **Указать дополнительного пользователя, от имени которого выполняется установка** – задает дополнительную учетную запись пользователя, от имени которого будет выполняться установка на узле Сервера. Дополнительную учетную запись нужно указать, если на этом узле имя пользователя с root-правами отличается от имени пользователя, заданного в пункте **Изменить пользователя, от имени которого выполняется установка**. Пароли всех учетных записей пользователей, от имени которых будет выполняться установка, должны совпадать.

  - **Включить аппаратный таймер наблюдения** – включает использование аппаратного таймера наблюдения. *Аппаратный таймер наблюдения* – это аппаратно реализованная схема контроля над зависанием системы. При наличии на узле аппаратного таймера наблюдения вы можете включить его использование в Kaspersky Industrial CyberSecurity for Networks. Если использование аппаратного таймера наблюдения включено, укажите для него путь в пункте **Указать путь к аппаратному таймеру наблюдения**.

  - **Выключить аппаратный таймер наблюдения** – выключает использование аппаратного таймера наблюдения.

- **Добавить функциональность взаимодействия программы с Kaspersky Security Center** – добавляет функциональность взаимодействия программы с Kaspersky Security Center, если эта функциональность не была добавлена. Этот пункт меню аналогичен пункту **Добавить функциональность взаимодействия программы с Kaspersky Security Center** в меню **Добавить Сервер**.

- **Удалить функциональность взаимодействия программы с Kaspersky Security Center** – удаляет функциональность взаимодействия программы с Kaspersky Security Center.

- **Включить синхронизацию времени между Сервером и сенсорами** – включает автоматическую синхронизацию времени Сервера с узлами, если автоматическая синхронизация не была включена. Этот пункт меню аналогичен пункту **Включить синхронизацию времени между Сервером и сенсорами** в меню **Добавить Сервер**.

- **Выключить синхронизацию времени между Сервером и сенсорами** – выключает автоматическую синхронизацию времени Сервера с узлами.

- **Создать базу данных заново** – удаляет существующую базу данных и создает новую при переустановке программы.

  При выборе этого пункта меню информация в существующей базе данных будет утеряна после установки Сервера.

- **Удалить Сервер** – удаляет узел Сервера.

Команды управления установкой сенсоров

Для управления установкой сенсоров вы можете использовать следующие команды в меню установки:

- **Добавить сенсор** – добавляет новый узел, которому будут назначены функции сенсора. При выборе этого пункта вам нужно указать основные параметры сенсора при появлении запроса **Введите IP-адрес узла для установки**. В запросе вы можете задать IP-адрес, который будет использоваться для подключения к компьютеру по протоколу SSH и установки сенсора.

- **Изменить параметры сенсора** – изменяет параметры добавленного сенсора. С помощью этого пункта меню вы можете изменить доступные для изменения основные параметры сенсора и настроить дополнительные параметры. При выборе этого пункта меню отображается список узлов, на которых добавлены сенсоры. После выбора узла появляется вложенное меню, в котором вы можете изменить следующие параметры:

  - **Указать дополнительного пользователя, от имени которого выполняется установка** – задает дополнительную учетную запись пользователя, от имени которого будет выполняться централизованная установка на узле сенсора. Дополнительную учетную запись нужно указать, если на этом узле имя пользователя с root-правами отличается от имени пользователя, заданного в пункте **Изменить пользователя, от имени которого выполняется установка**. Пароли всех учетных записей пользователей, от имени которых будет выполняться установка, должны совпадать.

  - **Включить аппаратный таймер наблюдения** – включает использование аппаратного таймера наблюдения. *Аппаратный таймер наблюдения* – это аппаратно реализованная схема контроля над зависанием системы. При наличии на узле аппаратного таймера наблюдения вы можете включить его использование в Kaspersky Industrial CyberSecurity for Networks. Если использование аппаратного таймера наблюдения включено, укажите для него путь в пункте **Указать путь к аппаратному таймеру наблюдения**.

- **Удалить сенсор** – удаляет узел сенсора. При выборе этого пункта отображается список узлов, на которых добавлены сенсоры.

Общие команды установки

К общим командам меню установки относятся следующие команды:

- **Изменить пользователя, от имени которого выполняется установка** – задает имя пользователя с root-правами, от имени которого выполняется централизованная установка компонентов программы. На всех компьютерах должен быть задан одинаковый пароль для учетных записей пользователей, от имени которых будет выполняться установка. Пароль запрашивается при установке компонентов.

- **Просмотреть параметры установки программы** – выводит список параметров установки и их значений.

Команды выхода из меню установки

Для выхода из меню централизованной установки вы можете использовать следующие команды:

- **Сохранить параметры и начать установку** – установить компоненты программы Kaspersky Industrial CyberSecurity for Networks в соответствии с заданными параметрами установки. При этом заданные параметры сохраняются в файле параметров установки. Скрипт централизованной установки программы сохраняет файл параметров установки на каждом компьютере, на котором этот скрипт выполняется.

- **Сохранить параметры и выйти без установки** – сохранить изменения в файле параметров установки, завершить работу скрипта централизованной установки программы и не выполнять установку компонентов.

- **Выйти без сохранения параметров** – завершить работу скрипта централизованной установки программы без сохранения изменений в файле параметров установки.

Изменение параметров и централизованная переустановка компонентов программы

Вы можете централизованно выполнить переустановку компонентов Kaspersky Industrial CyberSecurity for Networks. Переустановка компонентов может потребоваться, например, в следующих случаях:

- для добавления нового сенсора;

- для изменения параметров, которые могут быть заданы в меню централизованной установки.

Для централизованной переустановки компонентов программы скрипт kics4net-deploy-<номер версии программы>.bundle.sh использует файл параметров установки, который был сохранен на компьютере. Если на этом компьютере файл параметров установки поврежден или не найден в исходной директории, скрипт централизованной установки программы выполняет поиск копии файла на этом компьютере и на других компьютерах с установленными компонентами программы.

Чтобы централизованно переустановить компоненты Kaspersky Industrial CyberSecurity for Networks:

1. Запустите скрипт централизованной установки программы, выполнив пункты 1–3 процедуры установки.

2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.

   На экране отобразится главное меню централизованной установки.

3. Выполните следующие действия (в зависимости от нужного результата):

   - С помощью пункта меню **Изменить параметры Сервера** укажите нужные параметры Сервера.

     Вы не можете изменить IP-адрес Сервера. Если вы хотите изменить IP-адрес, вам нужно сначала удалить имеющийся Сервер и затем добавить его заново с новым IP-адресом с помощью пункта меню **Добавить Сервер** (этот пункт меню появляется, если Сервер не добавлен).

   - При установке Сервера с сенсорами укажите нужные параметры сенсоров с помощью пункта меню **Изменить параметры сенсора**.

     Вы не можете изменить IP-адрес ранее добавленного сенсора. Если вы хотите изменить IP-адрес, вам нужно сначала удалить имеющийся сенсор и затем добавить его заново с новым IP-адресом с помощью пункта меню **Добавить сенсор**. Вы также можете использовать этот пункт меню для добавления новых сенсоров.

   - С помощью пункта меню **Изменить пользователя, от имени которого выполняется установка** укажите имя пользователя с root-правами, от имени которого будет выполняться централизованная установка компонентов программы на компьютерах. Эта учетная запись будет использоваться на тех узлах, для которых не указана дополнительная учетная запись при настройке дополнительных параметров Сервера или сенсоров.

4. По окончании настройки параметров выберите пункт **Сохранить параметры и начать установку**.

   На экране отобразится приглашение для ввода пароля пользователя, от имени которого выполняется установка.

5. Введите пароль пользователя, от имени которого выполняется установка. Пароль требуется ввести дважды: сначала в приглашении `SSH password` и затем в приглашении `BECOME password`.

   Скрипт установки начнет установку компонентов. Во время установки на экране выводятся служебные сообщения о выполняемых операциях.

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh.

Централизованная установка компонентов программы в неинтерактивном режиме

Вы можете централизованно установить компоненты программы в неинтерактивном режиме, то есть без интерактивного ввода параметров установки. Для неинтерактивной централизованной установки требуется использовать специальные параметры при запуске скрипта централизованной установки компонентов программы kics4net-deploy-<номер версии программы>.bundle.sh.

Для неинтерактивной централизованной установки требуется подготовить файл параметров установки. Вы можете подготовить файл параметров установки с помощью скрипта kics4net-deploy-<номер версии программы>.bundle.sh.

Чтобы подготовить файл параметров централизованной установки с помощью скрипта:

1. Настройте параметры централизованной установки, выполнив пункты 1–5 процедуры установки.

2. Сохраните файл параметров установки с помощью пункта меню **Сохранить параметры и выйти без установки**.

   Файл параметров установки inventory.json сохранится в директории /home/<user>/.config/kaspersky/kics4net-deploy/ (при этом компоненты программы не будут установлены).

3. При необходимости скопируйте файл параметров централизованной установки в другую директорию.

После подготовки файла параметров централизованной установки вы можете централизованно установить компоненты программы в неинтерактивном режиме.

Чтобы централизованно установить компоненты программы в неинтерактивном режиме:

1. На компьютере, с которого будет выполняться централизованная установка, перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.

2. Введите команду:

   `bash kics4net-deploy-<номер версии программы>.bundle.sh --silent-mode`

   где `silent-mode` – параметр включения неинтерактивного режима установки (обязательный параметр).

   Дополнительно к обязательному параметру вы можете указать следующие параметры запуска скрипта установки:

   - `-i <путь к файлу параметров установки>` – указывает полный путь и имя файла параметров централизованной установки. Если параметр не задан, используется файл inventory.json в директории /home/<user>/.config/kaspersky/kics4net-deploy/.

   - `--enable-debug-grpc-server` – устанавливает отладочный gRPC-сервер. Этот gRPC-сервер используется для тестирования и не требуется при нормальном использовании программы.

     Если запуск скрипта выполнен с параметром `--enable-debug-grpc-server`, это приводит к выходу программы из сертифицированного состояния.

   После ввода команды запуска скрипта на экране отобразится приглашение для ввода пароля пользователя, от имени которого выполняется централизованная установка.

3. Введите пароль пользователя, от имени которого выполняется централизованная установка. Пароль требуется ввести дважды: сначала в приглашении `SSH password` и затем в приглашении `BECOME password`.

   Скрипт централизованной установки начнет установку компонентов. Во время установки на экране выводятся служебные сообщения о выполняемых операциях.

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh.

Усиление защиты компьютеров с установленными компонентами программы

После установки Kaspersky Industrial CyberSecurity for Networks рекомендуется усилить защиту операционных систем на компьютерах с установленными компонентами программы. Для усиления защиты вы можете использовать скрипт централизованной установки компонентов программы kics4net-deploy-<номер версии программы>.bundle.sh или скрипт для локального запуска kics4net-harden.sh, который находится на компьютере с установленным компонентом программы в директории /opt/kaspersky/kics4net/sbin/.

С помощью скрипта вы можете выполнить следующие действия:

- включить запрет запуска сервисов операционной системы, которые не требуются для работы компонентов программы (например, avahi-daemon и cups);
- изменить параметры сетевой конфигурации, влияющие на защищенность операционной системы (например, включить запрет обработки сетевых пакетов перенаправления по протоколу ICMP).

Скрипт централизованной установки компонентов программы выполняет действия по усилению защиты на всех компьютерах, на которых установлены компоненты программы.

Для усиления защиты скрипт использует файл параметров централизованной установки, который был сохранен на компьютере. Если на этом компьютере файл параметров централизованной установки поврежден или не найден в исходной директории, скрипт выполняет поиск копии файла на этом компьютере и на других компьютерах с установленными компонентами программы.

Чтобы усилить защиту компьютеров с помощью скрипта kics4net-deploy-<номер версии программы>.bundle.sh:

1. На компьютере, с которого выполнялась централизованная установка, перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.

2. Введите команду:

   `bash kics4net-deploy-<номер версии программы>.bundle.sh --harden <параметр>`

   где `<параметр>` – один из следующих параметров запуска:

   - `-s` – параметр для включения запрета запуска сервисов операционной системы;
   - `-n` – параметр для изменения параметров сетевой конфигурации;
   - `-a` – параметр для включения запрета запуска сервисов операционной системы и изменения параметров сетевой конфигурации.

3. В приглашениях `SSH password` и `BECOME password` введите пароль учетной записи пользователя, от имени которого выполняется централизованная установка.

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh. При успешном завершении на экране отобразится информация о выполненных действиях на компьютерах с установленными компонентами программы.

Централизованное удаление компонентов программы

Удаление компонентов Kaspersky Industrial CyberSecurity for Networks может выполняться централизованно с помощью скрипта kics4net-deploy-<номер версии программы>.bundle.sh. Этот скрипт позволяет удалять компоненты программы на узлах Сервера и сенсоров по отдельности или полностью удалить программу как текущей версии, так и предыдущих версий (начиная с версии 2.0).

Для удаления компонентов скрипт kics4net-deploy-<номер версии программы>.bundle.sh использует файл параметров централизованной установки, который был сохранен на компьютере. Если на этом компьютере файл параметров централизованной установки поврежден или не найден в исходной директории, скрипт установки программы выполняет поиск копии файла на этом компьютере и на других компьютерах с установленными компонентами программы.

Чтобы централизованно удалить компоненты программы на отдельных узлах:

1. Запустите скрипт централизованной установки компонентов программы, выполнив пункты 1–3 процедуры установки.
2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.

   На экране отобразится главное меню централизованной установки.
3. Выполните следующие действия (в зависимости от нужного результата):

   - С помощью пункта меню **Удалить Сервер** удалите узел Сервера.

     После удаления узла Сервера нужно добавить другой узел Сервера, чтобы обеспечить работоспособность программы.

   - С помощью пункта меню **Удалить сенсор** удалите узел сенсора (если в программу добавлено несколько сенсоров, выберите нужный узел в списке узлов с добавленными сенсорами).
4. По окончании настройки параметров выберите пункт **Сохранить параметры и начать установку**.
5. В приглашениях `SSH password` и `BECOME password` введите пароль учетной записи пользователя, от имени которого выполняется централизованное удаление компонентов программы.

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh.

Чтобы полностью удалить программу:

1. Запустите скрипт централизованной установки компонентов программы, выполнив пункты 1–3 процедуры установки.
2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.

   На экране отобразится главное меню централизованной установки
3. С помощью пункта меню **Удалить Сервер** удалите узел Сервера.

4. Если в программу добавлены сенсоры, с помощью пункта меню **Удалить сенсор** последовательно удалите все узлы сенсоров.

5. С помощью пункта меню **Параметры удаления** настройте дополнительные параметры централизованного удаления. При выборе этого пункта выводятся следующие запросы:

   - **Удалить программу вместе с данными (y/n)?** Если вы хотите удалить все данные, сохраненные программой в системе, введите символ `y`. Если удалять данные не требуется, введите символ `n`.

   - **Удалить Агент администрирования (y/n)?** Если вы хотите удалить компонент Kaspersky Security Center Агент администрирования, введите символ `y`. Если удалять этот компонент не требуется, введите символ `n`. Запрос выводится при обнаружении установленного Агента администрирования.

6. Выберите пункт **Сохранить параметры и начать установку**.

7. В приглашениях `SSH password` и `BECOME password` введите пароль пользователя, от имени которого выполняется централизованное удаление.

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh.

При удалении Kaspersky Industrial CyberSecurity for Networks не происходит автоматическое удаление скопированных и распакованных файлов из комплекта поставки. При необходимости эти файлы можно удалить вручную.

Использование скрипта локальной установки компонентов программы

В этой статье описана процедура локальной установки компонента программы (Сервера или сенсора) на компьютере с помощью скрипта kics4net-install.sh.

Перед локальной установкой компонентов требуется выполнить действия для подготовки к установке программы.

Скрипт локальной установки компонентов программы может установить на компьютере только один из компонентов: Сервер или сенсор. Если на компьютере уже установлен компонент программы (например, Сервер), на этом компьютере невозможно установить компонент другого типа (в приведенном примере невозможно установить сенсор). При попытке установить на компьютер компонент того же типа, скрипт локальной установки выполняет переустановку компонента.

При установке Сервера автоматически устанавливается компонент Агент администрирования Kaspersky Security Center. Для этого пакет для установки Агента администрирования должен присутствовать в директории kics4net-release_<номер версии программы>/linux-centos, созданной при подготовке к локальной установке.

Установка Агента администрирования Kaspersky Security Center не выполняется при обнаружении этого компонента, используемого другой программой "Лаборатории Касперского" (чтобы не нарушить взаимодействие этой программы с Сервером администрирования Kaspersky Security Center). При этом функциональность взаимодействия Kaspersky Industrial CyberSecurity for Networks с Kaspersky Security Center может быть доступна не в полном объеме, если версия установленного Агента администрирования отличается от версии этого компонента в комплекте поставки Kaspersky Industrial CyberSecurity for Networks.

Чтобы локально установить Сервер Kaspersky Industrial CyberSecurity for Networks:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить скрипт локальной установки.

2. Перейдите в директорию с файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.

3. Введите команду запуска локальной установки Сервера:

   ```
   bash kics4net-install.sh --server
   ```

   где `server` – параметр включения режима установки Сервера (обязательный параметр).

   Дополнительно вы можете указать следующие параметры запуска скрипта установки:

   `--product-language=< язык >` – указывает язык для локализации компонентов программы. Параметр поддерживается в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1. Для параметра предусмотрены следующие значения:

   - `english` – английский язык;
   - `russian` – русский язык;
   - `chinese-simplified` – упрощенный китайский язык.

   `--enable-debug-grpc-server` – устанавливает отладочный gRPC-сервер. Этот gRPC-сервер используется для тестирования и не требуется при нормальном использовании программы.

   Если запуск скрипта выполнен с параметром `--enable-debug-grpc-server`, это приводит к выходу программы из сертифицированного состояния.

4. При установке Сервера версии Kaspersky Industrial CyberSecurity for Networks 4.2.1: если команда запуска была введена без параметра `--product-language=< язык >`, перед началом процесса установки на экране отобразится меню выбора языка локализации. В этом случае введите номер нужного языка и нажмите на клавишу **ENTER**.

   Скрипт начнет установку компонента. Во время установки на экране выводятся служебные сообщения о выполняемых операциях.

Дождитесь завершения работы скрипта kics4net-install.sh.

Чтобы локально установить сенсор Kaspersky Industrial CyberSecurity for Networks:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить скрипт локальной установки.

2. Перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.

3. Введите команду запуска локальной установки сенсора:

   `bash kics4net-install.sh --sensor`

   где `sensor` – параметр включения режима установки сенсора (обязательный параметр).

   Скрипт начнет установку компонента. Во время установки на экране выводятся служебные сообщения о выполняемых операциях.

Дождитесь завершения работы скрипта kics4net-install.sh.

Использование скрипта локального удаления компонентов программы

В этой статье описана процедура локального удаления компонента программы (Сервера или сенсора) на компьютере с помощью скрипта kics4net-remove.sh.

Чтобы локально удалить компонент Kaspersky Industrial CyberSecurity for Networks на компьютере:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить скрипт локального удаления.

2. Перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.

3. Введите команду запуска скрипта локального удаления компонентов программы:

   - Если вы хотите удалить установленные файлы компонента и все данные, сохраненные программой в системе, введите команду:

     `bash kics4net-remove.sh --full`

   - Если вы хотите удалить только установленные файлы компонента, введите команду:

     `bash kics4net-remove.sh`

   Скрипт начнет удаление компонента. Во время удаления на экране выводятся служебные сообщения о выполняемых операциях.

Дождитесь завершения работы скрипта kics4net-remove.sh.

Установка плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center

Плагин управления Kaspersky Industrial CyberSecurity for Networks позволяет использовать функции Kaspersky Security Center для работы с Kaspersky Industrial CyberSecurity for Networks. В зависимости от версии Kaspersky Security Center и от действий, которые вы хотите выполнять с помощью Kaspersky Security Center, вы можете установить следующие плагины управления:

- Плагин управления для Консоли администрирования на основе консоли Microsoft Management Console (MMC) – этот плагин предназначен для использования в Kaspersky Security Center Windows.

  Установку плагина управления для Консоли администрирования на основе MMC требуется выполнить локально на том компьютере, где установлен Сервер администрирования Kaspersky Security Center. Для установки вам нужно использовать файл из комплекта поставки Kaspersky Industrial CyberSecurity for Networks. Описание предусмотренных процедур установки плагина приведено в этой статье.

- Веб-плагин управления для Kaspersky Security Center Web Console – этот плагин предназначен для использования в Kaspersky Security Center Linux, а также для реализации расширенных возможностей централизованного контроля и использования технологии единого входа в Kaspersky Security Center Windows.

  Установку и обновление веб-плагина управления для Kaspersky Security Center Web Console вы можете выполнять различными способами, доступными в интерфейсе Kaspersky Security Center Web Console.

Перед установкой плагина управления для Консоли администрирования на основе MMC вам нужно скопировать на компьютер с установленным Сервером администрирования файл kics4net-sc-plugin_<номер версии плагина>_<код локализации>.msi из архива комплекта поставки программы. Используйте файл с кодом локализации, который соответствует языку локализации Kaspersky Security Center. Вы можете скопировать файл из директории с распакованными файлами архива kics4net-release_<номер версии программы>.tar.gz на компьютере, на котором выполнялась подготовка к установке программы. После распаковки архива файлы для установки плагинов управления находятся во вложенной директории kics4net-release_<номер версии программы>/sc_plugin.

Вы можете установить плагин управления для Консоли администрирования на основе MMC одним из следующих способов:

- с помощью мастера;
- из командной строки.

Установку плагина управления нужно выполнять под учетной записью, которая входит в группу локальных администраторов.

Чтобы установить плагин управления с помощью мастера:

1. На компьютере, где установлен Сервер администрирования Kaspersky Security Center, запустите файл kics4net-sc-plugin_<номер версии плагина>_<код локализации>.msi.

   После завершения подготовительных действий запустится мастер установки плагина.

2. Следуйте указаниям мастера установки. При появлении запроса на внесение изменений со стороны контроля учетных записей Windows (User Account Control, UAC) нажмите на кнопку **Да** и при необходимости введите учетные данные локального администратора.

По окончании работы мастера установки плагин управления Kaspersky Industrial CyberSecurity for Networks появится в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center (окно свойств Сервера администрирования в Консоли администрирования на основе MMC, раздел **Дополнительно → Информация об установленных плагинах управления программами**).

Чтобы установить плагин управления из командной строки:

1. На компьютере, где установлен Сервер администрирования Kaspersky Security Center, откройте интерфейс командной строки.

2. Перейдите к папке, в которой находится файл kics4net-sc-plugin_<номер версии плагина>_<код локализации>.msi.

3. В командной строке введите команду:

   `msiexec /package kics4net-sc-plugin_<номер версии плагина>_<код локализации>.msi`

   После завершения подготовительных действий запустится мастер установки плагина.

4. Следуйте указаниям мастера установки. При появлении запроса на внесение изменений со стороны контроля учетных записей Windows (User Account Control, UAC) нажмите на кнопку **Да** и при необходимости введите учетные данные локального администратора.

По окончании работы мастера установки плагин управления Kaspersky Industrial CyberSecurity for Networks появится в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center (окно свойств Сервера администрирования в Консоли администрирования на основе MMC, раздел **Дополнительно → Информация об установленных плагинах управления программами**).

При работе с интерфейсом командной строки вы можете использовать другие стандартные параметры запуска программы установки плагина, предусмотренные для установщика Windows. Например, при необходимости вы можете удалить плагин управления с помощью соответствующего параметра запуска. Для получения сведений о предусмотренных параметрах запуска введите команду `kics4net-sc-plugin_<номер версии плагина>_<код локализации>.msi /help`.

Обновление с использованием скрипта переноса данных

Вы можете обновить предыдущую версию Kaspersky Industrial CyberSecurity for Networks с использованием скрипта переноса данных kics4net-backup.sh из комплекта поставки программы текущей (новой) версии. Возможность обновления на текущую версию с использованием скрипта kics4net-backup.sh поддерживается для версий программы, начиная с версии 4.0.

Скрипт kics4net-backup.sh позволяет перенести следующие данные из предыдущей версии программы:

- политика безопасности;
- данные о состоянии и режимах работы технологий и методов;
- параметры обновления баз и программных модулей;
- информация о добавленном лицензионном ключе;
- записи аудита;
- сообщения программы;
- риски категории Уязвимость;
- зарегистрированные события;
- сохраненный трафик для событий;
- данные карты сети.

Вы также можете использовать скрипт kics4net-backup.sh для создания резервной копии данных текущей версии программы. Дополнительно к данным, перечисленным выше, скрипт позволяет сохранить в резервной копии следующие данные:

- данные об исполняемых файлах;
- данные о компьютере узла с установленным компонентом программы:
  - конфигурация сервисов программы;
  - имя компьютера;
  - номер версии программы.

Скрипт kics4net-backup.sh может использоваться для создания резервной копии данных и загрузки данных из резервной копии локально на том компьютере, на котором запущен этот скрипт. Поэтому как для создания резервной копии данных, так и для загрузки данных из резервной копии, вам нужно последовательно запустить скрипт на каждом компьютере с установленным компонентом программы. Порядок работы с компьютерами Сервера и сенсоров для создания резервной копии данных и затем для загрузки данных из резервной копии может быть любым: вы можете сначала запускать скрипт на компьютере Сервера и затем на компьютерах сенсоров или наоборот.

Сценарий обновления предыдущей версии программы с использованием скрипта kics4net-backup.sh состоит из следующих этапов:

1. **Создание резервной копии данных от предыдущей версии программы на компьютерах Сервера и сенсоров**

   Для создания резервной копии данных от предыдущей версии программы вам нужно выполнить следующие действия на каждом компьютере с установленными компонентами программы:

   1. На компьютер с установленным компонентом программы предыдущей версии скопируйте в произвольную директорию архив kics4net-release_<номер версии программы>.tar.gz из комплекта поставки программы текущей (новой) версии.

   2. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки архива:

      `tar -zxvf kics4net-release_<номер версии программы>.tar.gz`

      Распакованные директории и файлы появятся во вложенной директории kics4net-release_<номер версии программы>.

   3. Перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.

   4. Запустите скрипт kics4net-backup.sh:

      - Если вы хотите создать резервную копию данных на компьютере Сервера, введите команду:

        `sudo bash kics4net-backup.sh -b -p <путь к файлу резервной копии> <необязательные параметры>`

      - Если вы хотите создать резервную копию данных на компьютере сенсора, введите команду:

        `sudo bash kics4net-backup.sh -s -p <путь к файлу резервной копии> <необязательные параметры>`

      где:

      - `-b` – параметр для включения режима записи данных Сервера в файл резервной копии (обязательный параметр при запуске на компьютере Сервера).
      - `-p` – параметр, указывающий полный путь и имя файла создаваемой резервной копии (обязательный параметр).
      - `-s` – параметр для включения режима записи данных сенсора в файл резервной копии (обязательный параметр при запуске на компьютере сенсора).
      - `<необязательные параметры>` – один или несколько необязательных параметров, перечисленных ниже.

      Вы можете использовать следующие необязательные параметры в команде запуска скрипта для создания файла резервной копии:

      - `-t` – параметр для выключения сохранения трафика (если параметр не указан, трафик сохраняется).
      - `-e` – параметр для выключения сохранения зарегистрированных событий (если параметр не указан, события сохраняются). Вы можете указать этот параметр только при создании резервной копии данных на компьютере Сервера.

- `-n` – параметр для выключения сохранения данных карты сети (если параметр не указан, данные карты сети сохраняются). Вы можете указать этот параметр только при создании резервной копии данных на компьютере Сервера.

- `-x` – параметр для выключения сохранения данных об исполняемых файлах (если параметр не указан, данные об исполняемых файлах сохраняются). Вы можете указать этот параметр только при создании резервной копии данных на компьютере Сервера.

- `-d` – параметр для остановки сервисов программы (если параметр не указан, происходит запуск сервисов программы после завершения работы скрипта).

> В качестве необязательного параметра для команды запуска скрипта предусмотрен также параметр `-f`, который предназначен для создания резервной копии данных текущей версии программы и сохранения всех доступных данных узла. Если указан этот параметр, сохраненные данные можно будет загрузить в полном объеме только на этом же узле.

Пример:
```
sudo bash kics4net-backup.sh -b -p ./old_kics4net_data -t
```

Скрипт начнет резервное копирование данных. Дождитесь завершения работы скрипта kics4net-backup.sh и сохраните созданный файл резервной копии.

2. **Удаление предыдущей версии программы**

   Этот этап выполняется, если вы хотите установить компоненты текущей версии программы на те же узлы, на которых установлены компоненты предыдущей версии.

   Если Сервер или сенсор текущей версии будет установлен на отдельный компьютер (не на узел с компонентом предыдущей версии), вам нужно скопировать созданный файл резервной копии на этот компьютер.

   Удаление компонентов предыдущей версии программы можно выполнить следующими способами:

   - Централизованно на всех узлах, на которых выполнялась установка предыдущей версии программы.

     Этот способ выполняется с помощью скрипта централизованной установки компонентов программы путем выполнения процедуры централизованного удаления.

   - Локально на каждом узле, на котором установлен компонент предыдущей версии программы.

     Этот способ выполняется с помощью скрипта локального удаления компонентов программы (если компонент предыдущей версии программы предусматривает возможности локальной установки и локального удаления).

   После удаления компонентов предыдущей версии программы убедитесь, что компьютеры удовлетворяют аппаратным и программным требованиям для установки текущей версии. При необходимости установите соответствующую версию операционной системы и подготовьте аппаратное и программное обеспечение на компьютерах.

3. **Установка текущей версии Kaspersky Industrial CyberSecurity for Networks и частичная подготовка программы к работе**

   На этом этапе вам нужно установить компоненты текущей версии Kaspersky Industrial CyberSecurity for Networks. Для этого вы можете выполнить процедуру централизованной установки или установить компоненты с помощью скрипта локальной установки компонентов программы.

   После установки компонентов вам нужно частично подготовить программу к работе, выполнив этапы 1–4 из описания процесса подготовки.

При добавлении точек мониторинга на те же сетевые интерфейсы, которые использовались в предыдущей версии программы, рекомендуется указать имена точек мониторинга, совпадающие с именами точек мониторинга в предыдущей версии программы. Это позволит сохранить привязку событий к новым точкам мониторинга при загрузке данных из резервной копии (иначе ненайденные имена старых точек мониторинга будут помечены в событиях как удаленные).

4 Загрузка данных из резервной копии после установки новой версии программы

Для загрузки данных из созданных файлов резервных копий вам нужно выполнить следующие действия на каждом компьютере с установленным компонентом программы:

1. На компьютере с установленным компонентом программы текущей версии перейдите в директорию, в которой находится скрипт kics4net-backup.sh. Вы можете перейти в ту же директорию, в которую был выполнен переход при выполнении этапа 1, или перейти в директорию /opt/kaspersky/kics4net/sbin/.

2. Запустите скрипт kics4net-backup.sh:

   - Если вы хотите загрузить данные из резервной копии на компьютере Сервера, введите команду:

     `sudo bash kics4net-backup.sh -r -p <путь к файлу резервной копии> <необязательный параметр>`

   - Если вы хотите загрузить данные из резервной копии на компьютере сенсора, введите команду:

     `sudo bash kics4net-backup.sh -l -p <путь к файлу резервной копии> <необязательный параметр>`

   где:

   - `-r` – параметр для включения режима чтения и загрузки данных из файла резервной копии Сервера (обязательный параметр при запуске на компьютере Сервера).
   - `-p` – параметр, указывающий полный путь и имя файла резервной копии (обязательный параметр).
   - `-l` – параметр для включения режима чтения и загрузки данных из файла резервной копии сенсора (обязательный параметр при запуске на компьютере сенсора).
   - `<необязательный параметр>` – параметр `-d` для остановки сервисов программы (если параметр не указан, происходит запуск сервисов программы после завершения работы скрипта).

   В качестве необязательного параметра для команды запуска скрипта предусмотрен также параметр `-f`, который предназначен для восстановления всех доступных данных узла из резервной копии данных текущей версии программы (если резервная копия получена на этапе 1 данного сценария с помощью параметра `-f`). При этом восстановление всех данных в полном объеме возможно только при загрузке из резервной копии на том же узле, на котором эти данные были сохранены.

Для специфических сценариев использования скрипта kics4net-backup.sh предусмотрен дополнительный параметр команды запуска `--restore-database`. Этот параметр предназначен для восстановления из файла резервной копии только базы данных Сервера. В сценарии обновления предыдущей версии программы этот параметр не используется. Чтение и загрузку данных из файла резервной копии Сервера, включающих и данные для восстановления базы данных, обеспечивает параметр `-r` (см. выше).

Пример:
```
sudo bash kics4net-backup.sh -r -p ./old_kics4net_data
```

Скрипт начнет загрузку данных из файла резервной копии в программу. Дождитесь завершения работы скрипта kics4net-backup.sh.

После завершения загрузки данных из резервных копий на всех узлах подключитесь к Серверу через веб-интерфейс и проверьте параметры развертывания узлов в разделе **Параметры** → **Развертывание**. При необходимости добавьте сенсоры.

Установка обновленной версии программы с патчем

При определенных условиях специалисты "Лаборатории Касперского" могут подготавливать обновленные файлы программы с примененными *патчами*. Патчи предназначены для дополнения или исправления функциональности программы в случаях, когда такие изменения невозможно применить с помощью обновления баз и программных модулей.

Обновленные файлы программы с примененным патчем (далее также "обновленные файлы программы") поставляются в виде архива, аналогичного архиву из комплекта поставки программы.

Если компоненты программы еще не были установлены на компьютерах, вы можете использовать для установки программы архив с обновленными файлами программы так же, как и архив из комплекта поставки. Для этого при выполнении действий по подготовке к установке программы распакуйте архив с обновленными файлами программы, а не архив из комплекта поставки. Все остальные действия для установки компонентов вы можете выполнять так же, как и при использовании архива из комплекта поставки.

Если компоненты программы текущей версии уже установлены на компьютерах, для установки обновленных файлов программы с патчем вам нужно использовать скрипт установки патчей kics4net-install-patch.sh. Скрипт kics4net-install-patch.sh позволяет заменить установленные компоненты программы текущей версии на компоненты программы обновленной версии с переносом данных, накопленных программой текущей версии. Если при замене установленных компонентов возникла ошибка, скрипт выполняет откат установки обновленных файлов программы и возвращает программу в то состояние, в котором она была на момент запуска скрипта.

При замене установленных компонентов программы текущей версии на компоненты программы обновленной версии скрипт kics4net-install-patch.sh позволяет перенести следующие накопленные данные:

- политика безопасности;
- данные о состоянии и режимах работы технологий и методов;
- параметры обновления баз и программных модулей;
- информация о добавленном лицензионном ключе;
- записи аудита;
- сообщения программы;
- риски категории Уязвимость;
- зарегистрированные события;
- сохраненный трафик для событий;

- данные карты сети;
- файлы дампа трафика.

Скрипт kics4net-install-patch.sh входит в комплект поставки программы, а также находится в архиве с обновленными файлами программы.

Вы можете применять скрипт kics4net-install-patch.sh для установки обновленных файлов программы текущей версии, а также для версий программы, начиная с версии 4.1 (при условии совместимости обновленных файлов программы с установленными версиями операционной системы и Kaspersky Industrial CyberSecurity for Networks).

Скрипт kics4net-install-patch.sh выполняет установку обновленных файлов программы локально на том компьютере, на котором запущен этот скрипт. Поэтому для обновления всех компонентов программы (Сервера и сенсоров) вам нужно последовательно запустить скрипт kics4net-install-patch.sh на каждом компьютере с установленным компонентом программы. Порядок обновления компонентов может быть любым: вы можете сначала обновить файлы программы на компьютере Сервера и затем на компьютерах сенсоров или наоборот.

Чтобы установить обновленные файлы программы на компьютере Сервера или сенсора Kaspersky Industrial CyberSecurity for Networks:

1. Подготовьте директорию, в которой будут находиться старые файлы из архива, использовавшегося в предыдущий раз (для установки компонентов или для последнего обновления файлов программы).

   Если директория со старыми распакованными файлами уже есть на компьютере (например, директория не была удалена после локальной установки компонента), вы можете использовать эту директорию для дальнейших действий. Если директория отсутствует, для ее подготовки выполните следующие действия:

   a. Скопируйте в произвольную директорию архив, который использовался в предыдущий раз (для установки компонентов или для последнего обновления файлов программы).

   b. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки архива:

      `tar -zxvf <имя файла архива>`

      Распакованные директории и файлы появятся во вложенной директории, имя которой совпадает с именем файла архива.

   В описании дальнейших действий эта подготовленная директория указана как *директория со старыми файлами*.

2. Подготовьте директорию, в которой будут находиться новые распакованные файлы из полученного архива с обновленными файлами программы.

   Для подготовки директории выполните следующие действия:

   a. Скопируйте на компьютер полученный архив с обновленными файлами программы.

   b. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки архива:

      `tar -zxvf <имя файла архива>`

      Распакованные директории и файлы появятся во вложенной директории, имя которой совпадает с именем файла архива.

   В описании дальнейших действий эта подготовленная директория указана как *директория с новыми файлами*.

3. В директории с новыми файлами перейдите во вложенную директорию <имя файла архива>/linux-centos. Эта директория содержит файлы скриптов и пакетов для установки, проверки и удаления компонентов программы.

4. Запустите скрипт kics4net-install-patch.sh:

   - Если вы хотите установить обновленные файлы программы на компьютере Сервера, введите команду:

     ```
     sudo bash kics4net-install-patch.sh -o <путь к директории со старыми файлами>/linux-centos -n <путь к директории с новыми файлами>/linux-centos -b <путь к директории для резервной копии> --backup-traffic
     ```

   - Если вы хотите установить обновленные файлы программы на компьютере сенсора, введите команду:

     ```
     sudo bash kics4net-install-patch.sh -s -o <путь к директории со старыми файлами>/linux-centos -n <путь к директории с новыми файлами>/linux-centos -b <путь к директории для резервной копии> --backup-traffic
     ```

   где:

   - `-o` – параметр, указывающий полный путь к директории, которая содержит файлы скриптов и пакетов для установки, проверки и удаления компонентов программы в директории со старыми файлами (обязательный параметр).

   - `-n` – параметр, указывающий полный путь к директории, которая содержит файлы скриптов и пакетов для установки, проверки и удаления компонентов программы в директории с новыми файлами (обязательный параметр).

   - `-b` – параметр, указывающий полный путь к директории для создания резервной копии (по умолчанию скрипт создает резервную копию во временной директории и автоматически удаляет созданные файлы при успешном завершении установки обновленных файлов программы или в случае отката установки из-за возникшей ошибки в процессе работы скрипта).

     Рекомендуется использовать этот параметр для сохранения резервной копии в нужной директории независимо от результатов работы скрипта kics4net-install-patch.sh. Также, если в программе накоплен большой объем данных, с помощью параметра `-b` вы можете указать монтированную директорию на другом жестком диске, чтобы избежать переполнения системного (корневого) раздела.

   - `--backup-traffic` – параметр для добавления в резервную копию файлов дампа трафика с последующим восстановлением этих файлов по окончании установки обновленных файлов программы (по умолчанию файлы дампа трафика не копируются в директорию для резервной копии, однако эти файлы останутся в исходном размещении и будут доступны для использования при успешном завершении установки). Параметр позволяет автоматически восстановить файлы дампа трафика в случае отката установки обновленных файлов программы из-за возникшей ошибки в процессе работы скрипта kics4net-install-patch.sh.

     Рекомендуется использовать этот параметр, если вам важно сохранить файлы дампа трафика и есть риск возникновения ошибок при установке обновленных файлов программы. Обычно директория, в которой программа хранит файлы дампа трафика, занимает большое пространство на диске. При использовании параметра `--backup-traffic` скрипт kics4net-install-patch.sh копирует эти файлы в директорию для резервной копии, что может потребовать значительного дополнительного пространства на диске. Также может существенно увеличиться время работы скрипта.

- `-s` – параметр включения режима установки обновленных файлов сенсора (применяется при запуске скрипта kics4net-install-patch.sh на компьютере сенсора).

  Пример:
  ```
  sudo bash kics4net-install-patch.sh -o /tmp/kics4net-release_< номер версии программы >/linux-centos -n
  /tmp/kics4net-patch1_< номер версии программы >/linux-centos -b ./old_kics4net_data --backup-traffic
  ```

Скрипт начнет установку обновленных файлов программы. Дождитесь завершения работы скрипта kics4net-install-patch.sh.

Чтобы просмотреть версию программы на Сервере и начать работу с программой после установки обновленных файлов:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс. Для подключения используйте IP-адрес компьютера Сервера.
2. Выберите раздел **О программе** и просмотрите версию программы, установленную на Сервере.
3. Выберите раздел **Начальная настройка**.
4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности. Для этого последовательно откройте документы по соответствующим ссылкам в названиях флажков **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **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 условия Политики конфиденциальности**.
5. Если вы полностью согласны с условиями Лицензионного соглашения и Политики конфиденциальности, то установите оба флажка.

   Если вы не согласны с условиями Лицензионного соглашения и/или Политики конфиденциальности, то закройте страницу веб-интерфейса и удалите установленные компоненты программы на компьютерах.

6. Нажмите на кнопку **Продолжить**.

Подготовка программы к работе

После установки компонентов Kaspersky Industrial CyberSecurity for Networks вам нужно подготовить программу к работе. Процесс подготовки состоит из следующих основных этапов:

1. **Начальная настройка программы**

   На этом этапе выполняется настройка основных параметров программы после установки Сервера. После выполнения этого этапа Сервер будет доступен для подключения и работы с программой через веб-интерфейс.

2. **Добавление и подключение сенсоров**

   Этот этап выполняется для способа установки Сервера и внешних сенсоров. После выполнения этого этапа узлы с установленными сенсорами будут готовы к дальнейшей настройке.

3. **Добавление точек мониторинга**

На этом этапе добавляются точки мониторинга на узлах с установленными компонентами программы. После выполнения этого этапа программа начинает анализировать трафик, поступающий из сегментов промышленной сети на сетевые интерфейсы с точками мониторинга.

4. **Добавление пользователей программы**

   На этом этапе создаются учетные записи пользователей программы в дополнение к учетной записи, созданной при начальной настройке программы. После выполнения этого этапа в программе будет несколько учетных записей пользователей, с помощью которых вы сможете разграничить доступ к функциям программы и контролировать выполняемые действия по записям аудита.

5. **Добавление лицензионного ключа**

   На этом этапе выполняется добавление в программу лицензионного ключа для активации соответствующей функциональности программы. После выполнения этого этапа вы сможете настроить и использовать функциональность обновления баз и программных модулей. Также, если лицензионный ключ активирует функциональность аудита безопасности, вы сможете использовать эту функциональность.

6. **Настройка обновления баз и программных модулей**

   После выполнения этого этапа вы сможете устанавливать обновления баз и программных модулей.

7. **Настройка контроля активов**

   На этом этапе формируются списки известных программе устройств. В некоторых случаях может потребоваться настройка адресных пространств. После выполнения этого этапа в программе будет настроено отслеживание нужных устройств в промышленной сети.

8. **Настройка контроля процесса**

   На этом этапе в программе настраиваются параметры устройств для контроля технологического процесса. После выполнения этого этапа вы сможете контролировать с помощью программы параметры технологического процесса (в том числе с помощью правил) и отслеживать передаваемые системные команды.

9. **Настройка контроля взаимодействий**

   На этом этапе в программе формируются правила для определения разрешенных и неразрешенных сетевых взаимодействий. После выполнения этого этапа в программе будут настроены правила, разрешающие взаимодействия между определенными устройствами и системные команды (правила, по которым программа не регистрирует события).

10. **Настройка обнаружения вторжений**

    Этот этап выполняется для настройки обнаружения вторжений с помощью программы. После выполнения этого этапа вы сможете использовать правила обнаружения вторжений (как встроенные, так и дополнительно загруженные в программу) и отслеживать аномалии трафика с признаками атак.

11. **Настройка аудита безопасности устройств**

    Этот этап выполняется для аудита безопасности контролируемых устройств с помощью Kaspersky Industrial CyberSecurity for Networks. После выполнения этого этапа в программе появляются возможности оценивать соответствие устройств стандартам безопасности и получать наиболее точную и полную информацию об устройствах и их конфигурациях с помощью заданий аудита безопасности.

Начальная настройка программы после установки Сервера

После установки Сервера, выполненной с помощью скрипта централизованной установки или другим способом, программа ожидает завершения начальной настройки. Завершить начальную настройку может любой пользователь, подключившийся к Серверу через веб-интерфейс.

Чтобы выполнить начальную настройку программы после установки Сервера:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс. Для подключения используйте IP-адрес компьютера Сервера.

2. Выберите раздел **Начальная настройка**.

3. Выберите язык локализации. Для этого выполните одно из следующих действий в зависимости от версии программы:

   - В версии Kaspersky Industrial CyberSecurity for Networks 4.2 – в поле **Язык локализации программы** выберите язык локализации компонентов Kaspersky Industrial CyberSecurity for Networks (и данных, которые предоставляют эти компоненты). Выбранный язык будет использоваться компонентами до удаления или переустановки программы.

   - В версии Kaspersky Industrial CyberSecurity for Networks 4.2.1 – в поле **Язык веб-интерфейса** выберите язык веб-интерфейса программы. В дальнейшем вы можете выбирать другой язык веб-интерфейса в основном режиме работы программы.

4. В блоке параметров **Учетная запись Администратора** задайте имя и пароль учетной записи первого пользователя программы. Этому пользователю будет назначена роль Администратор. Для этого пользователя не требуется регистрация в качестве учетной записи операционной системы компьютера Сервера или другого компьютера.

   В качестве имени учетной записи вы можете ввести произвольное имя с использованием прописных и строчных букв латинского алфавита, цифр, точки, а также специальных символов: _ и - (например, Admin_1). Имя должно содержать от 3 до 20 символов, начинаться с буквы и заканчиваться любым поддерживаемым символом, кроме точки.

   Пароль должен удовлетворять следующим требованиям:

   - содержит от 8 до 256 символов ASCII;
   - содержит одну или несколько прописных букв латинского алфавита;
   - содержит одну или несколько строчных букв латинского алфавита;
   - содержит одну или несколько цифр;
   - содержит не более трех одинаковых символов подряд.

5. В поле **Сервер программы** введите имя Сервера в составе решения Kaspersky Industrial CyberSecurity.

   Имя Сервера должно быть уникальным (не совпадать с именами сенсоров на других узлах) и может содержать не более 100 символов. Вы можете использовать буквы латинского алфавита, цифры, пробел, а также специальные символы _ и - (например, `Server_1`). Имя Сервера должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

6. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности. Для этого последовательно откройте документы по соответствующим ссылкам в названиях флажков **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **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 условия Политики конфиденциальности**.

7. Если вы полностью согласны с условиями Лицензионного соглашения и Политики конфиденциальности, то установите оба флажка.

   Если вы не согласны с условиями Лицензионного соглашения и/или Политики конфиденциальности, то закройте страницу веб-интерфейса и удалите установленные компоненты программы на компьютерах.

8. Нажмите на кнопку **Продолжить**.

   После применения заданных параметров откроется страница веб-интерфейса в основном режиме работы программы. Для текущего сеанса подключения будут использованы учетные данные первого пользователя программы.

При необходимости вы можете вернуть Сервер в начальное состояние с помощью скрипта для локального перевода узла в начальное состояние kics4net-reset-to-defaults.sh. Скрипт находится на компьютере с установленным компонентом программы в директории /opt/kaspersky/kics4net/sbin/.

Запуск и остановка программы

Компонент программы, установленный на компьютере, запускается автоматически при загрузке операционной системы компьютера. Для работы компонента программы требуется выполнить его настройку. Настройка работы компонентов выполняется при подготовке программы к работе.

Программа выполняет функции по анализу трафика промышленной сети, если получает трафик через точки мониторинга. Вы можете выключать и включать точки мониторинга, чтобы приостанавливать и возобновлять анализ трафика, поступающего на эти точки мониторинга.

Узлы с установленными компонентами Kaspersky Industrial CyberSecurity for Networks получают и обрабатывают данные от EPP-приложений, если на этих узлах добавлены серверы интеграции. Вы можете выключать и включать серверы интеграции, чтобы приостанавливать и возобновлять получение данных от EPP-приложений.

Программа позволяет проводить активные опросы устройств в рамках заданий активных опросов и заданий контроля конфигураций. Активные опросы выполняются с помощью коннекторов, которые позволяют получать различные сведения об устройствах, в том числе для формирования топологической карты. Вы можете выключать и включать коннекторы, чтобы приостанавливать и возобновлять отправку и получение данных через эти коннекторы.

Для управления работой программы и просмотра сведений вы можете подключаться к Серверу через веб-интерфейс. По окончании работы с Сервером рекомендуется выполнять действия для завершения сеанса подключения.

Для настройки подключения сенсора к Серверу и просмотра сведений о состоянии подключения вы можете подключаться к сенсору через веб-интерфейс. При подключении к сенсору не требуется вводить учетные данные пользователя, поэтому действия для завершения сеанса подключения не предусмотрены.

Подключение к Серверу через веб-интерфейс

Вы можете подключиться к Серверу через веб-интерфейс с помощью любого поддерживаемого браузера. Подключение возможно с компьютера, который имеет доступ по сети к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks.

Чтобы подключиться к Серверу Kaspersky Industrial CyberSecurity for Networks:

1. Откройте браузер и введите в адресной строке:
   `https://<имя Сервера>:<порт>`

   где:

   - `<имя Сервера>` – IP-адрес или имя компьютера Сервера, используемые веб-сервером на компьютере Сервера;
   - `<порт>` – номер порта, указанный для веб-сервера.

   Если для веб-сервера не указан номер порта (до начальной настройки программы) или указан номер порта по умолчанию (443), в адресной строке достаточно ввести только IP-адрес или имя компьютера Сервера. В этом случае протокол HTTPS и номер порта будут определены автоматически.

2. При появлении страницы ввода учетных данных введите имя и пароль пользователя программы и нажмите на кнопку **Войти**.

   В окне браузера откроется страница веб-интерфейса Сервера Kaspersky Industrial CyberSecurity for Networks. В имени вкладки браузера со страницей веб-интерфейса будет указано имя Сервера, заданное при начальной настройке программы после установки.

Сеанс подключения к Серверу ограничен по времени. Время действия сеанса составляет 10 часов. Если с момента подключения прошло 10 часов, происходит переход с текущей страницы веб-интерфейса программы на страницу ввода учетных данных. В этом случае для продолжения работы вам потребуется снова ввести имя и пароль пользователя программы.

Завершение сеанса подключения к Серверу через веб-интерфейс

По окончании работы с Сервером Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс выполните действия для завершения сеанса подключения в браузере.

Если вы закрыли окно браузера без завершения сеанса подключения, сеанс останется действующим. Время действия сеанса составляет 10 часов. В течение этого времени программа может предоставить доступ к веб-интерфейсу Сервера Kaspersky Industrial CyberSecurity for Networks без запроса учетных данных пользователя, если для повторного подключения используются те же компьютер, браузер и учетная запись операционной системы.

Чтобы завершить сеанс подключения к Серверу Kaspersky Industrial CyberSecurity for Networks:

1. На странице веб-интерфейса Сервера Kaspersky Industrial CyberSecurity for Networks откройте меню пользователя:
   - Если меню свернуто, нажмите на кнопку .
   - Если меню развернуто, нажмите на кнопку справа от имени текущего пользователя.
2. В меню пользователя выберите пункт **Выход**.

В окне браузера отобразится страница ввода учетных данных.

Подключение к сенсору через веб-интерфейс

При подключении к сенсору через веб-интерфейс вы можете выполнять следующие действия на странице веб-интерфейса сенсора:

- загружать на сенсор файл свертки для подключения сенсора к Серверу Kaspersky Industrial CyberSecurity for Networks;
- просматривать отпечаток запроса на подпись сертификата для сравнения с отпечатком на странице веб-интерфейса Сервера, если подключение сенсора к Серверу выполняется автоматически по сети;
- просматривать сведения о состоянии подключения сенсора к Серверу.

Для изменения параметров сенсора, управления точками мониторинга и технологиями, а также для контроля состояния этого узла вам нужно подключиться к Серверу программы через веб-интерфейс.

Вы можете подключиться к сенсору через веб-интерфейс с помощью любого поддерживаемого браузера. Подключение возможно с компьютера, который имеет доступ по сети к компьютеру сенсора.

Чтобы подключиться к сенсору Kaspersky Industrial CyberSecurity for Networks,

откройте браузер и введите в адресной строке:
`https://<имя сенсора>:<порт>`

где:

- `<имя сенсора>` – IP-адрес или имя компьютера сенсора, используемые веб-сервером сенсора;
- `<порт>` – номер порта, используемый веб-сервером сенсора.

Если для веб-сервера сенсора используется номер порта по умолчанию (443), в адресной строке достаточно ввести только IP-адрес или имя компьютера сенсора. В этом случае протокол HTTPS и номер порта будут определены автоматически.

В окне браузера откроется страница веб-интерфейса сенсора Kaspersky Industrial CyberSecurity for Networks. В имени вкладки браузера со страницей веб-интерфейса будет указано имя сенсора, заданное при добавлении сенсора.

Интерфейс программы

Этот раздел содержит информацию об основных элементах интерфейса программы.

Веб-интерфейс Сервера Kaspersky Industrial CyberSecurity for Networks

При подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс в браузере открывается страница веб-интерфейса Сервера. Содержание страницы веб-интерфейса зависит от режима работы программы и от роли учетной записи подключенного пользователя.

В зависимости от режима работы программы страница веб-интерфейса может содержать следующие элементы управления или сообщения:

- В режиме начальной настройки программы – элементы управления для настройки Сервера после его установки и для просмотра и принятия Лицензионного соглашения и Политики конфиденциальности.
- В основном режиме работы программы – элементы управления для настройки и использования функциональности программы.
- В режиме обслуживания программы – сообщение о выполняемой операции, до окончания которой Сервер недоступен для подключений.

В основном режиме работы программы ее доступная функциональность на странице веб-интерфейса зависит от роли учетной записи подключенного пользователя. Если роль пользователя не предоставляет права на использование функций управления работой программы, соответствующие элементы управления не отображаются на странице веб-интерфейса, либо становятся недоступны.

О веб-интерфейсе Сервера в режиме начальной настройки программы

После установки программы при первом подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс программа не запрашивает учетные данные пользователя для входа. Вместо страницы ввода учетных данных открывается страница, содержащая элементы управления для настройки Сервера и для просмотра и принятия Лицензионного соглашения и Политики конфиденциальности.

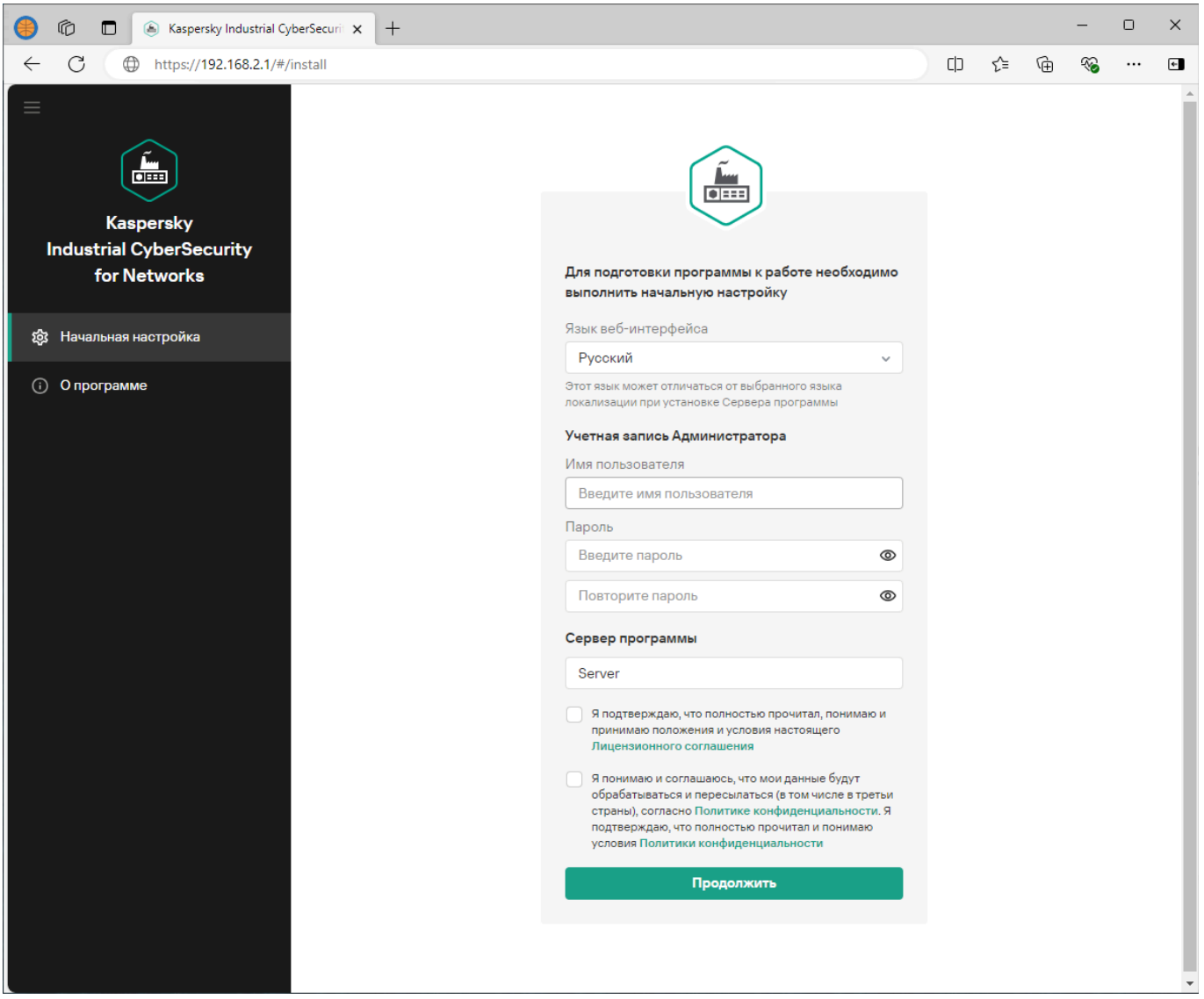
В левой части страницы веб-интерфейса отображается меню. Справа отображается содержимое выбранного раздела.

Меню веб-интерфейса содержит следующие элементы:

- – разворачивает и сворачивает меню. Если меню свернуто, элементы отображаются без текстовых пояснений.

- – открывает раздел **Начальная настройка**.

  В разделе **Начальная настройка** веб-интерфейса Сервера (см. рис. ниже) вы можете указать основные параметры Сервера программы, которые требуются для начала работы программы после ее установки.



Раздел **Начальная настройка**

Раздел содержит окно, с помощью которого вы можете настроить основные параметры Сервера, создать первого пользователя с ролью Администратор и ознакомиться и принять условия Лицензионного соглашения и Политики конфиденциальности. После выполнения этих действий данная страница веб-интерфейса автоматически закрывается (в том числе и в других сеансах подключения к Серверу через веб-интерфейс) и происходит переход на страницу веб-интерфейса Сервера в основном режиме работы программы.

- – открывает раздел с краткой информацией о программе.

О веб-интерфейсе Сервера в основном режиме работы программы

В основном режиме работы программы после подключения к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс открывается страница, содержащая средства для работы с программой. Состав доступных средств и их функциональность зависят от роли пользователя, под которым выполнено подключение к Серверу.

В левой части страницы веб-интерфейса отображается меню. Справа отображается содержимое выбранного раздела.

Меню веб-интерфейса содержит следующие элементы:

- – разворачивает и сворачивает меню. Если меню свернуто, элементы отображаются без текстовых пояснений.
- – открывает список уведомлений о проблемах в работе программы. О наличии уведомлений информирует значок, цвет которого соответствует статусу уведомлений.
- – открывает список фоновых операций. Список содержит информацию о выполнении операций, занимающих длительное время (например, формирование файла при экспорте большого количества событий). О количестве активных фоновых операций и о статусе их выполнения информирует значок. Значок имеет красный цвет, если есть операции, при выполнении которых возникли ошибки.
- – открывает раздел **Мониторинг**.
- – открывает раздел **Активы**.
- – открывает раздел **Карта сети**.
- – открывает раздел **События**.
- – открывает раздел **Отчеты**.
- – открывает раздел **Контроль процесса**.
- – открывает раздел **Разрешающие правила**.
- – открывает раздел **Обнаружение вторжений**.
- – открывает раздел **Риски**.
- – открывает раздел **Аудит безопасности**.
- – открывает раздел **Параметры**.
- – открывает раздел с краткой информацией о программе.
- – отображается, если какие-либо функции программы выключены или включен режим обучения для функций. Если меню развернуто, отображается уведомление **Не все функции защиты включены**. При нажатии на значок или текст открывается окно с информацией о выключенных функциях защиты.

- **Сервер подключения** – отображает имя Сервера, к которому выполнено подключение (имя, заданное при начальной настройке программы после установки).

- – если меню свернуто, открывает и закрывает меню пользователя. Если меню развернуто, рядом отображается имя текущего пользователя и его роль (в этом случае для открытия и закрытия меню пользователя вы можете использовать кнопку справа). Меню пользователя состоит из следующих разделов:

  - **Язык** – позволяет выбрать язык веб-интерфейса программы.

    Выбранный язык локализации веб-интерфейса программы не влияет на язык локализации Сервера Kaspersky Industrial CyberSecurity for Networks. Этот компонент использует язык локализации, заданный при установке или переустановке Kaspersky Industrial CyberSecurity for Networks. Вследствие этого язык локализации данных, которые предоставляет Сервер, может отличаться от выбранного языка локализации веб-интерфейса. Например, события и сообщения, которые поступают от Сервера (в том числе некоторые сообщения об ошибках), выводятся на языке локализации Сервера.

  - **Тема оформления** – позволяет выбрать тему цветового оформления страницы веб-интерфейса:

    - **Светлая** – элементы отображаются на белом фоне.

    - **Темная** – элементы отображаются на темном фоне.

  - **Учетная запись** – группирует пункты меню для выполнения действий с учетной записью текущего пользователя:

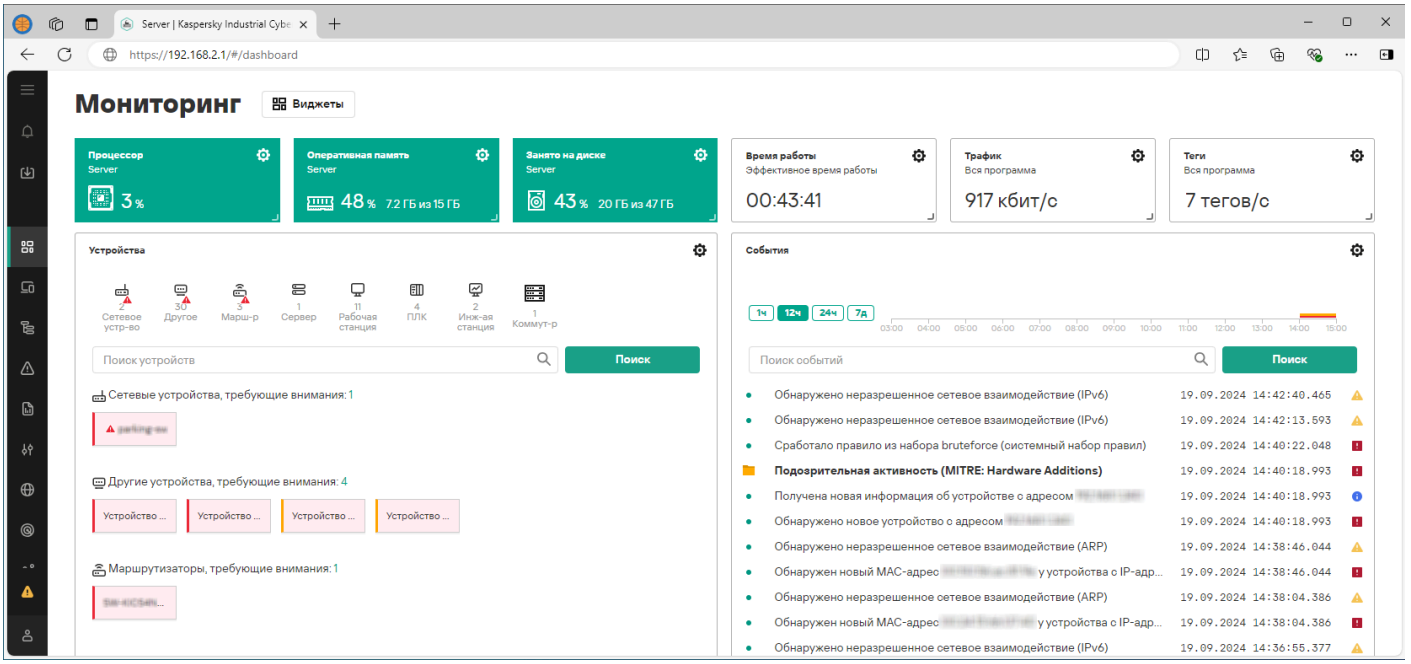
    - **Изменить пароль** – открывает окно для изменения пароля текущего пользователя.

    - **Выход** – завершает сеанс подключения к Серверу и открывает страницу ввода учетных данных для подключения.

  - **Дополнительная информация** – содержит пункт **Справка** для перехода на страницу онлайн-справки Kaspersky Industrial CyberSecurity for Networks.

Раздел Мониторинг

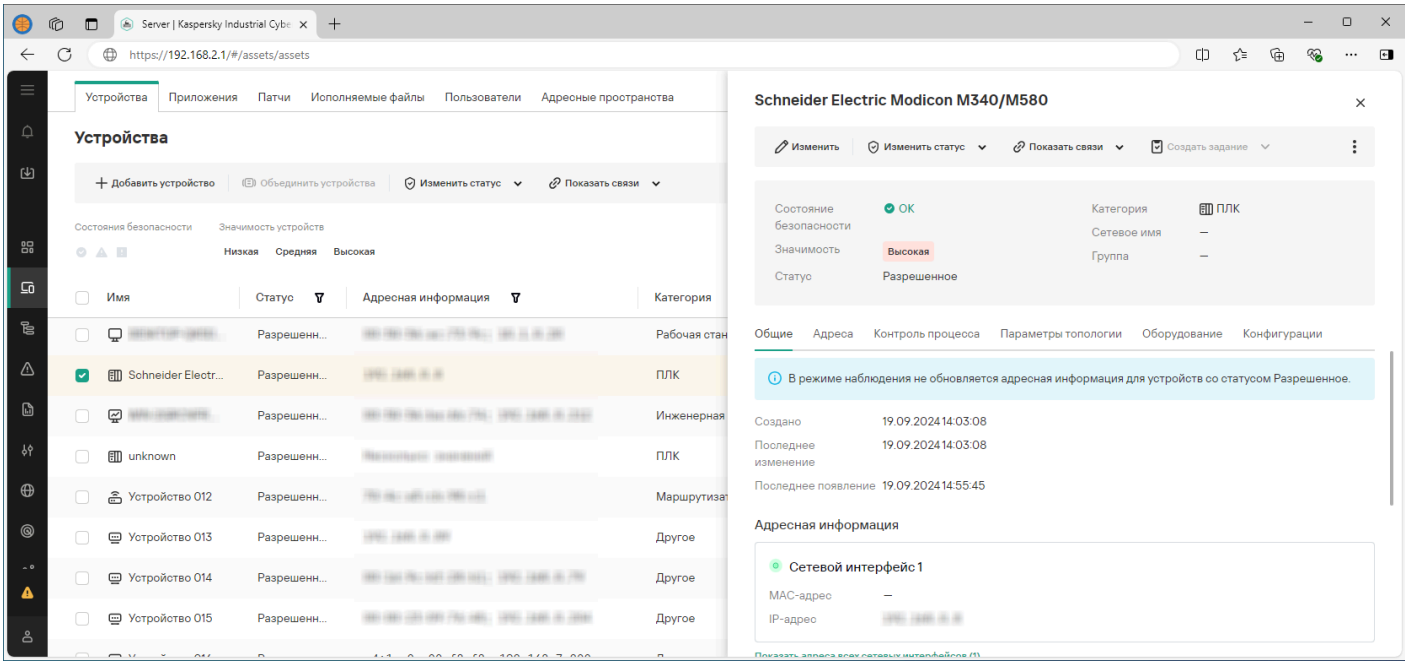
В разделе **Мониторинг** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать в онлайн-режиме сведения о текущем состоянии системы.



Раздел **Мониторинг**

Раздел Активы

В разделе **Активы** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и изменять сведения об устройствах и их основных объектах и параметры адресных пространств устройств.



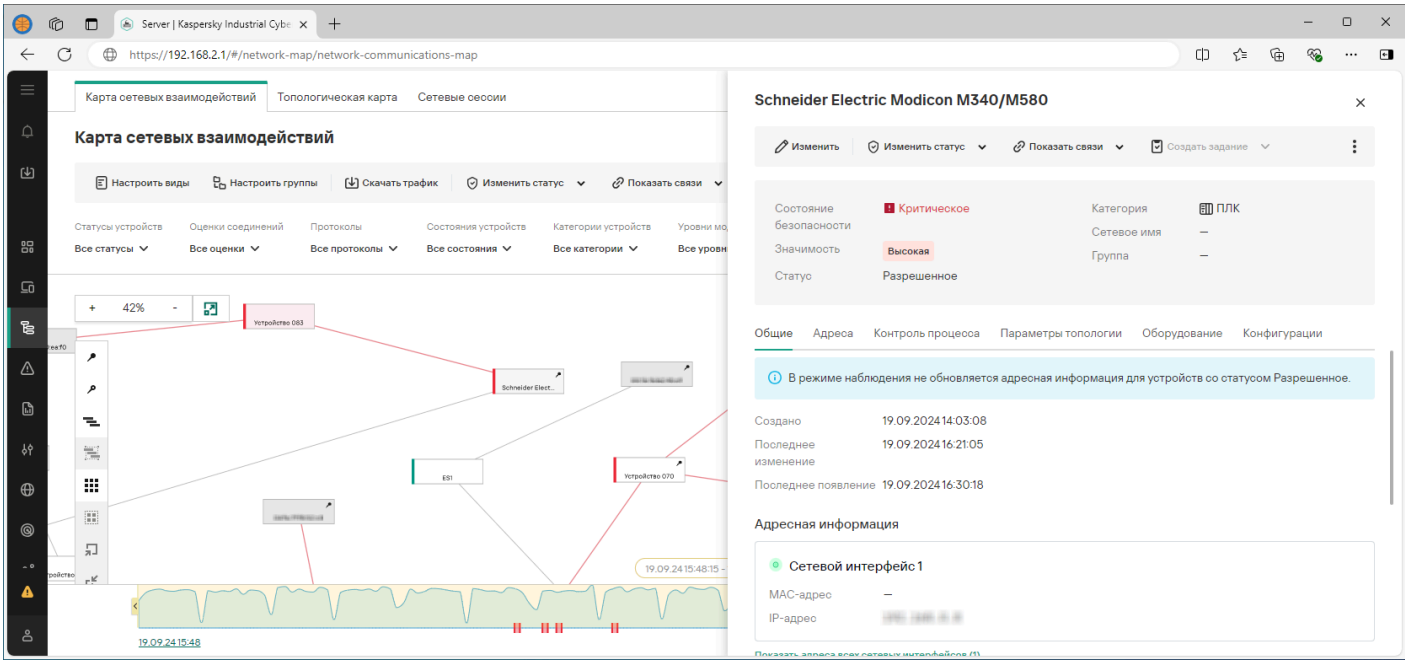
Раздел **Активы**

Раздел **Активы** содержит вкладку с таблицей устройств, вкладки с таблицами основных объектов на устройствах (приложения, патчи, исполняемые файлы и пользователи), а также вкладку со сведениями об адресных пространствах.

При выборе устройств и других объектов на вкладках открывается область деталей в правой части раздела. При выборе адресного пространства открывается блок со сведениями о правилах и подсетях адресного пространства. При выборе подсети адресного пространства открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранном объекте и инструменты для работы с ним.

Раздел Карта сети

В разделе **Карта сети** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать сведения о взаимодействиях на карте сети и в таблице сетевых сеансов, а также формировать топологическую карту.



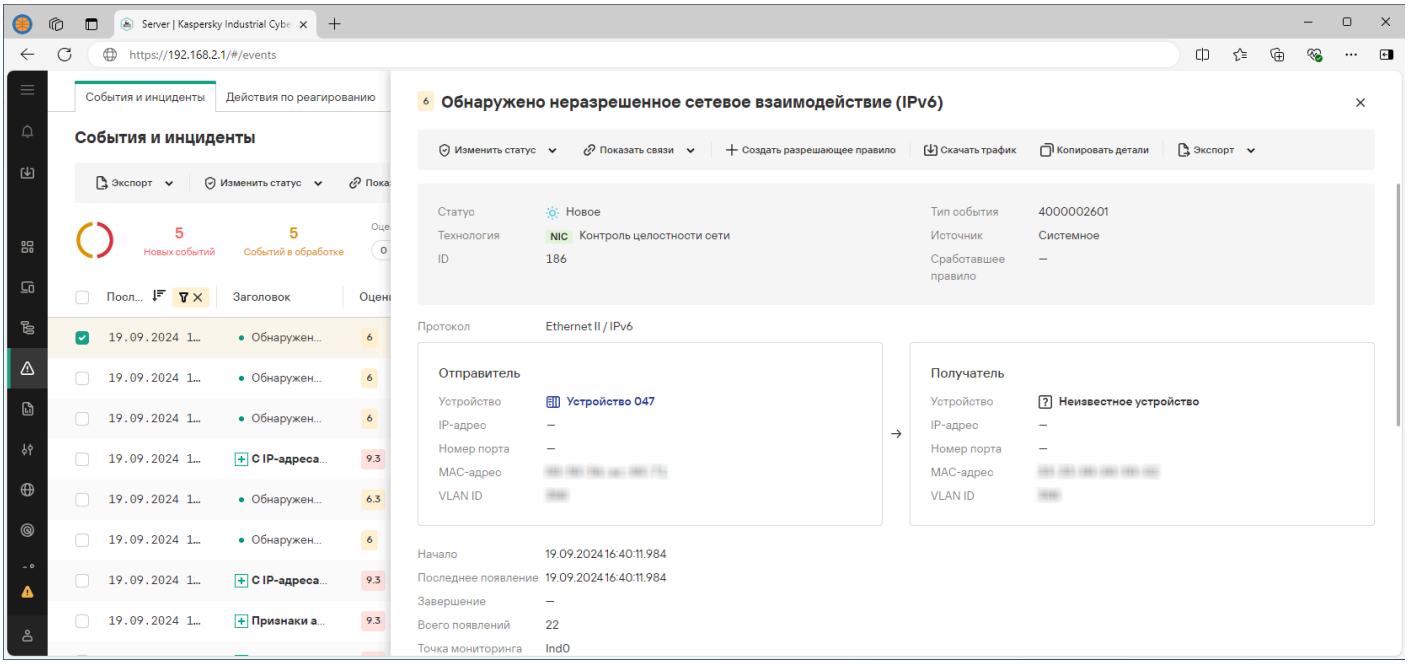
Раздел **Карта сети**

Раздел **Карта сети** содержит вкладки с картой сетевых взаимодействий, топологической картой и таблицей сетевых сеансов. Вкладки с картой сетевых взаимодействий и топологической картой содержат основную панель инструментов в верхней части, область отображения объектов карт и дополнительные панели инструментов для управления размещением объектов. В нижней части вкладки **Карта сетевых взаимодействий** расположена временная шкала для фильтрации объектов по периоду времени.

При выборе объекта открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранном объекте и инструменты для работы с ним.

Раздел События

В разделе **События** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и обрабатывать события и инциденты, а также управлять действиями по реагированию на угрозы.



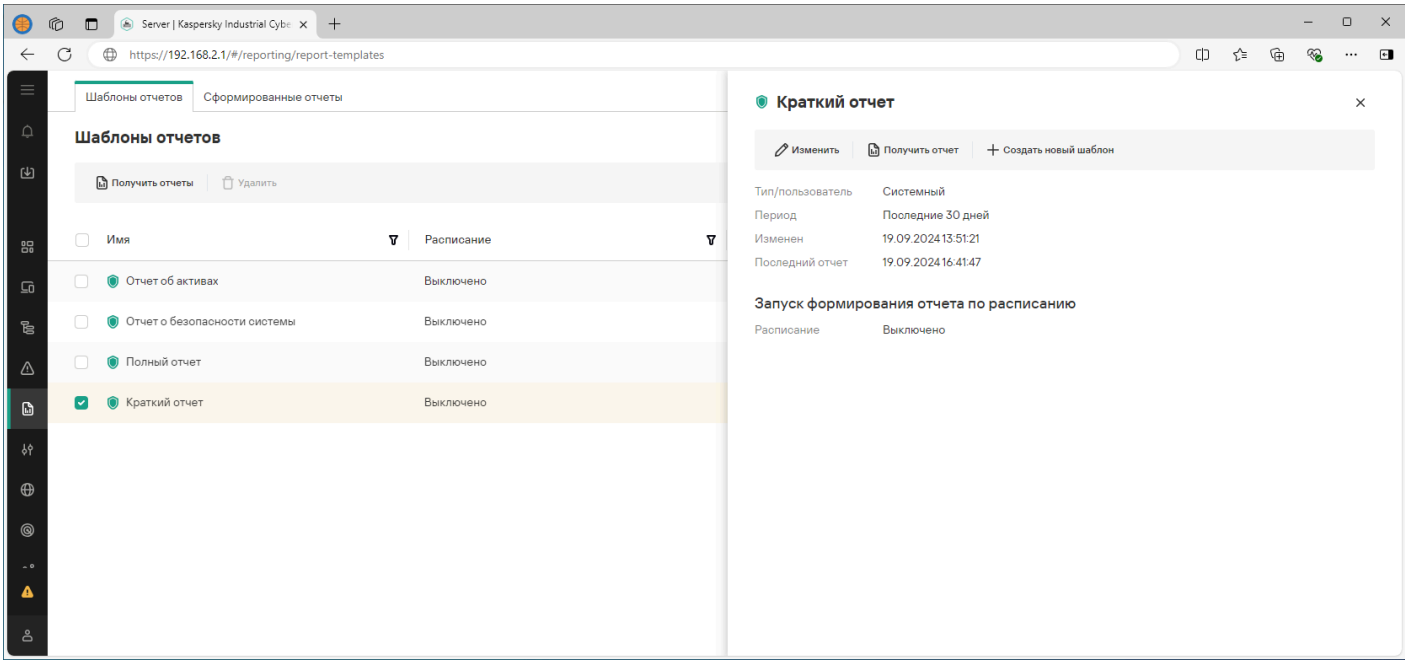
Раздел **События**

Раздел **События** содержит вкладки с таблицами событий и действий по реагированию.

При выборе события или действия открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранном объекте и инструменты для работы с ним.

Раздел Отчеты

В разделе **Отчеты** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать сформированные отчеты и шаблоны отчетов, а также управлять отчетами и шаблонами отчетов.



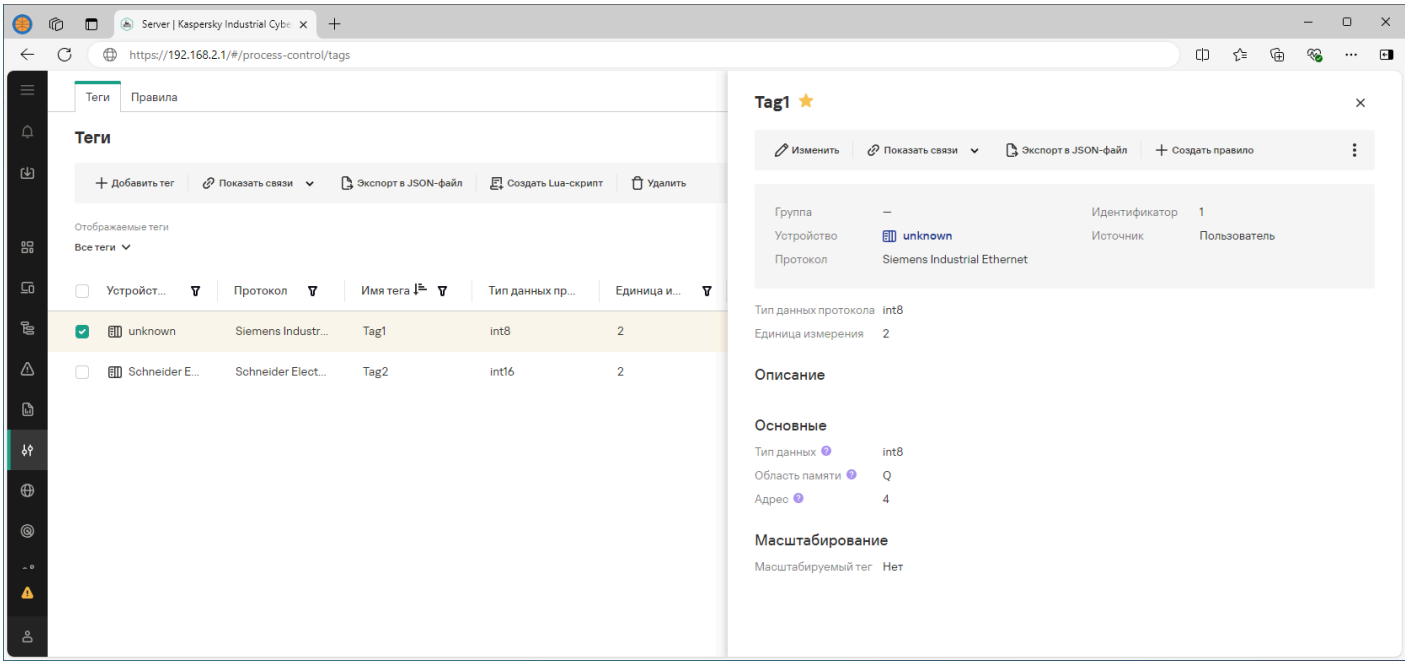
Раздел **Отчеты**

Раздел **Отчеты** содержит вкладки с таблицами шаблонов отчетов и сформированных отчетов.

При выборе шаблона отчета или сформированного отчета открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранном объекте и инструменты для работы с ним.

Раздел Контроль процесса

В разделе **Контроль процесса** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать значения параметров технологического процесса (тегов), а также настраивать теги и правила для контроля процесса.



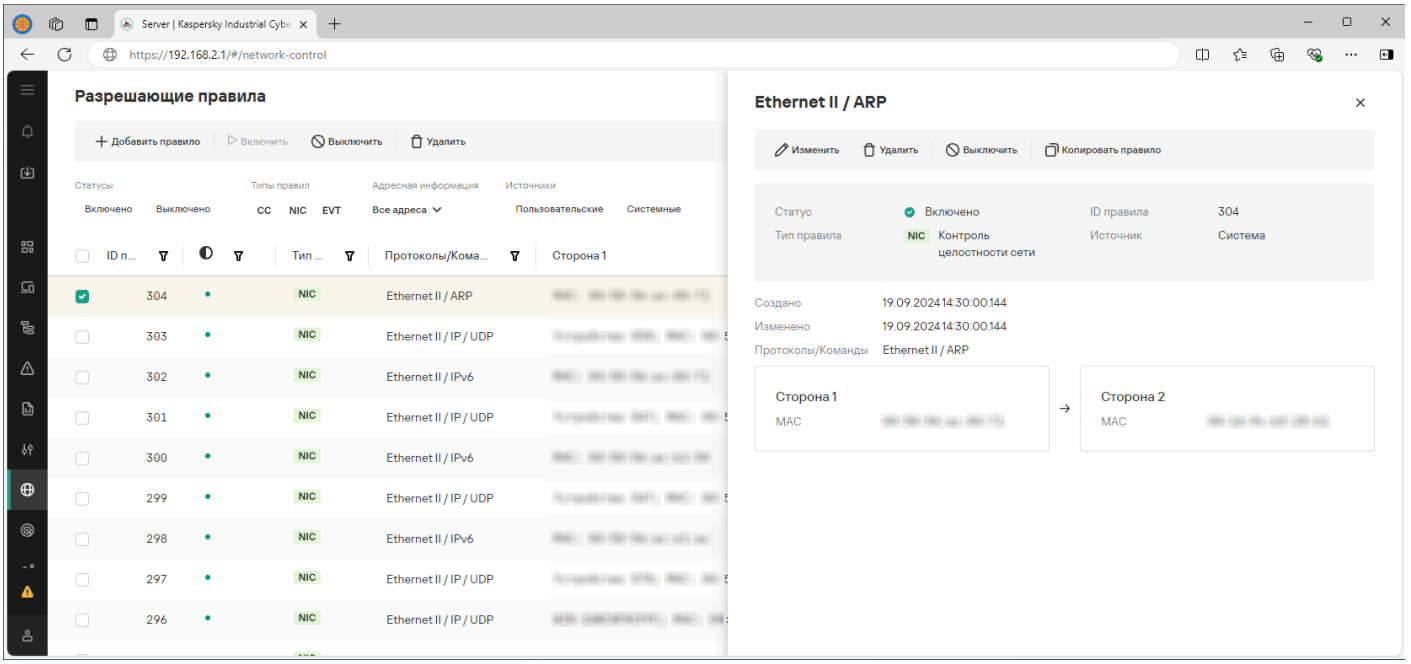
Раздел **Контроль процесса**

Раздел **Контроль процесса** содержит вкладки с таблицами тегов и правил контроля процесса.

При выборе тега или правила открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранном объекте и инструменты для работы с ним.

Раздел Разрешающие правила

В разделе **Разрешающие правила** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и изменять разрешающие правила для сетевых взаимодействий и событий.



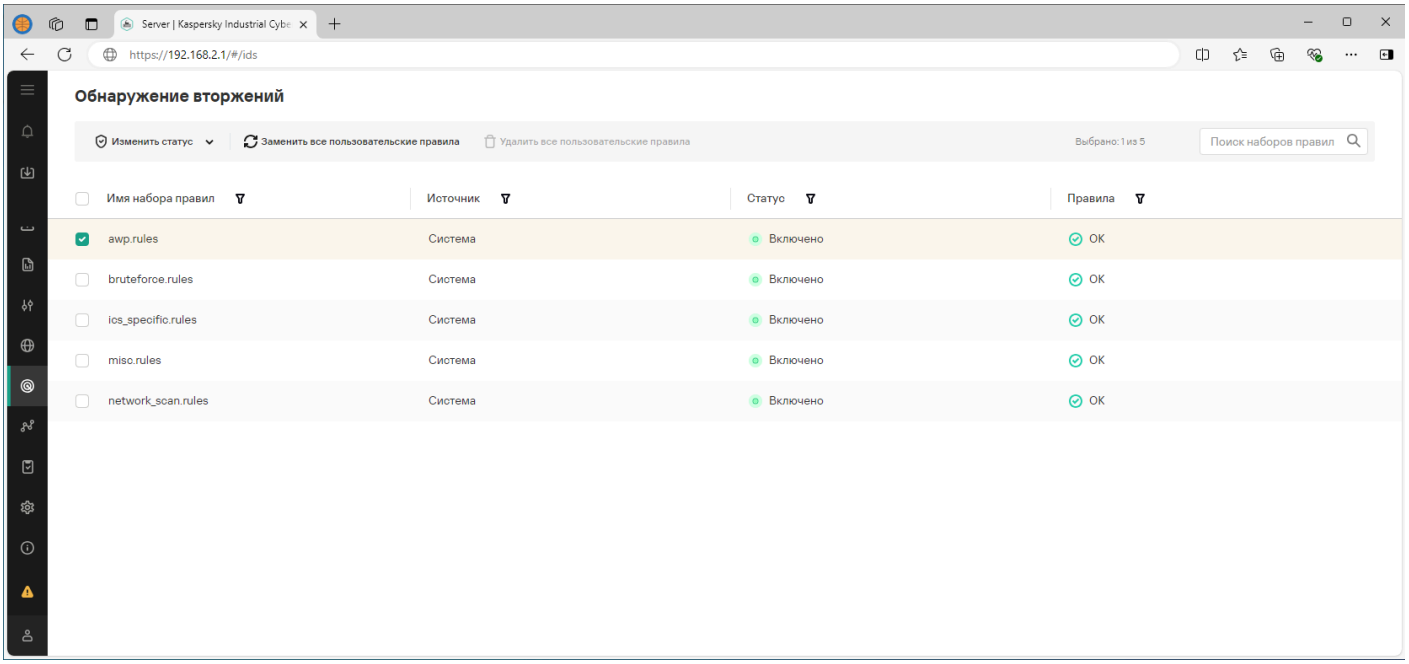
Раздел **Разрешающие правила**

Раздел **Разрешающие правила** содержит таблицу разрешающих правил.

При выборе правила открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранном правиле и инструменты для работы с ним.

Раздел Обнаружение вторжений

В разделе **Обнаружение вторжений** веб-интерфейса Сервера программы (см. рис. ниже) вы можете управлять наборами правил обнаружения вторжений.

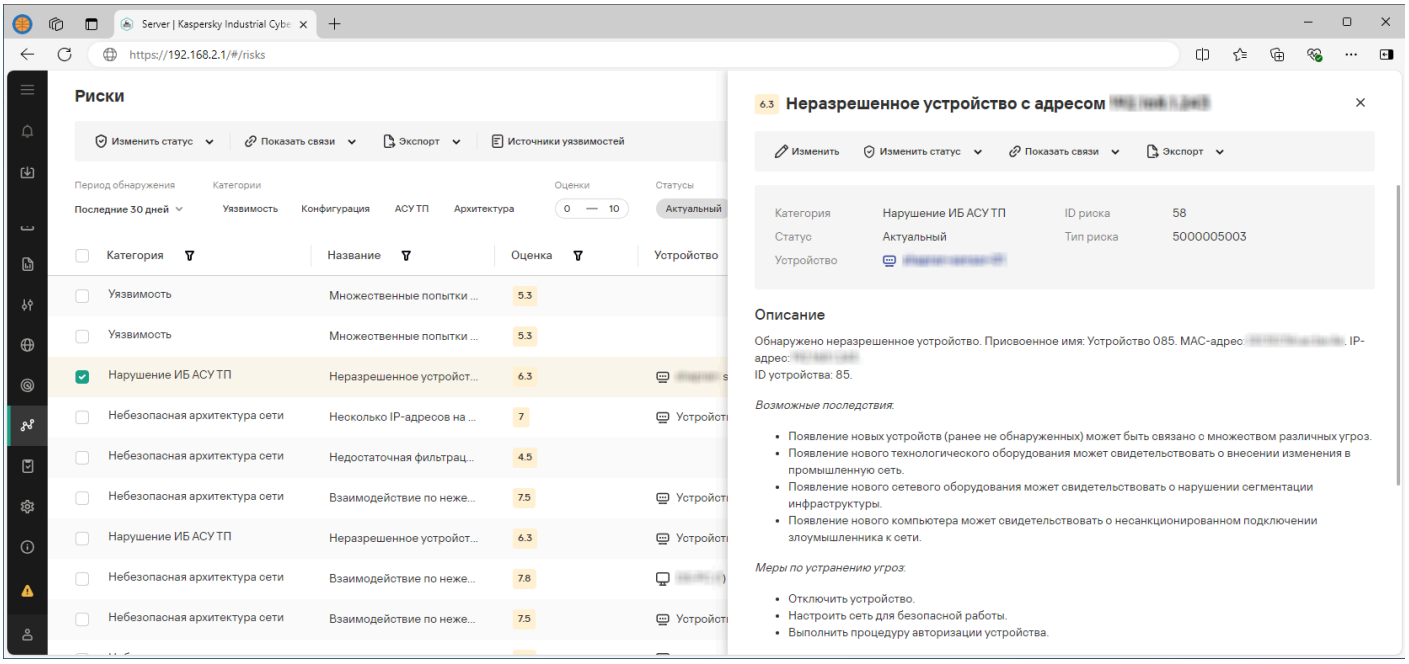


Раздел **Обнаружение вторжений**

Раздел **Обнаружение вторжений** содержит таблицу с наборами правил.

Раздел Риски

В разделе **Риски** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и обрабатывать риски, обнаруженные программой.



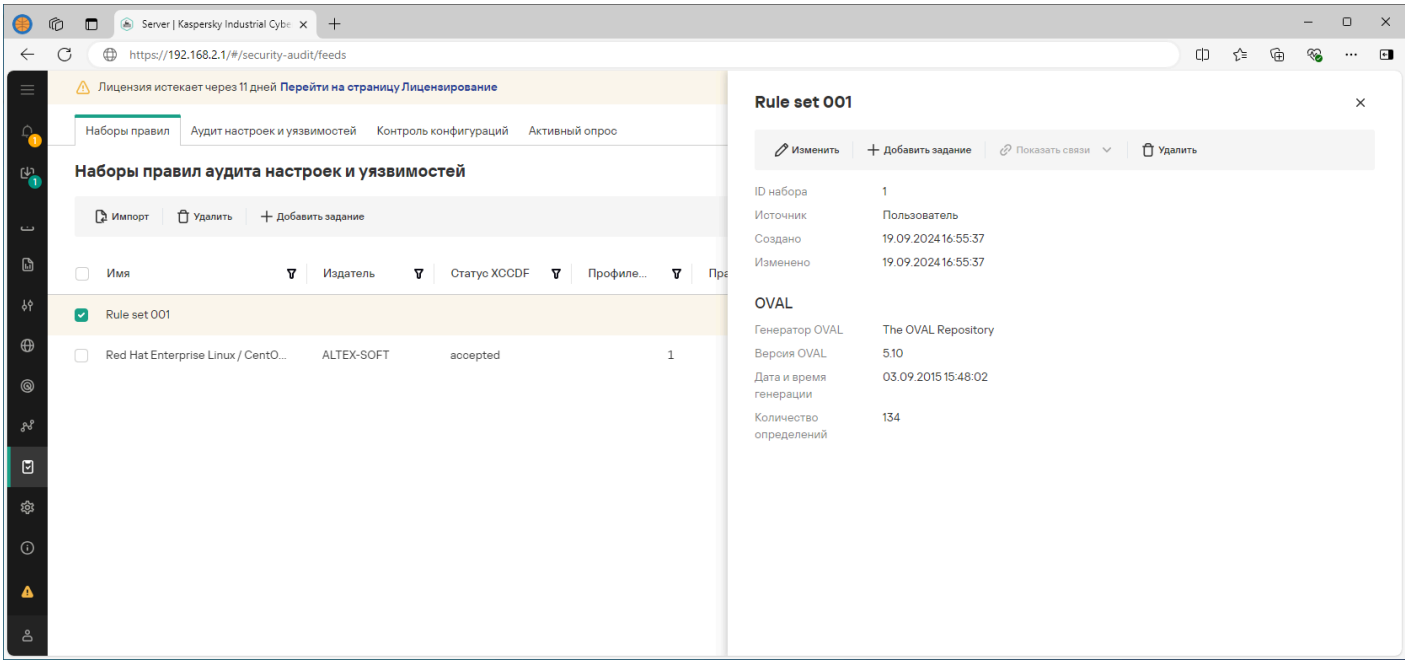
Раздел **Риски**

Раздел **Риски** содержит таблицу рисков.

При выборе риска открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранном риске и инструменты для работы с ним.

Раздел Аудит безопасности

В разделе **Аудит безопасности** веб-интерфейса Сервера программы (см. рис. ниже) вы можете управлять заданиями для аудита безопасности, а также управлять наборами правил для заданий аудита настроек и уязвимостей.



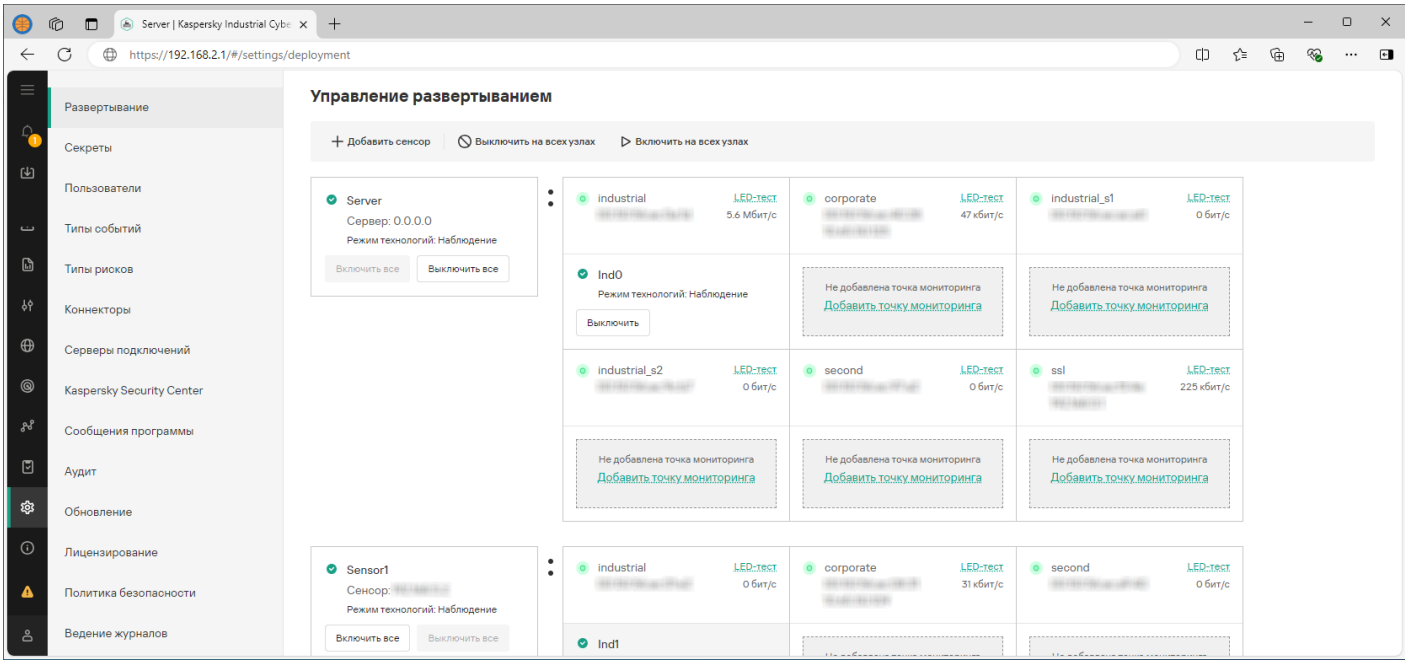
Раздел **Аудит безопасности**

Раздел **Аудит безопасности** содержит вкладки с таблицами наборов правил и заданий различных типов.

При выборе набора или задания открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранном объекте и инструменты для работы с ним.

Раздел Параметры

В разделе **Параметры** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и изменять параметры работы программы.



Раздел **Параметры**

При выборе раздела **Параметры** на странице веб-интерфейса появляется дополнительное меню. В этом меню вы можете перейти к следующим подразделам:

- **Развертывание**.

  В этом разделе вы можете просматривать сведения об узлах с установленными компонентами программы и о точках мониторинга на узлах. Если подключение к Серверу выполнено под учетной записью Администратора, в этом разделе также доступно управление параметрами развертывания.

- **Секреты**.

  В этом разделе вы можете управлять секретами с учетными данными для удаленных подключений. Раздел **Секреты** отображается, если подключение к Серверу выполнено под учетной записью Администратора.

- **Пользователи**.

  В этом разделе вы можете управлять учетными записями пользователей программы. Раздел **Пользователи** отображается, если подключение к Серверу выполнено под учетной записью Администратора.

- **Типы событий**.

  В этом разделе вы можете просматривать и изменять параметры типов событий.

- **Типы рисков**.

  В этом разделе вы можете просматривать и изменять параметры типов рисков.

- **Коннекторы**.

  В этом разделе вы можете управлять коннекторами для программы.

- **Серверы подключений**.

  В этом разделе вы можете просматривать и изменять параметры веб-сервера на компьютере Сервера (например, для использования доверенного сертификата), сервера REST API и серверов интеграции на узлах.

- **Kaspersky Security Center**.

  В этом разделе вы можете просматривать и изменять параметры функциональности взаимодействия с Kaspersky Security Center.

- **Сообщения программы**.

  В этом разделе вы можете просматривать сообщения о работе программы.

- **Аудит**.

  В этом разделе вы можете просматривать записи журнала аудита. Раздел **Аудит** отображается, если подключение к Серверу выполнено под учетной записью пользователя с ролью Администратор.

- **Обновление**.

  В этом разделе вы можете настроить и запустить обновление баз и модулей программы. Раздел **Обновление** отображается, если подключение к Серверу выполнено под учетной записью Администратора.

- **Лицензирование**.

  В этом разделе вы можете управлять лицензионным ключом для программы.

- **Политика безопасности**.

  В этом разделе вы можете управлять политикой безопасности программы.

- **Ведение журналов**.

  В этом разделе вы можете настроить уровни ведения журналов работы процессов.

Веб-интерфейс сенсора Kaspersky Industrial CyberSecurity for Networks

При подключении к сенсору Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс в браузере открывается страница веб-интерфейса сенсора. Содержание страницы веб-интерфейса зависит от состояния подключения сенсора к Серверу программы.

В зависимости от состояния подключения сенсора к Серверу программы страница веб-интерфейса может содержать следующие элементы управления или данные:

- До подключения сенсора к Серверу – элементы управления для выбора файла свертки и/или данные для автоматического подключения сенсора по сети.

- После подключения сенсора к Серверу – данные о Сервере и сенсоре (с возможностью перехода на страницу веб-интерфейса Сервера) и состояние соединения.

Лицензирование программы

Этот раздел содержит информацию о лицензировании Kaspersky Industrial CyberSecurity for Networks.

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 и примите условия Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- при начальной настройке программы;
- открыв документ license_ru.txt, входящий в комплект поставки программы (копия этого документа также сохраняется в директории установки программы).

Прочитайте и примите условия Лицензионного соглашения при начальной настройке программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать начальную настройку программы и не должны использовать программу.

О Политике конфиденциальности

Политика конфиденциальности – это документ, который информирует вас об условиях обработки ваших данных.

Внимательно ознакомьтесь и примите условия Политики конфиденциальности перед началом работы с программой.

Вы можете ознакомиться с условиями Политики конфиденциальности следующими способами:

- при начальной настройке программы;
- открыв документ privacy_policy_ru.txt, входящий в комплект поставки программы (копия этого документа также сохраняется в директории установки программы).

Прочитайте и примите условия Политики конфиденциальности при начальной настройке программы. Если вы не согласны с условиями Политики конфиденциальности, вы должны прервать начальную настройку программы и не должны использовать программу.

О лицензии

Лицензия – это право на использование программы, предоставляемое вам на основании Лицензионного соглашения. Вы можете использовать функциональность программы при условии приобретения Лицензионного сертификата.

Для текущей версии программы предусмотрены следующие типы лицензий:

- Upd&Sup – для бессрочного использования базовой функциональности программы, а также для использования функциональности обновления баз и программных модулей в течение срока действия лицензии.

  Этот тип лицензии применяется для лицензирования Сервера и всех используемых сенсоров программы. Функциональность обновления активируется в программе после добавления лицензионного ключа с действующей лицензией типа Upd&Sup или лицензионного ключа с действующей лицензией типа Limited Updates, который использовался для программы предыдущих версий.

- Security Audit – для бессрочного использования базовой функциональности программы, а также для использования функциональности аудита безопасности и функциональности активного опроса устройств в течение срока действия лицензии.

  Этот тип лицензии применяется только для лицензирования Сервера программы. Для лицензирования используемых сенсоров требуется дополнительно приобрести лицензии типа Upd&Sup. Указанная функциональность активируется в программе после добавления лицензионного ключа с действующей лицензией типа Security Audit или лицензионного ключа с действующей лицензией типа Active Polling, который использовался для программы предыдущих версий.

- Remote Collector – для совместного использования с решением Kaspersky SD-WAN в сценариях, предусмотренных для режима интеграции.

  Этот тип лицензии не требует добавления лицензионного ключа в программу. Однако если вы не приобрели лицензию типа Remote Collector, вы не можете использовать Kaspersky Industrial CyberSecurity for Networks в режиме интеграции с решением Kaspersky SD-WAN.

С помощью лицензионного ключа вы можете активировать либо только функциональность для типа лицензии Upd&Sup, либо одновременно и функциональность для типа лицензии Upd&Sup, и функциональность для типа лицензии Security Audit. В программу можно добавить только один лицензионный ключ. Информацию о добавленном лицензионном ключе вы можете просмотреть при подключении к Серверу через веб-интерфейс.

По истечении срока действия лицензии программа продолжает работу, но соответствующая функциональность становится недоступна. В этом случае, чтобы продолжить использование функциональности, вам нужно добавить новый лицензионный ключ с действующей лицензией нужного типа.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в программном обеспечении на территории США.

Услуги технической поддержки предоставляются при наличии действующего Договора об оказании технической поддержки. Для получения услуг технической поддержки вам требуется назначить контактных лиц, имеющих право открывать заявки на оказание услуг технической поддержки.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам при приобретении лицензии и подтверждает право на использование программы.

В Лицензионном сертификате для Kaspersky Industrial CyberSecurity for Networks содержится следующая информация:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе и компоненте, на который распространяется лицензия;
- ограничение на количество единиц лицензирования (например, сенсоров);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

Лицензионный ключ (далее также *ключ*) – последовательность бит, с помощью которой вы можете активировать и затем использовать функциональность, которая определена типом лицензии. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в программу, применив *файл лицензионного ключа*. Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

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

О файле лицензионного ключа

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

Вы получаете файл лицензионного ключа после приобретения Kaspersky Industrial CyberSecurity for Networks. Способ получения файла лицензионного ключа определяется дистрибьютором "Лаборатории Касперского", у которого вы приобрели программу (например, файл лицензионного ключа может быть отправлен по указанному вами адресу электронной почты).

Вы также можете добавить в программу лицензионный ключ из файла лицензионного ключа, полученного при приобретении Kaspersky Industrial CyberSecurity for Networks предыдущей версии. Лицензионный ключ можно добавить в программу до даты окончания его срока годности.

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

Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс

Вы можете добавить лицензионный ключ в Kaspersky Industrial CyberSecurity for Networks при подключении к Серверу через веб-интерфейс или с использованием функциональности автоматического распространения лицензионных ключей в Kaspersky Security Center.

Добавлять лицензионный ключ могут только пользователи с ролью Администратор.

Чтобы добавить лицензионный ключ:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Лицензирование**.
3. Нажмите на кнопку **Добавить лицензионный ключ**. Кнопка отсутствует, если лицензионный ключ уже был добавлен в программу.

   Откроется стандартное окно используемого браузера для выбора файла лицензионного ключа.
4. Укажите путь к файлу лицензионного ключа с расширением key.
5. Нажмите на кнопку открытия файла.

Лицензионный ключ из выбранного файла будет загружен в программу.

Просмотр информации о добавленном лицензионном ключе

При подключении к Серверу через веб-интерфейс вы можете просматривать информацию о добавленном лицензионном ключе. Информация о лицензионном ключе отображается в разделе **Параметры** → **Лицензирование**. Дополнительно в списке уведомлений о проблемах в работе программы могут отображаться предупреждения о статусе лицензионного ключа.

Чтобы просмотреть информацию о лицензионном ключе,

выберите раздел **Параметры** → **Лицензирование**.

Для добавленного лицензионного ключа отображается следующая информация:

- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Описание** – сведения о доступной функциональности.
- **Дата активации** – дата первого добавления лицензионного ключа в программу.
- **Срок действия** – дата окончания срока годности лицензионного ключа.
- **Истекает** – количество оставшихся дней до окончания срока годности.
- Информация о статусе ключа или предупреждение о возникшей проблеме.

Удаление лицензионного ключа

При подключении к Серверу через веб-интерфейс вы можете удалить добавленный лицензионный ключ из программы (например, если требуется заменить текущий лицензионный ключ на другой). После удаления лицензионного ключа в программе будет недоступна соответствующая функциональность. Недоступная функциональность снова активируется при следующем добавлении лицензионного ключа.

Удалять лицензионный ключ могут только пользователи с ролью Администратор.

Чтобы удалить добавленный лицензионный ключ:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Лицензирование**.
3. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
4. Подтвердите удаление лицензионного ключа.

Лицензионный ключ будет удален из программы.

Предоставление данных

Условия Лицензионного соглашения описывают обрабатываемые в автоматическом режиме данные для обеспечения работы программы. Правообладатель обрабатывает предоставленные данные в соответствии с Политикой конфиденциальности, в которой описываются, в частности, меры по защите данных, территории обработки и права субъектов данных. Часть предоставляемых данных по законодательству некоторых стран может категоризироваться как персональные данные.

Программа не передает пользовательские персональные данные в "Лабораторию Касперского". Пользовательские персональные данные обрабатываются на компьютерах, на которых установлены компоненты программы.

Программа обрабатывает и сохраняет следующие данные, имеющие отношение к пользовательским персональным данным:

- имена учетных записей пользователей, созданных в программе (пользователи программы);
- IP-адреса или имена компьютеров с установленными компонентами программы;
- IP-адреса, MAC-адреса и другие сведения об устройствах, полученные программой;
- данные об адресных пространствах и подсетях;
- данные о параметрах технологического процесса в правилах контроля процесса;
- IP-адрес или имя компьютера с Kaspersky Security Center;
- IP-адреса или имена компьютеров, которые подключаются к программе через коннекторы;
- адреса электронной почты получателей, указанные в коннекторах электронной почты и в шаблонах отчетов;
- данные в сформированных отчетах программы;
- данные в трафике промышленной сети, передаваемые между устройствами и содержащие пользовательские персональные данные (эти данные обрабатываются программой вместе с остальными данными при анализе трафика промышленной сети);
- данные об обнаруженных рисках, которым подвержены ресурсы информационной системы;
- данные о возможно зараженных объектах или возможных угрозах, полученные от EPP-приложений и содержащие IP-адреса, интернет-адреса и адреса электронной почты;
- данные о приложениях и патчах, полученные от EPP-приложений или по результатам заданий аудита безопасности;
- данные об исполняемых файлах, полученные от EPP-приложений или по результатам заданий аудита безопасности;
- данные об учетных записях пользователей, полученные от EPP-приложений или по результатам заданий аудита безопасности;
- данные о результатах выполненных проверок на устройствах с использованием правил аудита настроек и уязвимостей;

- данные о конфигурациях устройств, полученные по результатам заданий аудита безопасности;
- идентификационная и аутентификационная информация, введенная пользователем программы и сохраненная в хранилище секретов.

Обработка перечисленных данных выполняется для обеспечения работы программы и для анализа нарушений технологического процесса, обнаружения угроз и аномалий сетевого трафика, которые могут являться признаками атак.

Программа сохраняет полученные данные в журналах.

Если администратор программы настроил отправку данных программы в сторонние системы, то обработка и хранение полученных данных в сторонней системе выполняется в соответствии с ее функциональностью и назначением.

Если с помощью скрипта централизованной установки программы созданы файлы для предоставления информации в Службу технической поддержки "Лаборатории Касперского", в этих файлах сохраняются следующие данные:

- Содержимое директорий для хранения данных программы:
  - файлы журналов работы процессов, относящихся к компонентам программы, к СУБД и к системе обнаружения вторжений;
  - файлы рабочих данных Сервера и сенсоров;
  - файл параметров установки, созданный скриптом централизованной установки программы;
  - журнал аудита и журнал сообщений программы.
- Политика безопасности, примененная на Сервере.

- Информация о текущем статусе сервисов, которые обеспечивают работу компонентов программы:
  - kics4net;
  - kics4net-apm;
  - kics4net-asset-config-repo;
  - kics4net-asset-inventory;
  - kics4net-blob-storage;
  - kics4net-config-control-orchestrator;
  - kics4net-connectors;
  - kics4net-connectors-launcher;
  - kics4net-email-gateway;
  - kics4net-epp-proxy;
  - kics4net-fts;
  - kics4net-nats-server;
  - kics4net-oval-facade;
  - kics4net-postgresql;
  - kics4net-risk-oval-detector;
  - kics4net-report-builder;
  - kics4net-report-data-source;
  - kics4net-report-renderer;
  - kics4net-report-templates-catalog;
  - kics4net-report-templates-catalog-view;
  - kics4net-responses-manager;
  - kics4net-scan-oval-manager;
  - kics4net-scap-manager;
  - kics4net-scap-manager-view;
  - kics4net-scheduler;
  - kics4net-secrets;
  - kics4net-suricata;

    - kics4net-task-manager;
    - kics4net-task-manager-view;
    - kics4net-vault;
    - kics4net-webserver;
    - kics4net-websensor;
    - klnagent.
- Информация о версии и дистрибутиве операционной системы на компьютерах с установленными компонентами программы (для получения информации используется команда `uname -a`).
- Информация о сетевых интерфейсах на компьютерах с установленными компонентами программы (для получения информации используется команда `ifconfig`).
- Записи, сохраненные службой аудита auditd в файле /var/log/audit/audit.log.
- Параметры, статус и режим работы межсетевого экрана в операционной системе.
- Если указаны соответствующие параметры при запуске скрипта централизованной установки программы, дополнительно сохраняются следующие файлы и данные:
    - файлы дампа трафика;
    - данные о конфигурации системы обнаружения вторжений;
    - данные о сертификатах, используемых в Kaspersky Industrial CyberSecurity for Networks (кроме сертификатов, изданных доверенными центрами сертификации).

Программа не отслеживает доступ к файлу параметров установки, созданному скриптом централизованной установки программы. При этом факты запуска компонентов программы и других подключений к Серверу, при которых происходит проверка учетных данных пользователей, отслеживаются программой.

При получении обновлений с серверов "Лаборатории Касперского" программа отправляет данные, необходимые для автоматического выбора нужных обновлений. Отправляемые данные не содержат пользовательских персональных данных. Программа отправляет следующие данные:

- версию Kaspersky Industrial CyberSecurity for Networks;
- код языка локализации компонентов Kaspersky Industrial CyberSecurity for Networks;
- идентификаторы обновляемых элементов;
- идентификатор установки Kaspersky Industrial CyberSecurity for Networks;
- идентификатор типа, версии и разрядности операционной системы.

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

Директории для хранения данных программы

Удаление или изменение любого файла в указанных директориях может привести к нарушению работоспособности программы.

На Сервере Kaspersky Industrial CyberSecurity for Networks программа использует для хранения данных следующие директории и их поддиректории:

- Директории установки компонентов и сервисов:
  - /opt/kaspersky/kics4net/ – для Сервера;
  - /opt/kaspersky/kics4net-apm/ – для коннектора активного опроса;
  - /opt/kaspersky/kics4net-asset-config-repo/ – для сервиса хранения конфигураций устройств;
  - /opt/kaspersky/kics4net-asset-inventory/ – для сервиса обработки результатов сканирования атрибутов устройств с помощью OVAL®-правил;
  - /opt/kaspersky/kics4net-blob-storage/ – для сервиса хранения массивов двоичных данных (англ. Binary Large Object, BLOB);
  - /opt/kaspersky/kics4net-config-control-orchestrator/ – для сервиса управления процессами контроля конфигураций и активного опроса;
  - /opt/kaspersky/kics4net-connectors/ – для системных коннекторов;
  - /opt/kaspersky/kics4net-connectors-launcher/ – для сервиса регистрации и запуска управляемых коннекторов;
  - /opt/kaspersky/kics4net-email-gateway/ – для сервиса отправки почтовых уведомлений;
  - /opt/kaspersky/kics4net-epp-proxy/ – для сервиса интеграции с EPP-приложениями;
  - /opt/kaspersky/kics4net-fts/ – для системы полнотекстового поиска;
  - /opt/kaspersky/kics4net-nats-server/ – для брокера сообщений;
  - /opt/kaspersky/kics4net-oval-facade/ – для сервиса сканирования удаленных устройств по OVAL-правилам;
  - /opt/kaspersky/kics4net-postgresql/ – для СУБД;
  - /opt/kaspersky/kics4net-report-builder/ – для сервиса формирования отчетов;
  - /opt/kaspersky/kics4net-report-data-source/ – для сервиса предоставления данных для отчетов;
  - /opt/kaspersky/kics4net-report-renderer/ – для сервиса визуального отображения блоков данных в отчетах;
  - /opt/kaspersky/kics4net-report-templates-catalog/ – для сервиса управления шаблонами отчетов;
  - /opt/kaspersky/kics4net-report-templates-catalog-view/ – для сервиса предоставления данных о шаблонах отчетов;
  - /opt/kaspersky/kics4net-responses-manager/ – для сервиса управления заданиями реагирования;
  - /opt/kaspersky/kics4net-risk-oval-detector/ – для сервиса обработки результатов сканирования устройств с помощью OVAL-правил на предмет наличия рисков;

- /opt/kaspersky/kics4net-scan-oval-manager/ – для сервиса управления сканирования устройств с помощью OVAL-правил;
- /opt/kaspersky/kics4net-scap-manager/ – для сервиса управления аудита безопасности;
- /opt/kaspersky/kics4net-scap-manager-view/ – для сервиса предоставления данных об аудите безопасности;
- /opt/kaspersky/kics4net-scheduler/ – для сервиса планировщика задач;
- /opt/kaspersky/kics4net-secrets/ – для фасада к хранилищу секретов;
- /opt/kaspersky/kics4net-suricata/ – для системы обнаружения вторжений;
- /opt/kaspersky/kics4net-task-manager/ – для сервиса управления задачами;
- /opt/kaspersky/kics4net-task-manager-view/ – для сервиса предоставления данных о задачах;
- /opt/kaspersky/kics4net-vault/ – для сервиса хранения секретов в хранилище;
- /opt/kaspersky/kics4net-webserver/ – для веб-сервера;
- /opt/kaspersky/klnagent64/ – для Агента администрирования.

- Директории для хранения сертификатов и рабочих данных:
  - /opt/kaspersky/kics4net/share/ids/ – для системы обнаружения вторжений;
  - /var/opt/kaspersky/kics4net/ – для Сервера;
  - /var/opt/kaspersky/kics4net-apm/ – для коннектора активного опроса;
  - /va/opt/kaspersky/kics4net-asset-config-repo/ – для сервиса хранения конфигураций устройств;
  - /var/opt/kaspersky/kics4net-asset-inventory/ – для сервиса обработки результатов сканирования атрибутов устройств с помощью OVAL-правил;
  - /var/opt/kaspersky/kics4net-blob-storage/ – для сервиса BLOB;
  - /var/opt/kaspersky/kics4net-config-control-orchestrator/ – для сервиса управления процессами контроля конфигураций и активного опроса;
  - /var/opt/kaspersky/kics4net-connectors/ – для системных коннекторов;
  - /var/opt/kaspersky/kics4net-connectors-launcher/ – для сервиса регистрации и запуска управляемых коннекторов;
  - /var/opt/kaspersky/kics4net-email-gateway/ – для сервиса отправки почтовых уведомлений;
  - /var/opt/kaspersky/kics4net-epp-proxy/ – для сервиса интеграции;
  - /var/opt/kaspersky/kics4net-fts/ – для системы полнотекстового поиска;
  - /var/opt/kaspersky/kics4net-nats-server/ – для брокера сообщений;

- /var/opt/kaspersky/kics4net-oval-facade/ – для сервиса сканирования удаленных устройств по OVAL-правилам;
- /var/opt/kaspersky/kics4net-postgresql/ – для СУБД;
- /var/opt/kaspersky/kics4net-report-builder/ – для сервиса формирования отчетов;
- /var/opt/kaspersky/kics4net-report-data-source/ – для сервиса предоставления данных для отчетов;
- /var/opt/kaspersky/kics4net-report-renderer/ – для сервиса представления блоков данных в отчетах;
- /var/opt/kaspersky/kics4net-report-templates-catalog/ – для сервиса управления шаблонами отчетов;
- /var/opt/kaspersky/kics4net-report-templates-catalog-view/ – для сервиса предоставления данных о шаблонах отчетов;
- /var/opt/kaspersky/kics4net-responses-manager/ – для сервиса управления заданиями реагирования;
- /var/opt/kaspersky/kics4net-risk-oval-detector/ – для сервиса обработки результатов сканирования устройств с помощью OVAL-правил на предмет наличия рисков;
- /var/opt/kaspersky/kics4net-scan-oval-manager/ – для сервиса управления сканирования устройств с помощью OVAL-правил;
- /var/opt/kaspersky/kics4net-scap-manager/ – для сервиса управления аудита безопасности;
- /var/opt/kaspersky/kics4net-scap-manager-view/ – для сервиса предоставления данных об аудите безопасности;
- /var/opt/kaspersky/kics4net-scheduler/ – для сервиса планировщика задач;
- /var/opt/kaspersky/kics4net-task-manager/ – для сервиса управления задачами;
- /var/opt/kaspersky/kics4net-task-manager-view/ – для сервиса предоставления данных о задачах;
- /var/opt/kaspersky/kics4net-vault/ – для сервиса хранения секретов в хранилище;
- /var/opt/kaspersky/kics4net-webserver/ – для веб-сервера;
- /var/opt/kaspersky/klnagent/ – для Агента администрирования.

- Директории для хранения журналов работы процессов:
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – для хранения журналов работы процессов установки и файла параметров установки (если централизованная установка компонентов программы выполнялась с этого компьютера);
  - /var/log/kaspersky/kics4net/ – для Сервера;
  - /var/log/kaspersky/kics4net-apm/ – для коннектора активного опроса;
  - /var/log/kaspersky/kics4net-asset-config-repo/ – для сервиса хранения конфигураций устройств;
  - /var/log/kaspersky/kics4net-asset-inventory/ – для сервиса обработки результатов сканирования атрибутов устройств с помощью OVAL-правил;
  - /var/log/kaspersky/kics4net-blob-storage/ – для сервиса BLOB;
  - /var/log/kaspersky/kics4net-config-control-orchestrator/ – для сервиса управления процессами контроля конфигураций и активного опроса;
  - /var/log/kaspersky/kics4net-connectors/ – для системных коннекторов;
  - /var/log/kaspersky/kics4net-connectors-launcher/ – для сервиса регистрации и запуска управляемых коннекторов;
  - /var/log/kaspersky/kics4net-email-gateway/ – для сервиса отправки почтовых уведомлений;
  - /var/log/kaspersky/kics4net-epp-proxy/ – для сервиса интеграции;
  - /var/log/kaspersky/kics4net-fts/ – для системы полнотекстового поиска;
  - /var/log/kaspersky/kics4net-nats-server/ – для брокера сообщений;
  - /var/log/kaspersky/kics4net-oval-facade/ – для сервиса сканирования удаленных устройств по OVAL-правилам;
  - /var/log/kaspersky/kics4net-postgresql/ – для СУБД;
  - /var/log/kaspersky/kics4net-report-builder/ – для сервиса формирования отчетов;
  - /var/log/kaspersky/kics4net-report-data-source/ – для сервиса предоставления данных для отчетов;
  - /var/log/kaspersky/kics4net-report-renderer/ – для сервиса представления блоков данных в отчетах;
  - /var/log/kaspersky/kics4net-report-templates-catalog/ – для сервиса управления шаблонами отчетов;
  - /var/log/kaspersky/kics4net-report-templates-catalog-view/ – для сервиса предоставления данных о шаблонах отчетов;
  - /var/log/kaspersky/kics4net-responses-manager/ – для сервиса управления заданиями реагирования;
  - /var/log/kaspersky/kics4net-risk-oval-detector/ – для сервиса обработки результатов сканирования устройств с помощью OVAL-правил на предмет наличия рисков;
  - /var/log/kaspersky/kics4net-scan-oval-manager/ – для сервиса управления сканирования устройств с помощью OVAL-правил;

- /var/log/kaspersky/kics4net-scap-manager/ – для сервиса управления аудита безопасности;
- /var/log/kaspersky/kics4net-scap-manager-view/ – для сервиса предоставления данных об аудите безопасности;
- /var/log/kaspersky/kics4net-scheduler/ – для сервиса планировщика задач;
- /var/log/kaspersky/kics4net-secrets/ – для фасада к хранилищу секретов;
- /var/log/kaspersky/kics4net-suricata/ – для системы обнаружения вторжений;
- /var/log/kaspersky/kics4net-task-manager/ – для сервиса управления задачами;
- /var/log/kaspersky/kics4net-task-manager-view/ – для сервиса предоставления данных о задачах;
- /var/log/kaspersky/kics4net-vault/ – для сервиса хранения секретов в хранилище;
- /var/log/kaspersky/kics4net-webserver/ – для веб-сервера (также веб-сервер сохраняет данные о работе процессов в системном журнале операционной системы);
- /var/log/kaspersky/klnagent64/ – для Агента администрирования.

- Директории для хранения конфигурационных файлов:
  - /etc/opt/kaspersky/kics4net/ – для Сервера;
  - /etc/opt/kaspersky/kics4net-asset-config-repo/ – для сервиса хранения конфигураций устройств;
  - /etc/opt/kaspersky/kics4net-asset-inventory/ – для сервиса обработки результатов сканирования атрибутов устройств с помощью OVAL-правил;
  - /etc/opt/kaspersky/kics4net-blob-storage/ – для сервиса BLOB;
  - /etc/opt/kaspersky/kics4net-config-control-orchestrator/ – для сервиса управления процессами контроля конфигураций и активного опроса;
  - /etc/opt/kaspersky/kics4net-email-gateway/ – для сервиса отправки почтовых уведомлений;
  - /etc/opt/kaspersky/kics4net-epp-proxy/ – для сервиса интеграции;
  - /etc/opt/kaspersky/kics4net-fts/ – для системы полнотекстового поиска;
  - /etc/opt/kaspersky/kics4net-nats-server/ – для брокера сообщений;
  - /etc/opt/kaspersky/kics4net-oval-facade/ – для сервиса сканирования удаленных устройств по OVAL-правилам;
  - /etc/opt/kaspersky/kics4net-report-builder/ – для сервиса формирования отчетов;
  - /etc/opt/kaspersky/kics4net-report-data-source/ – для сервиса предоставления данных для отчетов;
  - /etc/opt/kaspersky/kics4net-report-renderer/ – для сервиса представления блоков данных в отчетах;
  - /etc/opt/kaspersky/kics4net-report-templates-catalog/ – для сервиса управления шаблонами отчетов;

- /etc/opt/kaspersky/kics4net-report-templates-catalog-view/ – для сервиса предоставления данных о шаблонах отчетов;
- /etc/opt/kaspersky/kics4net-responses-manager/ – для сервиса управления заданиями реагирования;
- /etc/opt/kaspersky/kics4net-risk-oval-detector/ – для сервиса обработки результатов сканирования устройств с помощью OVAL-правил на предмет наличия рисков;
- /etc/opt/kaspersky/kics4net-scan-oval-manager/ – для сервиса управлением сканирования устройств с помощью OVAL-правил;
- /etc/opt/kaspersky/kics4net-scap-manager/ – для сервиса управления аудита безопасности;
- /etc/opt/kaspersky/kics4net-scap-manager-view/ – для сервиса предоставления данных об аудите безопасности;
- /etc/opt/kaspersky/kics4net-scheduler/ – для сервиса планировщика задач;
- /etc/opt/kaspersky/kics4net-secrets/ – для фасада к хранилищу секретов;
- /etc/opt/kaspersky/kics4net-task-manager/ – для сервиса управления задачами;
- /etc/opt/kaspersky/kics4net-task-manager-view/ – для сервиса предоставления данных о задачах;
- /etc/opt/kaspersky/kics4net-vault/ – для сервиса хранения секретов в хранилище;
- /etc/opt/kaspersky/kics4net-webserver/ – для веб-сервера;
- /etc/opt/kaspersky/klnagent/ – для Агента администрирования;
- /usr/lib/systemd/system/ – для размещения конфигурационных файлов сервисов Kaspersky Industrial CyberSecurity for Networks (например, kics4net.service);
- /var/opt/kaspersky/kics4net-deploy/ – для хранения копии файла параметров установки, созданного при централизованной установке программы;
- /var/run/ – для хранения переменных данных о состоянии системы после загрузки в самой директории (например, файл klnagent.pid) или в поддиректориях (например, в поддиректории /kics4net/).

На сенсоре Kaspersky Industrial CyberSecurity for Networks программа использует для хранения данных следующие директории и их поддиректории:

- Директории установки компонентов и сервисов:
  - /opt/kaspersky/kics4net/ – для сенсора;
  - /opt/kaspersky/kics4net-apm/ – для коннектора активного опроса;
  - /opt/kaspersky/kics4net-connectors/ – для системных коннекторов;
  - /opt/kaspersky/kics4net-connectors-launcher/ – для сервиса регистрации и запуска управляемых коннекторов;
  - /opt/kaspersky/kics4net-epp-proxy/ – для сервиса интеграции;
  - /opt/kaspersky/kics4net-nats-server/ – для брокера сообщений;
  - /opt/kaspersky/kics4net-oval-facade/ – для сервиса сканирования удаленных устройств по OVAL-правилам;
  - /opt/kaspersky/kics4net-suricata/ – для системы обнаружения вторжений;
  - /opt/kaspersky/kics4net-websensor/ – для веб-сервера.
- Директории для хранения сертификатов и рабочих данных:
  - /opt/kaspersky/kics4net/share/ids/ – для системы обнаружения вторжений;
  - /var/opt/kaspersky/kics4net/ – для сенсора;
  - /var/opt/kaspersky/kics4net-apm/ – для коннектора активного опроса;
  - /var/opt/kaspersky/kics4net-connectors/ – для системных коннекторов;
  - /var/opt/kaspersky/kics4net-connectors-launcher/ – для сервиса регистрации и запуска управляемых коннекторов;
  - /var/opt/kaspersky/kics4net-epp-proxy/ – для сервиса интеграции;
  - /var/opt/kaspersky/kics4net-nats-server/ – для брокера сообщений;
  - /var/opt/kaspersky/kics4net-oval-facade/ – для сервиса сканирования устройств с помощью OVAL-правил без Агента администрирования;
  - /var/opt/kaspersky/kics4net-websensor/ – для веб-сервера.

- Директории для хранения журналов работы процессов:
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – для хранения журналов работы процессов установки и файла параметров установки (если централизованная установка компонентов программы выполнялась с этого компьютера);
  - /var/log/kaspersky/kics4net/ – для сенсора;
  - /var/log/kaspersky/kics4net-apm/ – для коннектора активного опроса;
  - /var/log/kaspersky/kics4net-connectors/ – для системных коннекторов;
  - /var/log/kaspersky/kics4net-connectors-launcher/ – для сервиса регистрации и запуска управляемых коннекторов;
  - /var/log/kaspersky/kics4net-epp-proxy/ – для сервиса интеграции;
  - /var/log/kaspersky/kics4net-nats-server/ – для брокера сообщений;
  - /var/log/kaspersky/kics4net-oval-facade/ – для сервиса сканирования удаленных устройств по OVAL-правилам;
  - /var/log/kaspersky/kics4net-suricata/ – для системы обнаружения вторжений;
  - /var/log/kaspersky/kics4net-websensor/ – для веб-сервера (также веб-сервер сохраняет данные о работе процессов в системном журнале операционной системы).
- Директории для хранения конфигурационных файлов:
  - /etc/opt/kaspersky/kics4net/ – для сенсора;
  - /etc/opt/kaspersky/kics4net-epp-proxy/ – для сервиса интеграции;
  - /etc/opt/kaspersky/kics4net-nats-server/ – для брокера сообщений;
  - /etc/opt/kaspersky/kics4net-oval-facade/ – для сервиса сканирования удаленных устройств по OVAL-правилам;
  - /etc/opt/kaspersky/kics4net-websensor/ – для веб-сервера;
  - /etc/opt/kaspersky/klnagent/ – для Агента администрирования;
  - /usr/lib/systemd/system/ – для размещения конфигурационных файлов сервисов Kaspersky Industrial CyberSecurity for Networks (например, kics4net.service);
  - /var/opt/kaspersky/kics4net-deploy/ – для хранения копии файла параметров установки, созданного при централизованной установке программы;
  - /var/run/ – для хранения переменных данных о состоянии системы после загрузки в самой директории или в поддиректориях.

Для изменения файлов программы нужно иметь root-права в операционной системе.

О журналах

Kaspersky Industrial CyberSecurity for Networks сохраняет данные о своей работе в журналах. В зависимости от типа журнала программа сохраняет данные в базе данных Сервера или в файлах в локальных директориях на узле Сервера или сенсора.

Журналы, сохраняемые в базе данных Сервера

Программа размещает в базе данных Сервера следующие журналы:

- журнал событий и инцидентов;
- журнал аудита;
- журнал сообщений программы.

Вы можете просматривать содержимое перечисленных журналов при подключении к Серверу через веб-интерфейс.

При необходимости вы также можете настроить передачу данных из этих журналов в сторонние системы через коннекторы.

Журналы, сохраняемые в файлах

Информация о работе процессов программы сохраняется в виде файлов в локальных директориях. Файлы с журналами работы процессов могут содержать следующую информацию:

- данные о запуске и остановке процессов Kaspersky Industrial CyberSecurity for Networks;
- диагностические сообщения, которые могут потребоваться при обращении в Службу технической поддержки;
- сообщения об ошибках.

Информация о работе процессов сохраняется в соответствии с заданными уровнями ведения журналов работы процессов.

Вы можете просматривать файлы с журналами работы процессов с помощью текстового редактора. Для доступа к журналам нужно иметь root-права в операционной системе.

Файлы с журналами работы процессов хранятся в незашифрованном виде. Рекомендуется обеспечить защиту информации от несанкционированного доступа.

Администрирование Kaspersky Industrial CyberSecurity for Networks

Этот раздел содержит информацию о действиях для администрирования Kaspersky Industrial CyberSecurity for Networks.

Развертывание узлов

Для развертывания узлов с установленными компонентами программы вы можете добавлять и удалять сенсоры, настраивать параметры хранения данных программы на узлах, а также управлять функциями защиты.

Если вы будете использовать Сервер без внешних сенсоров, вам не нужно добавлять сенсоры после установки программы. В этом случае параметры развертывания потребуется настроить только для узла Сервера. Для способа установки Сервера и внешних сенсоров вы можете добавлять сенсоры при подключении к Серверу через веб-интерфейс. В программе используются только те сенсоры, которые добавлены в программу и подключены.

По умолчанию для хранения данных программы на Сервере и сенсорах заданы параметры, обеспечивающие долговременный срок хранения и оптимальное использование свободного пространства на диске. При необходимости вы можете изменить параметры хранения данных на каком-либо узле с учетом особенностей вашей системы (например, если аппаратное обеспечение компьютера не вполне соответствует требованиям).

Программа контролирует работу имеющихся точек мониторинга и предусмотренных технологий, чтобы своевременно оповещать пользователя о недействующих функциях защиты в программе. Если какие-либо точки мониторинга или технологии не включены, программа отображает сообщение о выключенных функциях защиты. Такое сообщение отображается и для технологий, которые работают в режиме обучения (этот режим доступен для некоторых технологий). Выключать точки мониторинга и технологии, а также использовать режим обучения технологий, рекомендуется на ограниченное время. Например, вы можете выключить точку мониторинга на время проведения профилактических и пусконаладочных работ в соответствующем сегменте промышленной сети.

Вы можете просматривать сведения об узлах и управлять параметрами развертывания в разделе **Параметры** → **Развертывание** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks. Управлять параметрами развертывания могут только пользователи с ролью Администратор.

Добавление и удаление сенсоров

После установки и начальной настройки Сервера Kaspersky Industrial CyberSecurity for Networks вы можете добавлять сенсоры в программу. Добавление сенсоров выполняется на странице веб-интерфейса Сервера.

Для добавления сенсора на компьютере должны быть установлены соответствующие пакеты из комплекта поставки программы. Вы можете установить эти пакеты с помощью скрипта централизованной установки компонентов программы или скрипта локальной установки.

Вы можете удалить сенсор из программы. При удалении сенсора на Сервере программы удаляются регистрационные данные этого сенсора, в результате чего подключение сенсора к этому Серверу будет невозможно.

После удаления сенсора на этом узле остаются файлы компонента сенсора. В дальнейшем вы можете заново добавить этот узел в качестве сенсора без необходимости устанавливать соответствующие пакеты. Причем добавление сенсора возможно как к текущему Серверу, так и к любому другому Серверу Kaspersky Industrial CyberSecurity for Networks, с которым есть соединение.

Добавление и подключение сенсора с использованием веб-интерфейса сенсора

При добавлении сенсора на Сервере формируется конфигурационный пакет, содержащий сертификат и конфигурационные данные для сенсора. Подключение добавленного сенсора выполняется с использованием веб-интерфейса сенсора. Веб-интерфейс сенсора позволяет загрузить конфигурационный пакет и подключить сенсор следующими способами:

- С помощью файла свертки. Для этого способа конфигурационный пакет сохраняется в виде файла, в котором сертификат защищен паролем. Этот файл называется *файлом свертки*. Файл свертки требуется безопасно доставить на компьютер, имеющий доступ по сети к компьютеру сенсора, и загрузить на странице веб-интерфейса сенсора. После загрузки файла свертки сенсор автоматически подключается к Серверу, на котором был создан этот файл.

- Автоматически по сети. Этот способ позволяет передать конфигурационный пакет по сети на указанный IP-адрес компьютера сенсора. Сенсор обрабатывает конфигурационный пакет, формирует на его основе запрос на подпись сертификата (CSR) и отправляет этот запрос на Сервер. После получения запроса на странице веб-интерфейса Сервера отображается отпечаток полученного запроса в виде последовательности символов. Такой же отпечаток запроса в это время отображается и на странице веб-интерфейса сенсора. Вам нужно убедиться в идентичности отпечатков перед завершением добавления сенсора.

Добавление и подключение сенсора с помощью файла свертки

Чтобы добавить и подключить сенсор с помощью файла свертки:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Развертывание**.

3. Нажмите на кнопку **Добавить сенсор**.

   В правой части окна веб-интерфейса появится область деталей.

4. На вкладке **С помощью файла свертки** выполните следующие действия:

   a. Введите имя сенсора, под которым сенсор будет представлен в составе решения Kaspersky Industrial CyberSecurity for Networks.

   Имя сенсора должно быть уникальным (не совпадать с именами других сенсоров и Сервера) и может содержать не более 100 символов. Вы можете использовать буквы латинского алфавита, цифры, пробел, а также специальные символы `_` и `-` (например, `Sensor_1`). Имя сенсора должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

   b. Введите IP-адрес Сервера, который будет использовать сенсор для подключения к Серверу.

   c. Введите IP-адрес, используемый веб-сервером на компьютере сенсора.

   d. Введите пароль, с помощью которого будет зашифрован сертификат в файле свертки.

   Пароль должен удовлетворять следующим требованиям:

   - содержит от 8 до 256 символов ASCII;
   - содержит одну или несколько прописных букв латинского алфавита;
   - содержит одну или несколько строчных букв латинского алфавита;
   - содержит одну или несколько цифр;
   - содержит не более трех одинаковых символов подряд.

5. Нажмите на кнопку **Создать файл свертки**. Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

6. Подключитесь к сенсору через веб-интерфейс.

7. На странице веб-интерфейса сенсора нажмите на кнопку **Выберите файл**.

   Откроется стандартное окно используемого браузера для выбора файла.

8. Укажите путь к файлу свертки.

9. Нажмите на кнопку открытия файла.

10. После загрузки содержимого файла введите пароль для доступа к сертификату сенсора в файле свертки.

Сенсор подключится к Серверу, после чего на страницах веб-интерфейса сенсора и Сервера отобразятся сведения о подключении.

Добавление и подключение сенсора автоматически по сети

Чтобы добавить и подключить сенсор автоматически по сети:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Развертывание**.

3. Нажмите на кнопку **Добавить сенсор**.

   В правой части окна веб-интерфейса появится область деталей.

4. На вкладке **Автоматически по сети** выполните следующие действия:

   a. Введите имя сенсора, под которым сенсор будет представлен в составе решения Kaspersky Industrial CyberSecurity for Networks.

      Имя сенсора должно быть уникальным (не совпадать с именами других сенсоров и Сервера) и может содержать не более 100 символов. Вы можете использовать буквы латинского алфавита, цифры, пробел, а также специальные символы `_` и `-` (например, `Sensor_1`). Имя сенсора должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

   b. Введите IP-адрес Сервера, который будет использовать сенсор для подключения к Серверу.

   c. Введите IP-адрес, используемый веб-сервером на компьютере сенсора.

5. Нажмите на кнопку **Соединиться и добавить сенсор**.

   Программа установит соединение с компьютером сенсора, после чего на странице веб-интерфейса Сервера появится запрос для подтверждения полученного отпечатка запроса на подпись сертификата.

6. Подключитесь к сенсору через веб-интерфейс.

   На странице веб-интерфейса сенсора отобразится сообщение, содержащее информацию об отпечатке запроса сертификата, который был отправлен на Сервер.

7. Убедитесь в идентичности последовательностей символов, представляющих отпечаток запроса сертификата на страницах веб-интерфейса сенсора и Сервера.

8. На странице веб-интерфейса Сервера нажмите на кнопку подтверждения полученного отпечатка запроса сертификата.

Сенсор подключится к Серверу, после чего на страницах веб-интерфейса сенсора и Сервера отобразятся сведения о подключении.

Создание нового файла свертки для сенсора

При необходимости вы можете создать для сенсора новый файл свертки (например, если требуется обновить сертификат, используемый для соединения сенсора с Сервером).

Чтобы создать новый файл свертки для сенсора:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Развертывание**.

3. Выберите карточку узла того сенсора, для которого вы хотите создать новый файл свертки.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Получить новый файл свертки**. Если кнопка не отображается в панели инструментов, нажмите на кнопку ⋮ и выберите нужный пункт в открывшемся меню.

5. В открывшемся окне **Генерация нового файла свертки** выполните следующие действия:

   a. Введите IP-адрес Сервера, который будет использовать сенсор для подключения к Серверу.

   b. Введите пароль, с помощью которого будет зашифрован сертификат в файле свертки.

      Пароль должен удовлетворять следующим требованиям:

      - содержит от 8 до 256 символов ASCII;
      - содержит одну или несколько прописных букв латинского алфавита;
      - содержит одну или несколько строчных букв латинского алфавита;
      - содержит одну или несколько цифр;
      - содержит не более трех одинаковых символов подряд.

6. Нажмите на кнопку **Создать файл**.

   Сервер сформирует новый файл свертки для выбранного сенсора, после чего браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

7. На компьютере сенсора переведите сенсор в начальное состояние с помощью скрипта для локального перевода узла в начальное состояние kics4net-reset-to-defaults.sh. Скрипт находится на компьютере с установленным компонентом программы в директории /opt/kaspersky/kics4net/sbin/.

8. Подключитесь к сенсору через веб-интерфейс.

9. На странице веб-интерфейса сенсора загрузите новый файл свертки.

   Загрузка нового файла свертки выполняется аналогично, как при добавлении сенсора с помощью файла свертки.

Удаление сенсора

Чтобы удалить сенсор:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Развертывание**.

3. Выберите карточку узла того сенсора, который вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

5. В окне запроса нажмите на кнопку **OK**.

Изменение основных параметров узла

Для Сервера и добавленных сенсоров вы можете изменять следующие основные параметры:

- параметры хранения данных программы на узле;
- имя узла;
- параметры использования внешнего хранилища для файлов дампа трафика.

Изменение параметров хранения данных программы на узле

Вы можете изменить ограничения максимального объема для хранения данных программы на узле.

Чтобы изменить ограничения максимального объема:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку нужного узла.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров узла.
5. На вкладке **Общие** в блоке **Параметры хранения** задайте ограничения максимального объема для данных программы. Набор типов данных, доступных для настройки, зависит от типа узла (Сервер или сенсор).

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   Для некоторых типов данных (например, для событий) вы можете задать ограничение времени хранения в днях.
6. Нажмите на кнопку **Сохранить**.

Изменение имени узла с установленным компонентом программы

Вы можете изменить заданное имя узла с установленным компонентом программы (Сервера или сенсора).

Чтобы изменить имя узла:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.

3. Выберите карточку нужного узла.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.

5. В поле с текущим именем узла введите новое имя.

   Имя узла должно быть уникальным (не совпадать с именами других узлов) и может содержать не более 100 символов. Вы можете использовать буквы латинского алфавита, цифры, пробел, а также специальные символы _ и - (например, Server_1). Имя узла должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

6. Нажмите на кнопку **Сохранить**.

Подключение и настройка внешнего хранилища для файлов дампа трафика

Программа сохраняет трафик, полученный через точки мониторинга, в виде файлов дампа трафика. Для оперативного хранения файлов и анализа трафика, сохраненного в этих файлах, программа использует внутреннее хранилище на каждом узле. Программа сохраняет и удаляет файлы во внутреннем хранилище в соответствии с заданными параметрами для внутреннего хранилища на узле. Если вы хотите обеспечить долговременное хранение файлов дампа трафика, вы можете подключить и настроить внешнее хранилище на узле. Файлы дампа трафика, хранящиеся во внешнем хранилище, можно использовать для загрузки трафика в файлы формата PCAP (например, для загрузки трафика сетевых сеансов, если файлы дампа этого трафика уже удалены из внутреннего хранилища на узле).

Для внешнего хранилища вам нужно использовать директорию в локальной файловой системе компьютера узла. Эту директорию нужно монтировать на жесткий диск, на котором достаточно свободного пространства и не располагается директория /var/. Вы также можете использовать для внешнего хранилища директорию, на которую выполнено монтирование общего сетевого ресурса другого компьютера (например, директорию, аналогичную директории для экспорта событий на сетевой ресурс). К директории в локальной файловой системе должны быть предоставлены права доступа для учетной записи kics4net (включая права на создание вложенных директорий).

Действия для создания и монтирования директории для внешнего хранилища выполняются с помощью стандартных средств операционной системы на компьютере узла.

Чтобы подключить и настроить внешнее хранилище для файлов дампа трафика на узле:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Развертывание**.

3. Выберите карточку нужного узла.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров узла.

5. Перейдите на вкладку **Внешнее хранилище** и включите режим использования внешнего хранилища с помощью переключателя **Подключить внешнее хранилище для файлов дампа трафика**.

6. Укажите путь к директории для внешнего хранилища в локальной файловой системе узла.

7. Задайте ограничение занимаемого объема для хранения файлов дампа трафика в блоке параметров **Максимальный объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

8. При необходимости в блоке **Фильтрация сохраняемого трафика** включите фильтрацию и введите выражение для фильтрации с использованием технологии BPF (Berkley Packet Filter) по адресным параметрам в сетевых пакетах.

   Фильтрация позволяет сократить объем сохраняемого трафика за счет отбрасывания сетевых пакетов, не удовлетворяющих фильтру. Однако в этом случае вам нужно учитывать, что при последующем просмотре файлов дампа трафика или при загрузке трафика из этих файлов вы не сможете загрузить сетевые пакеты, отброшенные во время сохранении трафика.

9. При необходимости в блоке **Ограничение времени хранения** включите ограничение на минимальное время хранения файлов и укажите нужное количество дней для хранения.

10. Нажмите на кнопку **Сохранить**.

Управление точками мониторинга на узлах

Для получения и обработки трафика промышленной сети в Kaspersky Industrial CyberSecurity for Networks используются точки мониторинга. Точки мониторинга можно добавлять и удалять на любом узле с установленными компонентами программы (в том числе на узле, который выполняет функции Сервера). При этом не требуется перезагружать компьютер, на котором установлены компоненты программы, или выполнять переустановку компонентов на этом компьютере.

Каждая точка мониторинга должна быть связана с сетевым интерфейсом, на который поступает копия трафика из определенного сегмента промышленной сети. Для добавления точек мониторинга вы можете использовать сетевые интерфейсы, которые удовлетворяют следующим условиям:

- Тип сетевого интерфейса: Ethernet.
- MAC-адрес: отличается от 00:00:00:00:00:00.
- Сетевой интерфейс предназначен для получения копии трафика промышленной сети и этот интерфейс не используется в других целях (например, для соединения узлов с установленными компонентами программы).

Точки мониторинга можно включать и выключать. Вы можете выключить точку мониторинга, чтобы временно прекратить наблюдение за сегментом промышленной сети, из которого поступает копия трафика на сетевой интерфейс. Как только вам потребуется продолжить наблюдение за сегментом промышленной сети, вы можете включить точку мониторинга.

После выключения или удаления точки мониторинга программа в течение некоторого времени может регистрировать события, в которых указана эта точка мониторинга. Это связано с возможной задержкой обработки поступившего трафика во время высокой загруженности Сервера.

Добавление точки мониторинга

Для получения и обработки трафика, поступающего из промышленной сети на сетевой интерфейс узла, вам нужно добавить точку мониторинга на этот сетевой интерфейс.

Добавлять точки мониторинга на сетевые интерфейсы могут только пользователи с ролью Администратор.

Чтобы добавить точку мониторинга на сетевой интерфейс:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Откройте область деталей по ссылке **Добавить точку мониторинга** в карточке нужного сетевого интерфейса. Ссылка отображается, если точка мониторинга не добавлена на сетевой интерфейс.

   В правой части окна веб-интерфейса появится область деталей.
4. В поле ввода в верхней части области деталей введите имя точки мониторинга.

   Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, символы `_` и `-`.

   Имя точки мониторинга должно удовлетворять следующим требованиям:

   - является уникальным (не присвоено другой точке мониторинга);
   - содержит от 1 до 100 символов.
5. Нажмите на кнопку **Добавить точку мониторинга**.

Включение точек мониторинга

Программа не получает и не обрабатывает трафик, поступающий на сетевой интерфейс выключенной точки мониторинга. Вам нужно включить точку мониторинга, если вы хотите возобновить получение и обработку трафика.

Вы можете включать точки мониторинга как по отдельности, так и одновременно на одном узле или на всех узлах.

Включать точки мониторинга могут только пользователи с ролью Администратор.

Чтобы включить точки мониторинга:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.

3. Выполните одно из следующих действий:

   - Если вы хотите включить одну точку мониторинга, нажмите на кнопку **Включить** в карточке сетевого интерфейса с точкой мониторинга. Кнопка доступна, если точка мониторинга выключена.

   - Если вы хотите включить все точки мониторинга на узле, нажмите на кнопку **Включить все** в карточке узла, к которому относятся выключенные точки мониторинга. Кнопка доступна, если на узле есть сетевые интерфейсы с выключенными точками мониторинга.

   - Если вы хотите включить все точки мониторинга на всех узлах, воспользуйтесь ссылкой **Включить на всех узлах** в панели инструментов.

4. Дождитесь применения изменений.

Выключение точек мониторинга

Вы можете выключить точку мониторинга, если требуется временно приостановить получение и обработку трафика на сетевом интерфейсе этой точки мониторинга.

Вы можете выключать точки мониторинга как по отдельности, так и одновременно на одном узле или на всех узлах.

Выключать точки мониторинга могут только пользователи с ролью Администратор.

Чтобы выключить точки мониторинга:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Развертывание**.

3. Выполните одно из следующих действий:

   - Если вы хотите выключить одну точку мониторинга, нажмите на кнопку **Выключить** в карточке сетевого интерфейса с точкой мониторинга. Кнопка доступна, если точка мониторинга включена.

   - Если вы хотите выключить все точки мониторинга на узле, нажмите на кнопку **Выключить все** в карточке узла, к которому относятся включенные точки мониторинга. Кнопка доступна, если на узле есть сетевые интерфейсы с включенными точками мониторинга.

   - Если вы хотите выключить все точки мониторинга на всех узлах, воспользуйтесь ссылкой **Выключить на всех узлах** в панели инструментов.

4. Дождитесь применения изменений.

Переименование точки мониторинга

Вы можете переименовать точку мониторинга, связанную с сетевым интерфейсом.

> Новое имя точки мониторинга появится в событиях, зарегистрированных после ее переименования. В ранее зарегистрированных событиях отображается старое имя точки мониторинга.

Переименовать точку мониторинга могут только пользователи с ролью Администратор.

Чтобы переименовать точку мониторинга:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку сетевого интерфейса с точкой мониторинга, которую вы хотите переименовать.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить** и введите новое имя в появившемся поле.

   Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, символы `_` и `-`.

   Имя точки мониторинга должно удовлетворять следующим требованиям:

   - является уникальным (не присвоено другой точке мониторинга);
   - содержит от 1 до 100 символов.
5. Нажмите на кнопку **Сохранить**.

Удаление точки мониторинга

Вы можете удалить точку мониторинга, связанную с сетевым интерфейсом. Удаление точки мониторинга может потребоваться, если этот сетевой интерфейс больше не будет использоваться для получения трафика промышленной сети.

В случае, если требуется временно приостановить получение трафика на сетевом интерфейсе точки мониторинга (например, на время проведения профилактических и пусконаладочных работ), вы можете выключить точку мониторинга, не удаляя ее.

> В базе данных не удаляется трафик, полученный с точки мониторинга до ее удаления. Также информация об этой точке мониторинга сохраняется в таблице зарегистрированных событий.

Удалить точку мониторинга могут только пользователи с ролью Администратор.

Чтобы удалить точку мониторинга:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку сетевого интерфейса с точкой мониторинга, которую вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.
4. В области деталей нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения. Если точка мониторинга включена, программа предложит выключить точку мониторинга.
5. В окне запроса подтвердите удаление точки мониторинга.

Определение Ethernet-порта, связанного с сетевым интерфейсом

Компьютер, на котором установлены компоненты программы, может иметь несколько Ethernet-портов для подключения к локальной сети. С помощью программы вы можете включить режим индикации для сетевого интерфейса и определить, какой Ethernet-порт связан с этим интерфейсом. При включенном режиме индикации рядом с Ethernet-портом в течение 15 секунд мигает LED-индикатор.

Если сетевой интерфейс не поддерживает LED-индикацию (например, рядом с Ethernet-портом отсутствует LED-индикатор или сетевой интерфейс является объединенным логическим интерфейсом), при включении режима индикации возникает ошибка.

Включать режим индикации Ethernet-порта могут только пользователи с ролью Администратор.

Чтобы определить Ethernet-порт, связанный с сетевым интерфейсом:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Нажмите на кнопку **LED-тест** в карточке сетевого интерфейса.

   Если сетевой интерфейс поддерживает LED-индикацию, в карточке сетевого интерфейса начнет мигать значок подключения сетевого кабеля. Одновременно на соответствующем сетевом адаптере компьютера начнет мигать LED-индикатор рядом с Ethernet-портом.

Пока включен режим индикации для одного сетевого интерфейса, вы не можете включить режим индикации для другого сетевого интерфейса на этом же узле.

Управление технологиями

В Kaspersky Industrial CyberSecurity for Networks используются различные технологии для анализа трафика промышленной сети. Вы можете включать и выключать использование технологий по отдельности. Для некоторых технологий доступна возможность выбора режима работы: режим обучения или режим наблюдения.

Режим обучения технологий рекомендуется включать на заранее определенное время, чтобы программа автоматически переводила технологии в режим наблюдения в нужный момент. Режим наблюдения является штатным для использования технологий (в отличие от режима обучения, при котором программа только накапливает данные для дальнейшего использования). При настройке режима обучения вы можете задать нужное время для автоматического переключения технологии в режим наблюдения.

Вы можете настроить одинаковые параметры использования технологий на всех узлах и точках мониторинга или настроить специфические параметры для некоторых узлов и/или точек мониторинга. Параметры использования технологий могут автоматически наследоваться от родительских объектов к дочерним. Если включено наследование технологий для узла или точки мониторинга, на этом объекте применяются параметры использования технологий, заданные для родительского объекта (Сервера или сенсора). Если наследование технологий выключено, вы можете настроить на этом узле или точке мониторинга специфические параметры использования технологий.

По умолчанию после установки программы включены все технологии, за исключением контроля проектов ПЛК и обнаружения неизвестных тегов. Для технологий, поддерживающих изменение режима, по умолчанию включен режим обучения. При добавлении сенсоров и точек мониторинга в программу для этих объектов по умолчанию включено наследование технологий, заданных для родительского объекта.

Включение и выключение технологий

Вы можете включать и выключать использование технологий для Сервера, сенсоров и точек мониторинга. При этом включение и выключение технологий на сенсорах и точках мониторинга доступно, если на этих объектах выключено наследование технологий.

Некоторые технологии включают в себя методы, которые можно включать или выключать по отдельности. Если технология или метод выключены, программа не контролирует взаимодействия устройств по этой технологии или по этому методу. При этом вы можете настраивать параметры работы программы, относящиеся к выключенным технологиям или методам (например, добавлять или изменять правила).

Включение и выключение поддерживается для следующих технологий и методов:

- Контроль активов:
  - Обнаружение активности устройств.
  - Обнаружение сведений об устройствах.
  - Контроль проектов ПЛК.
  - Обнаружение сетевых сессий.
  - Обнаружение рисков (только на узле Сервера).
- Контроль сети:
  - Контроль целостности сети.
  - Контроль системных команд.

- Контроль процесса:
  - Контроль процесса по правилам.
  - Обнаружение неизвестных тегов.
  - Обнаружение устройств для контроля процесса.
- Обнаружение вторжений:
  - Обнаружение вторжений по правилам.
  - Обнаружение ARP-спуфинга.
  - Обнаружение аномалий в протоколе IP.
  - Обнаружение аномалий в протоколе TCP.
  - Обнаружение атак подбора и сканирования.

По умолчанию после установки программы включены не все технологии и методы. Для повышения защищенности программы вам нужно включить метод Обнаружение атак подбора и сканирования, если этот метод выключен. Использование этого метода должно быть включено для Сервера, а также для всех сенсоров и точек мониторинга в программе. Кроме того, метод Обнаружение атак подбора и сканирования, совместно с другими технологиями и методами, обеспечивает работу программы в сертифицированном состоянии после установки актуальных обновлений баз и программных модулей.

В этой статье описана процедура включения и выключения технологий на узле Сервера. Действия для включения и выключения технологий на узлах сенсоров и на точках мониторинга выполняются аналогично после выключения наследования технологий на этих объектах.

Чтобы изменить состояние технологий и методов на узле Сервера:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку Сервера.

   В правой части окна веб-интерфейса появится область деталей. На вкладке **Управление технологиями** отобразится список технологий и методов, доступных для включения и выключения.

   Если изменение состояний технологий и методов невозможно в текущий момент, переключатели в списке недоступны. В этом случае рекомендуется проверить статус сервиса kics4net на компьютере Сервера. Если сервис не активен, требуется его запустить.
4. Включите или выключите применение нужных технологий и/или методов с помощью переключателей слева. Вы можете включить или выключить все технологии и методы одновременно с помощью ссылок **Включить все** и **Выключить все**.
5. После включения или выключения технологии или метода дождитесь применения изменений. До завершения перевода в другое состояние переключатель недоступен.

Настройка режимов работы технологий

Вы можете настраивать режим обучения технологий или вручную включать режим наблюдения для Сервера, сенсоров и точек мониторинга. При этом указанные действия доступны на сенсорах и точках мониторинга, если на этих объектах выключено наследование технологий.

Изменение режима поддерживается для следующих технологий и методов:

- Обнаружение активности устройств.
- Контроль системных команд.
- Контроль процесса по правилам.
- Контроль целостности сети.

В этом разделе описана процедура изменения и настройки режимов технологий на узле Сервера. Действия для изменения и настройки режимов технологий на узлах сенсоров и на точках мониторинга выполняются аналогично после выключения наследования технологий.

Чтобы изменить и настроить режимы технологий и методов на узле Сервера:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку Сервера.

   В правой части окна веб-интерфейса появится область деталей. На вкладке **Управление технологиями** отобразится список технологий и методов, доступных для включения и выключения.

   > Если изменение режимов работы технологий и методов невозможно в текущий момент, переключатели в списке недоступны. В этом случае рекомендуется проверить статус сервиса kics4net на компьютере Сервера. Если сервис не активен, требуется его запустить.

4. Для технологий и методов, поддерживающих работу в режиме обучения, выберите нужный режим (**Обучение** или **Наблюдение**) в раскрывающемся списке справа от названия технологии или метода. Если вы хотите выбрать одинаковый режим для всех этих технологий и методов, используйте раскрывающийся список **Режим**.

   При выборе разных режимов раскрывающийся список **Режим** отображает значение **Смешанный**.

5. После выбора режима дождитесь применения изменений. До применения режима в раскрывающемся списке отображается статус **Изменение**.
6. Для технологий и методов в режиме обучения укажите дату и время автоматического переключения в режим наблюдения. Для этого нажмите на ссылку **Указать срок** и выберите дату и время. Если дата и время были настроены ранее, то они отображаются напротив названия режима.

Управление наследованием технологий

Если вы хотите, чтобы сенсор или точка мониторинга автоматически получали параметры использования технологий, настроенные для родительского объекта, вы можете включить наследование технологий. При этом сенсор получает параметры использования технологий, заданные для Сервера, а точка мониторинга получает параметры, заданные для того узла, на котором точка мониторинга была добавлена (для Сервера или для сенсора).

При необходимости вы можете выключить наследование технологий на сенсоре или точке мониторинга. Это позволит настроить на этом объекте специфические параметры использования технологий.

Чтобы включить или выключить наследование технологий на узле сенсора:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку сенсора.

   В правой части окна веб-интерфейса появится область деталей.
4. Установите переключатель **Наследовать технологии Сервера** в нужное положение.

Чтобы включить или выключить наследование технологий на точке мониторинга:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку сетевого интерфейса с точкой мониторинга, для которой вы хотите включить или выключить наследование технологий.

   В правой части окна веб-интерфейса появится область деталей.
4. Установите переключатель для наследования технологий в нужное положение.

Загрузка трафика, поступившего на точки мониторинга узлов

Вы можете загружать трафик, поступивший в программу через точки мониторинга на узлах. Загрузка трафика выполняется в файл формата PCAP. Для загрузки нужных данных вы можете настраивать фильтрацию сетевых пакетов.

Программа загружает трафик из хранилищ с файлами дампа трафика. Для загрузки может использоваться как внутреннее хранилище каждого узла (созданное автоматически при установке компонента программы на узле), так и внешнее хранилище, если оно подключено на узле.

При загрузке трафика вам нужно учитывать следующие особенности:

- Файлы дампа трафика хранятся в хранилищах временно и автоматически удаляются по мере поступления нового трафика (периодичность удаления файлов зависит от интенсивности поступающего трафика и от заданных параметров хранения данных программы). Загрузка трафика невозможна, если соответствующие ему файлы дампа трафика уже удалены из хранилищ.

- Загружать трафик, поступивший на точки мониторинга узлов, могут только пользователи с ролью Администратор.

Чтобы загрузить трафик, поступивший на точки мониторинга узлов:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Развертывание**.

3. Выполните одно из следующих действий:

   - Если вы хотите загрузить трафик, поступивший на точки мониторинга определенного узла, выберите карточку этого узла.

   - Если вы хотите загрузить трафик, поступивший на определенную точку мониторинга, выберите карточку сетевого интерфейса с этой точкой мониторинга.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Скачать трафик**. Если кнопка не отображается в панели инструментов, нажмите на кнопку ⋮ и выберите нужный пункт в открывшемся меню.

5. В открывшемся окне выполните следующие действия:

   - Если вы хотите загрузить трафик за определенный период времени, задайте нужные границы с помощью параметра **Период трафика для скачивания**.

     По умолчанию задан период длительностью один час.

   - Задайте ограничение максимального объема для загрузки трафика в блоке **Ограничение объема скачивания**.

     Если объем загружаемого трафика превысит заданное ограничение, будет отброшен более поздний трафик.

   - Если выбрана карточка узла, при необходимости включите фильтрацию в блоке **Фильтрация по точкам мониторинга** и укажите точки мониторинга этого узла, на которые поступал нужный трафик (блок отображается, если выбрана карточка узла).

     По умолчанию заданы все точки мониторинга, имеющиеся на выбранном узле.

   - При необходимости включите фильтрацию в блоке **Фильтрация по адресным пространствам** и укажите адресные пространства, к которым относятся адреса в сетевых пакетах (блок отображается, если в программу добавлены дополнительные адресные пространства).

     По умолчанию заданы все адресные пространства, созданные в программе.

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием BPF** и введите выражение для фильтрации с использованием технологии BPF (Berkley Packet Filter) по адресным параметрам в сетевых пакетах.

     Пример выражения для фильтрации:
     `tcp port 102 or tcp port 502`

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием регулярных выражений** и введите выражение для фильтрации по данным, составляющим полезную нагрузку в сетевых пакетах.

     Пример выражения для фильтрации:
     `^test.+xABxCD`

6. Нажмите на кнопку **Скачать**.

7. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции формирования файла.

   c. Нажмите на кнопку **Скачать файл**.

Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Контроль состояния Kaspersky Industrial CyberSecurity for Networks

Этот раздел содержит инструкции для контроля состояния программы.

Контроль состояния программы при подключении через веб-интерфейс

Вы можете просматривать информацию о текущем состоянии программы при подключении к Серверу через веб-интерфейс. Для контроля состояния программы предусмотрены соответствующие виджеты в разделе **Мониторинг**.

Дополнительно программа информирует о выключенных функциях защиты и о проблемах в работе.

Информация о выключенных функциях защиты

Если выключены некоторые функции защиты, в нижней части меню на странице веб-интерфейса программы отображается уведомление **Не все функции защиты включены**. Уведомление отображается в следующих случаях:

- выключена одна или несколько точек мониторинга;
- выключена одна или несколько функций защиты (например, обнаружение вторжений по правилам);
- включен режим обучения для одной или нескольких функций защиты (например, для технологии Контроль целостности сети).

Чтобы просмотреть информацию о выключенных функциях защиты:

1. Нажмите на уведомление **Не все функции защиты включены**.

   Появится окно **Компоненты, не обеспечивающие защиту**.

2. Выберите одну из следующих вкладок:

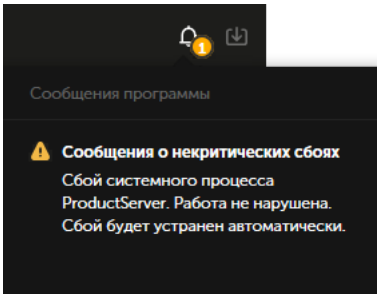
   - **Сервер** – для просмотра информации о выключенных функциях защиты Сервера.

     Если на узлах сенсоров и точек мониторинга включено наследование технологий, в правом верхнем углу вкладки **Сервер** отображается сообщение **Включено наследование технологий на всех компонентах**.

   - **Сенсоры** – для просмотра информации о выключенных функциях защиты сенсоров.
   - **Точки мониторинга** – для просмотра информации о выключенных функциях защиты точек мониторинга.

Уведомления о проблемах в работе программы

В верхней части меню веб-интерфейса расположена кнопка для открытия списка уведомлений о проблемах в работе программы (см. рис. ниже).



Список уведомлений о проблемах в работе программы в окне браузера

Если в списке есть уведомления о критических проблемах (например, появились сообщения о нарушении работы программы), отображается значок красного цвета. Если в списке есть только уведомления о некритических проблемах, отображается значок желтого цвета.

Список содержит только актуальные уведомления. Если проблема устранена (например, восстановлено потерянное соединение с Сервером), соответствующее уведомление автоматически удаляется из списка.

Вы можете просмотреть подробную информацию об уведомлениях (кроме уведомлений о недоступности Сервера или базы данных).

Чтобы просмотреть информацию об уведомлении, выполните следующие действия

1. В меню нажмите на кнопку .
2. В списке уведомлений нажмите на текст уведомления.

   В окне браузера откроется раздел с информацией, которая относится к уведомлению (например, в разделе **Параметры** → **Сообщения программы**).

Просмотр сообщений программы

В журнале сообщений программы сохраняется информация об ошибках в работе программы и операциях, выполненных системными процессами Kaspersky Industrial CyberSecurity for Networks.

Вы можете просматривать сообщения программы при подключении к Серверу через веб-интерфейс. При необходимости вы также можете настроить отправку сообщений программы в сторонние системы через коннекторы.

Чтобы просмотреть сообщения программы:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс.
2. Выберите раздел **Параметры** → **Сообщения программы**.

   В таблице отобразятся сообщения программы, которые соответствуют заданным параметрам фильтрации и поиска.

Параметры сообщений программы отображаются в следующих столбцах таблицы:

- **Дата и время**.

  Дата и время регистрации сообщения программы.

- **Статус**.

  Название статуса сообщения. Для сообщений предусмотрены следующие статусы:

  - *Нормальная работа* – для информационных сообщений.
  - *Неизвестно*, *Сбой* – для сообщений о некритических сбоях в работе программы.
  - *Серьезный сбой*, *Критический сбой*, *Неустранимый сбой* – для сообщений о нарушении работы программы.

- **Узел**.

  Имя или IP-адрес узла, от которого поступило сообщение.

- **Системный процесс**.

  Процесс программы, который вызвал регистрацию сообщения.

- **Сообщение**.

  Числовой идентификатор и текст сообщения.

При просмотре таблицы сообщений программы вы можете использовать функции фильтрации, поиска и сортировки.

Просмотр записей аудита действий пользователей

Kaspersky Industrial CyberSecurity for Networks может сохранять информацию о действиях, совершенных пользователями в программе. Информация сохраняется в журнале аудита, если включен аудит действий пользователей.

Вы можете просматривать записи аудита при подключении к Серверу через веб-интерфейс. При необходимости вы также можете настроить отправку записей аудита в сторонние системы через коннекторы.

Просматривать записи аудита могут только пользователи с ролью Администратор.

Чтобы просмотреть записи аудита:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Аудит**.

   В таблице отобразятся записи аудита, которые соответствуют заданным параметрам фильтрации и поиска.

Параметры записей аудита отображаются в следующих столбцах таблицы:

- **Дата и время**.

  Дата и время регистрации данных о действии пользователя.

- **Действие**.

  Зарегистрированное действие, которое совершил пользователь.

- **Результат**.

  Результат выполнения зарегистрированного действия (успешно или неуспешно).

- **Пользователь**.

  Имя пользователя, который совершил зарегистрированное действие.

- **Узел пользователя**.

  IP-адрес узла, на котором совершено зарегистрированное действие.

- **Описание**.

  Дополнительные сведения о зарегистрированном действии.

При просмотре таблицы записей аудита вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Просмотр сведений об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах

Просматривать сведения об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах могут как пользователи с ролью Администратор, так и пользователи с ролью Оператор.

Чтобы просмотреть сведения об узлах и сетевых интерфейсах:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс.

2. Выберите раздел **Параметры** → **Развертывание**.

   В окне веб-интерфейса отобразятся карточки узлов (слева) и карточки сетевых интерфейсов, обнаруженных на этих узлах (справа от каждого узла).

3. Если вы хотите просмотреть подробные сведения об узле или сетевом интерфейсе, выберите карточку нужного узла или сетевого интерфейса.

   В правой части окна веб-интерфейса появится область деталей.

Отображаемые сведения об узлах с установленными компонентами программы

В карточке узла отображаются следующие сведения:

- Текущий статус узла:
  - *OK*. Узел доступен, и от этого узла не поступали сообщения программы о некритических сбоях или нарушении работы.
  - *Некритический сбой*. Узел доступен, и от этого узла поступили сообщения программы со статусами *Неизвестно* или *Сбой*.
  - *Нарушена работа*. Узел доступен, и от этого узла поступили сообщения программы со статусами *Серьезный сбой*, *Критический сбой* или *Неустранимый сбой*.
  - *Нет соединения*. Узел недоступен.
- Имя узла.
- Компонент программы, установленный на узле: **Сервер** или **Сенсор**.
- IP-адрес для подключения к узлу (адрес 0.0.0.0 соответствует всем возможным IP-адресам на компьютере).
- Текущий режим технологий, для которых доступна возможность выбора режима работы. Карточка содержит название режима *Обучение* или *Наблюдение*, если все технологии работают в этом режиме. Если для технологий выбраны разные режимы, отображается значение *Смешанный*.
- Если для сенсора выключено наследование технологий Сервера, отображается значок .

Отображаемые сведения о сетевых интерфейсах

В карточке сетевого интерфейса отображаются следующие сведения:

- Значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса:
  - – сетевой кабель подключен;
  - – сетевой кабель отключен.

  Значок мигает при включенном режиме индикации Ethernet-порта.
- Имя сетевого интерфейса в операционной системе.
- MAC-адрес.

- Скорость поступления входящего трафика на сетевой интерфейс.
- Сведения о точке мониторинга, если она добавлена:
  - Текущий статус точки мониторинга:
    - *OK*. Точка мониторинга доступна.
    - *Переключение*. Происходит переключение режима работы точки мониторинга.
    - *Ошибка*. Обнаружена ошибка при переключении режима работы точки мониторинга.
  - Имя точки мониторинга.
  - Текущий режим работы точки мониторинга:
    - Если точка мониторинга выключена, отображается значение *Выключена*.
    - Если точка мониторинга включена, отображается текущий режим технологий, для которых доступна возможность выбора режима работы. Карточка содержит название режима *Обучение* или *Наблюдение*, если все технологии работают в этом режиме. Если для технологий выбраны разные режимы, отображается значение *Смешанный*.
  - Если для точки мониторинга выключено наследование технологий узла, отображается значок .

Отображаемые сведения об узле в области деталей

Для выбранного узла в области деталей отображаются следующие сведения:

- Имя узла.
- На вкладке **Управление технологиями** отображается список технологий и методов, которые можно включать и выключать на узле.

  Для технологий с возможностью выбора режима работы отображается текущий режим: **Обучение** или **Наблюдение**. Если включен режим обучения, справа от названия режима отображается дата и время автоматического переключения в режим наблюдения (дата и время не отображаются, если срок автоматического переключения не задан).
- На вкладке **Параметры** отображается следующая информация:
  - **Статус** – текущий статус узла в виде значка и текстового описания (как и в карточке узла).
  - **Тип узла** – компонент программы, установленный на узле: **Сервер** или **Сенсор**.
  - **Текущий объем данных программы** – пространство на диске, занятое файлами программы. Включает в себя установленные файлы и файлы, созданные в процессе работы программы.
  - **Максимально возможный объем данных программы** – пространство на диске, которое могут занять файлы программы. Включает в себя установленные файлы и сумму всех заданных ограничений по объему в правилах хранения данных. Значение не может превышать объем доступного пространства на диске.
  - **Занято на диске** – пространство на диске, занятое всеми файлами. Включает в себя файлы программы и файлы операционной системы и других приложений. Объем пространства рассчитывается на диске, который содержит директорию /var/ в файловой системе узла.
  - **Свободно на диске** – пространство на диске, не занятое файлами. Объем пространства рассчитывается на диске, который содержит директорию /var/ в файловой системе узла.
  - **Объем диска** – общий объем пространства на диске, который содержит директорию /var/ в файловой системе узла.
  - **Наследование технологий** – признак включенного или выключенного наследования технологий Сервера (только для узла сенсора).
  - **BPF-фильтрация** – признак включенной или выключенной на узле фильтрации с использованием технологии BPF (Berkley Packet Filter) по адресным параметрам в сетевых пакетах.
  - **Правила хранения** – текущие и максимальные значения объема, количества элементов и времени хранения данных программы.

Отображаемые сведения о сетевом интерфейсе в области деталей

Для сетевого интерфейса, на который не добавлена точка мониторинга, в области деталей отображаются следующие сведения:

- **Сетевой интерфейс** – имя сетевого интерфейса в операционной системе.
- **Подключение** – значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса:
  - – сетевой кабель подключен;
  - – сетевой кабель отключен.

  Значок мигает при включенном режиме индикации Ethernet-порта.
- **MAC-адрес** – MAC-адрес сетевого интерфейса.
- **IP-адрес** – IP-адрес сетевого интерфейса. Если на сетевом интерфейсе обнаружено несколько IP-адресов, то в области деталей отображаются не более 16 IP-адресов.

Если на сетевой интерфейс добавлена точка мониторинга, отображаются следующие сведения:

- Имя точки мониторинга.
- **Статус** – текущий статус точки мониторинга в виде значка и текстового описания:
  - *OK*. Точка мониторинга доступна.
  - *Переключение*. Происходит переключение режима работы точки мониторинга.
  - *Ошибка*. Обнаружена ошибка при переключении режима работы точки мониторинга.
- **Подключение** – значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса:
  - – сетевой кабель подключен;
  - – сетевой кабель отключен.

  Значок мигает при включенном режиме индикации Ethernet-порта.
- **Сетевой интерфейс** – имя сетевого интерфейса в операционной системе.
- **Режим** – текущий режим работы точки мониторинга:
  - *Включена*.
  - *Выключена*.

- На вкладке **Управление технологиями** отображается список технологий и методов, которые можно включать и выключать на точке мониторинга.

  Для технологий с возможностью выбора режима работы отображается текущий режим: *Обучение* или *Наблюдение*. Если включен режим обучения, справа от названия режима отображается дата и время автоматического переключения в режим наблюдения (дата и время не отображаются, если срок автоматического переключения не задан).

- На вкладке **Параметры**:

  - **Наследование технологий** – признак включенного или выключенного наследования технологий узла.
  - **MAC-адрес** – MAC-адрес сетевого интерфейса.
  - **IP-адрес** – IP-адрес сетевого интерфейса. Если на сетевом интерфейсе обнаружено несколько IP-адресов, то в области деталей отображаются не более 16 IP-адресов.

Просмотр статуса сервисов, обеспечивающих работу компонентов программы

Вы можете просмотреть статус сервисов, которые обеспечивают работу компонентов программы. Если сервис активен, это означает, что его запуск выполнен успешно.

Чтобы просмотреть статус сервиса:

1. На компьютере, на котором установлен компонент программы, откройте консоль операционной системы.

2. Введите команду:

   `sudo service <имя сервиса> status`

   где `<имя сервиса>` – имя сервиса, информацию о котором вы хотите просмотреть. Вы можете указать следующие сервисы:

   - `kics4net` – основной сервис (запуск команды возможен только на компьютере, который выполняет функции Сервера);
   - `kics4net-apm` – сервис коннектора активного опроса (присутствует на компьютере, который выполняет функции Сервера или сенсора);
   - `kics4net-asset-config-repo` – сервис хранения конфигураций устройств (присутствует на компьютере, который выполняет функции Сервера);
   - `kics4net-asset-inventory` – сервис обработки результатов сканирования атрибутов устройств с помощью OVAL-правил (присутствует только на компьютере, который выполняет функции Сервера);
   - `kics4net-blob-storage` – сервис хранения массивов двоичных данных (присутствует только на компьютере, который выполняет функции Сервера);
   - `kics4net-config-control-orchestrator` – сервис управления процессами контроля конфигураций и активного опроса (присутствует только на компьютере, который выполняет функции Сервера);
   - `kics4net-connectors-launcher` – сервис регистрации и запуска управляемых коннекторов (присутствует на компьютере, который выполняет функции Сервера или сенсора);
   - `kics4net-email-gateway` – сервис отправки почтовых уведомлений (присутствует только на компьютере, который выполняет функции Сервера);
   - `kics4net-epp-proxy` – сервис интеграции с EPP-приложениями (присутствует на компьютере, который выполняет функции Сервера или сенсора);
   - `kics4net-fts` – сервис системы полнотекстового поиска (присутствует только на компьютере, который выполняет функции Сервера);
   - `kics4net-nats-server` – сервис брокера сообщений (присутствует на компьютере, который выполняет функции Сервера или сенсора);
   - `kics4net-oval-facade` – сервис сканирования удаленных устройств по OVAL-правилам (присутствует на компьютере, который выполняет функции Сервера или сенсора);
   - `kics4net-postgresql` – сервис СУБД (присутствует только на компьютере, который выполняет функции Сервера);
   - `kics4net-report-builder` – сервис формирования отчетов (присутствует только на компьютере, который выполняет функции Сервера);
   - `kics4net-report-data-source` – сервис предоставления данных для отчетов (присутствует только на компьютере, который выполняет функции Сервера);

- `kics4net-report-renderer` – сервис визуального отображения блоков данных в отчетах (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-report-templates-catalog` – сервис управления шаблонами отчетов (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-report-templates-catalog-view` – сервис предоставления данных о шаблонах отчетов (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-responses-manager` – сервис управления заданиями реагирования (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-risk-oval-detector` – сервис обработки результатов сканирования устройств с помощью OVAL-правил на предмет наличия рисков (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-scan-oval-manager` – сервис управления сканирования устройств с помощью OVAL-правил (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-scap-manager` – сервис управления аудита безопасности (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-scap-manager-view` – сервис предоставления данных об аудите безопасности (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-scheduler` – сервис планировщика задач (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-secrets` – сервис фасада к хранилищу секретов (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-task-manager` – сервис управления задачами (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-task-manager-view` – сервис предоставления данных о задачах (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-vault` – сервис хранения секретов в хранилище (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-websensor` – сервис веб-сервера (присутствует только на компьютере, который выполняет функции сенсора);
- `kics4net-webserver` – сервис веб-сервера (присутствует только на компьютере, который выполняет функции Сервера);
- `klnagent` – сервис Агента администрирования (присутствует только на компьютере, который выполняет функции Сервера).

  Пример:
  ```
  sudo service kics4net status
  ```

Если сервис не активен, вы можете перезагрузить компьютер или перезапустить сервис.

Перезагрузка компьютера с установленными компонентами программы

При перезагрузке компьютера, который выполняет функции Сервера или сенсора, происходит автоматический запуск компонентов программы. Перезагрузка не влияет на последующую работу этих компонентов (кроме некоторых ситуаций, когда возникает сбой после непредвиденной перезагрузки).

Перезагрузка может потребоваться, например, в следующих случаях:

- Закончилось свободное пространство на жестком диске компьютера.
- Произошла непредвиденная перезагрузка компьютера, после которой работа компонентов программы не восстановлена.
- Не активен один из сервисов программы.
- Не восстанавливается потерянное соединение Сервера с сенсором. В этом случае следует перезагрузить компьютер, выполняющий функции сенсора.

Вы можете перезагрузить компьютер с установленными компонентами программы с помощью штатных команд операционной системы.

Если по каким-либо причинам невозможно выполнить перезагрузку компьютера, вы можете перезапустить сервисы, обеспечивающие работу компонентов программы.

Чтобы перезапустить сервисы:

1. Откройте консоль операционной системы.
2. В зависимости от того, какие функции выполняет компьютер, выполните соответствующие действия:

- Если компьютер выполняет функции Сервера, введите команды в следующей последовательности:

```
sudo service kics4net-postgresql restart
sudo service kics4net-nats-server restart
sudo service kics4net restart
sudo service kics4net-connectors-launcher restart
sudo service kics4net-epp-proxy restart
sudo service kics4net-oval-facade restart
sudo service kics4net-asset-inventory restart
sudo service kics4net-blob-storage restart
sudo service kics4net-email-gateway restart
sudo service kics4net-fts restart
sudo service kics4net-report-builder restart
sudo service kics4net-report-data-source restart
sudo service kics4net-report-renderer restart
sudo service kics4net-report-templates-catalog restart
sudo service kics4net-report-templates-catalog-view restart
sudo service kics4net-responses-manager restart
sudo service kics4net-risk-oval-detector restart
sudo service kics4net-scap-manager restart
sudo service kics4net-scap-manager-view restart
sudo service kics4net-scan-oval-manager restart
sudo service kics4net-scheduler restart
sudo service kics4net-vault restart
sudo service kics4net-secrets restart
sudo service kics4net-task-manager restart
sudo service kics4net-task-manager-view restart
sudo service kics4net-webserver restart
sudo service kics4net-asset-config-repo restart
sudo service kics4net-config-control-orchestrator restart
sudo service klnagent restart
```

- Если компьютер выполняет функции сенсора, введите команды в следующей последовательности:

```
sudo service kics4net restart
sudo service kics4net-connectors-launcher restart
sudo service kics4net-epp-proxy restart
sudo service kics4net-nats-server restart
sudo service kics4net-oval-facade restart
```

```
sudo service kics4net-websensor restart
```

Проверка регистрации событий с помощью тестового сетевого пакета

Для проверки регистрации событий в Kaspersky Industrial CyberSecurity for Networks вы можете использовать тестовый сетевой пакет. При обнаружении такого пакета в трафике программа регистрирует тестовые события по следующим технологиям:

- Контроль технологического процесса. Событие регистрируется независимо от наличия правил контроля процесса и тегов.
- Контроль целостности сети. Событие регистрируется независимо от наличия правил контроля взаимодействий. При этом должно быть включено применение технологии Контроль целостности сети.
- Обнаружение вторжений. Событие регистрируется независимо от наличия правил обнаружения вторжений. При этом должно быть включено применение метода обнаружения вторжений по правилам.
- Контроль активов. Событие регистрируется независимо от наличия устройств в таблице устройств, известных программе. При этом должно быть включено применение метода обнаружения активности устройств.

Для регистрации используются системные типы событий, которым присвоены следующие коды:

- 4000000001 – для события по технологии Контроль технологического процесса;
- 4000000002 – для события по технологии Контроль целостности сети;
- 4000000003 – для события по технологии Обнаружение вторжений;
- 4000000004 – для события по технологии Контроль активов.

Вы можете просмотреть тестовые события в таблице зарегистрированных событий.

Для проверки функции аудита Kaspersky Industrial CyberSecurity for Networks сохраняет информацию о регистрации тестовых событий в журнале аудита. По каждому зарегистрированному событию создается запись аудита, в которой указана технология регистрации тестового события.

Тестовый сетевой пакет представляет собой пакет протокола UDP с определенными значениями параметров. Параметры заданы таким образом, чтобы исключить вероятность получения такого пакета в обычном трафике промышленной сети.

В параметрах тестового сетевого пакета должны быть заданы следующие данные:

- Заголовок Ethernet II:
  - MAC-адрес отправителя: `00:00:00:00:00:00`.
  - MAC-адрес получателя: `ff:ff:ff:ff:ff:ff`.
  - EtherType: `0x0800 (IPv4)`.
- Заголовок IP:
  - IP-адрес отправителя: `127.0.20.20`.
  - IP-адрес получателя: `127.0.20.20`.
  - ID: `20`.
  - TTL: `20`.
  - Protocol type: `17 (UDP)`.
  - Флаги: `0x00`.
- Заголовок UDP:
  - Порт отправителя: `20`.
  - Порт получателя: `20`.
- Содержимое пакета:
  - Длина содержимого пакета, байт: `20`.
  - Содержимое пакета: "`KICS4Net Sentinel 20`".

Для формирования и отправки тестового сетевого пакета вы можете использовать программу генерации сетевых пакетов, например Scapy. Отправку тестового сетевого пакета нужно выполнить с узла, трафик которого контролируется Kaspersky Industrial CyberSecurity for Networks.

Пример:

Чтобы отправить тестовый сетевой пакет с помощью программы Scapy в операционной системе Linux:

1. В консоли операционной системы компьютера введите команду запуска интерактивного режима работы Scapy:

   ```
   sudo scapy
   ```

2. Введите команду отправки тестового сетевого пакета:

   ```
   sendp(
   Ether(src='00:00:00:00:00:00', dst='ff:ff:ff:ff:ff:ff')/
   IP(src='127.0.20.20', dst='127.0.20.20', id=20, ttl=20)/
   UDP(sport=20, dport=20)/
   "KICS4Net Sentinel 20",
   iface="< имя интерфейса >"
   )
   ```

   где `< имя интерфейса >` – имя сетевого интерфейса, подключенного к промышленной сети (например, `eth0`).

После обнаружения пакета в трафике программа Kaspersky Industrial CyberSecurity for Networks зарегистрирует тестовые события.

Контроль целостности модулей программы

Вы можете проверить целостность установленных модулей программы, чтобы убедиться в отсутствии изменений в этих модулях после установки. Проверка выполняется путем сравнения контрольных сумм установленных модулей программы с эталонными значениями. Запускать проверку целостности требуется по отдельности на каждом узле с установленными модулями программы.

Для запуска проверки целостности на узле предусмотрены следующие способы:

- Локальный запуск с использованием скрипта kics4net-manifest-checker-<номер версии программы>.bundle.sh.
- Запуск при подключении к Серверу через веб-интерфейс.

Локальный запуск проверки целостности с использованием скрипта

Скрипт kics4net-manifest-checker-<номер версии программы>.bundle.sh входит в комплект поставки Kaspersky Industrial CyberSecurity for Networks. Этот скрипт проверяет файлы модулей программы по специальным спискам, которые хранятся в *файлах манифеста*. Файлы манифеста включены в пакеты для установки программы и содержат списки файлов соответствующих пакетов. Для каждого пакета программы имеется свой файл манифеста. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

Результаты работы скрипта kics4net-manifest-checker-<номер версии программы>.bundle.sh могут быть неправильными в случае внесения каких-либо изменений в файл скрипта. Для правильных результатов работы используйте только ту версию скрипта, которая входит в комплект поставки Kaspersky Industrial CyberSecurity for Networks.

В процессе работы скрипт последовательно проверяет контрольные суммы файлов из пакетов программы, установленных в операционной системе.

Чтобы проверить целостность модулей программы на компьютере узла с использованием скрипта kics4net-manifest-checker-<номер версии программы>.bundle.sh:

1. Скопируйте в произвольную директорию файл скрипта kics4net-manifest-checker-<номер версии программы>.bundle.sh из директории с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.
2. В консоли операционной системы перейдите в директорию, в которой находится файл скрипта, и введите команду:

   ```
   sudo bash kics4net-manifest-checker-<номер версии программы>.bundle.sh
   ```

   Информация о результатах проверки отобразится в консоли операционной системы.

Результаты проверки целостности модулей программы на компьютере признаются успешными, если выполнены оба следующих условия:

- Скрипт kics4net-manifest-checker-<номер версии программы>.bundle.sh завершил работу с сообщением: `Проверка файлов всех установленных пакетов, содержащих файл манифеста, завершена успешно`.

- Для всех пакетов программы, которые должны быть установлены на компьютере согласно выполняемым функциям, отсутствуют сообщения об ошибках или хотя бы одно из следующих сообщений:

  - `Пакет не установлен в операционной системе`.

  - `Файл манифеста для пакета не найден`.

Запуск проверки целостности при подключении к Серверу через веб-интерфейс

Вы можете запустить проверку целостности модулей программы на узле при подключении к Серверу через веб-интерфейс. Проверка целостности на узле при таком способе запуска выполняется аналогичными методами, как при использовании скрипта kics4net-manifest-checker-<номер версии программы>.bundle.sh.

Чтобы проверить целостность модулей программы на компьютере узла при подключении к Серверу через веб-интерфейс:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Развертывание**.

3. Выберите карточку нужного узла.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Проверить целостность**. Если кнопка не отображается в панели инструментов, нажмите на кнопку ⋮ и выберите нужный пункт в открывшемся меню.

   На экране появится сообщение о запуске проверки целостности, после чего в списке фоновых операций некоторое время будет доступна информация о выполнении операции. При необходимости вы можете просмотреть текущий список фоновых операций с помощью кнопки в меню веб-интерфейса программы.

5. Для просмотра информации о результате проверки целостности перейдите в раздел **Параметры** → **Сообщения программы**.

Результаты проверки целостности модулей программы на компьютере признаются успешными, если в списке сообщений программы присутствует следующее сообщение для соответствующего узла: `Успешно завершена проверка целостности программных модулей на узле`.

Если в списке сообщений программы нет сообщения об успешной проверке и присутствует сообщение об ошибках, проверка считается неуспешной. Вы можете определить пакеты программы, которые не прошли проверку целостности, с помощью скрипта kics4net-manifest-checker-<номер версии программы>.bundle.sh (см. выше).

Синхронизация времени на узлах Kaspersky Industrial CyberSecurity for Networks с источником времени для устройств промышленной сети

Для правильного сопоставления времени регистрации событий с моментами, когда события произошли в промышленной сети, в системе необходимо обеспечить синхронизацию времени. Синхронизация времени должна выполняться на узлах с установленными компонентами Kaspersky Industrial CyberSecurity for Networks с общим источником времени, который используют устройства промышленной сети.

При централизованной установке Kaspersky Industrial CyberSecurity for Networks вы можете включить автоматическую синхронизацию времени Сервера с узлами, на которых установлены сенсоры. В этом случае источником времени для узлов с установленными сенсорами будет узел с установленным Сервером. Синхронизацию времени Сервера с общим источником времени, который используют устройства в промышленной сети, рекомендуется настроить с помощью программных средств из состава операционной системы компьютера, выполняющего функции Сервера. Для синхронизации времени Сервера вы можете использовать стандартные протоколы Network Time Protocol (NTP) и Precision Time Protocol (PTP).

Для автоматической синхронизации времени Сервера с другими узлами используется протокол NTP. При этом на узлах с установленными сенсорами нельзя настраивать синхронизацию с другими источниками времени и использовать протокол PTP.

Если установка сенсора выполнена локально с помощью скрипта kics4net-install.sh, на этом узле не выполняется автоматическая синхронизация времени с Сервером. В этом случае требуется настроить синхронизацию времени как на Сервере, так и на всех узлах с сенсорами, которые были установлены локально.

Примеры последовательности действий для настройки синхронизации времени см. в Приложении.

Обновление сертификатов SSL-соединений

В Kaspersky Industrial CyberSecurity for Networks могут использоваться следующие сертификаты:

- сертификаты для соединений между узлами Kaspersky Industrial CyberSecurity for Networks;
- сертификаты для подключения к Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс;
- сертификаты для подключения через Kaspersky Industrial CyberSecurity for Networks API;
- сертификаты для подключения коннекторов;
- сертификаты для соединений с программными компонентами Endpoint Agent.

Рекомендуется обновлять сертификаты в следующих случаях:

- текущие сертификаты скомпрометированы;
- закончился срок действия сертификатов;
- нужно выполнить регулярное обновление сертификатов в соответствии с требованиями информационной безопасности на предприятии.

Обновление сертификатов для соединений между узлами Kaspersky Industrial CyberSecurity for Networks

Во время установки Kaspersky Industrial CyberSecurity for Networks происходит автоматическое обновление сертификатов для соединений между узлами Kaspersky Industrial CyberSecurity for Networks. Вы можете принудительно обновить эти сертификаты, не выполняя переустановку компонентов программы.

Чтобы обновить сертификаты для соединений между узлами Kaspersky Industrial CyberSecurity for Networks:

1. На компьютере Сервера перейдите в директорию /opt/kaspersky/kics4net/sbin/ и введите команду запуска скрипта локального обновления сертификатов:

   ```
   sudo bash kics4net-update-certs.sh
   ```

2. После завершения работы скрипта переведите все сенсоры в начальное состояние с помощью скрипта для локального перевода узла в начальное состояние kics4net-reset-to-defaults.sh. Скрипт находится на компьютере с установленным компонентом программы в директории /opt/kaspersky/kics4net/sbin/.

3. Заново добавьте и подключите сенсоры.

Обновление сертификата для подключения к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс

Для обновления сертификата для подключения к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс вам нужно заменить сертификат, используемый веб-сервером. Вы можете указать новый сертификат веб-сервера в разделе **Параметры** → **Серверы подключений** на вкладке **Веб-сервер**.

Обновление сертификата для подключения к Серверу через Kaspersky Industrial CyberSecurity for Networks API

Для обновления сертификата для подключения к Серверу через Kaspersky Industrial CyberSecurity for Networks API вам нужно заменить сертификат, используемый сервером REST API. Вы можете указать новый сертификат сервера REST API в разделе **Параметры** → **Серверы подключений** на вкладке **Сервер REST API**.

Обновление сертификатов для подключения коннекторов

Вы можете обновлять сертификаты для подключения неуправляемых коннекторов (или коннекторов с включенным режимом игнорирования функций управляемого коннектора) при создании новых файлов свертки для коннекторов. Для обновления сертификатов управляемых коннекторов вам нужно удалить и заново добавить эти коннекторы.

Обновление сертификатов для соединений с программными компонентами Endpoint Agent

Вы можете обновлять сертификаты для соединений с программными компонентами Endpoint Agent при изменении параметров серверов интеграции.

Обновление баз и программных модулей

В Kaspersky Industrial CyberSecurity for Networks предусмотрена возможность обновления следующих баз и программных модулей:

- системные правила обнаружения вторжений;
- модули обработки протоколов прикладного уровня для контроля технологического процесса;
- правила корреляции событий для регистрации инцидентов;
- правила получения сведений об устройствах и протоколах взаимодействий;
- база данных уязвимостей промышленного оборудования;
- список отозванных сертификатов Kaspersky Digital Signature (KDS);
- конфигурация функциональности программы;
- системные правила аудита безопасности;
- криптографический модуль (библиотека) OpenSSL;
- база данных уязвимостей Kaspersky ICS CERT для АСУ ТП;
- методы определения техник возможных атак по событиям обнаружения системных команд.

Базы и программные модули обновляются после установки обновлений, выпускаемых "Лабораторией Касперского".

Своевременная установка обновлений обеспечивает максимальную защиту промышленной сети с помощью Kaspersky Industrial CyberSecurity for Networks. Кроме того, обновления могут дополнять и обновлять программные модули, участвующие в обеспечении безопасности программы. Если не выполняется регулярная установка обновлений, с течением времени появляются риски для безопасности программы из-за появления новых угроз. Дополнительно необходимо устанавливать обновления безопасности операционной системы.

Сразу после установки компонентов Kaspersky Industrial CyberSecurity for Networks рекомендуется вручную запустить установку обновлений. Для регулярной установки обновлений вы можете настроить параметры автоматического запуска по расписанию.

Вы можете использовать следующие источники обновлений:

- серверы обновлений "Лаборатории Касперского";
- Сервер администрирования Kaspersky Security Center.

В качестве источника обновлений вы также можете использовать файлы из локального ресурса, если запуск установки обновлений выполняется вручную.

Вы можете настраивать параметры и запускать установку обновлений при подключении к Серверу через веб-интерфейс.

Обновление баз и программных модулей имеет следующие особенности и ограничения:

- Функциональность обновления доступна после добавления лицензионного ключа.

  Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в программном обеспечении на территории США.

- После установки обновления библиотеки OpenSSL требуется перезапустить сервисы на узлах с установленными компонентами программы.

- Для загрузки обновлений с серверов обновлений "Лаборатории Касперского" требуется доступ в интернет. При подключении к серверам обновлений с компьютера, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks, соединение осуществляется по протоколу HTTPS (при этом соединение через прокси-сервер не поддерживается).

- Для загрузки обновлений с Сервера администрирования Kaspersky Security Center в Kaspersky Industrial CyberSecurity for Networks должна быть добавлена функциональность взаимодействия программы с Kaspersky Security Center. Вы можете добавить эту функциональность при установке или переустановке Kaspersky Industrial CyberSecurity for Networks. Загрузка обновлений выполняется из хранилища Сервера администрирования, которое заполняется при использовании соответствующей задачи в Kaspersky Security Center.

Запуск обновления вручную

Вы можете запустить обновление в любой момент. Возможность запуска обновления доступна после добавления лицензионного ключа.

Запускать обновление вручную могут только пользователи с ролью Администратор.

Чтобы запустить обновление вручную:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Обновление**.

3. В блоке параметров **Источник для обновления вручную** выберите один из следующих вариантов использования источников обновлений:

   - Локальный источник обновлений – позволяет загрузить обновления из файлов по указанному локальному пути. Вы можете указать локальный путь к файлам с помощью кнопки **Обзор**.

   - **Серверы обновлений "Лаборатории Касперского"** – для загрузки обновлений с серверов обновлений "Лаборатории Касперского".

   - **Сервер администрирования Kaspersky Security Center** – для загрузки обновлений с Сервера администрирования Kaspersky Security Center (этот вариант доступен, если добавлена функциональность взаимодействия программы с Kaspersky Security Center).

4. Нажмите на кнопку **Обновить сейчас**.

Настройка автоматического обновления

После добавления лицензионного ключа вы можете настроить автоматическое обновление по расписанию.

Настраивать автоматическое обновление по расписанию могут только пользователи с ролью Администратор.

Чтобы включить и настроить автоматическое обновление по расписанию:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Обновление**.

3. С помощью переключателя **Обновление по расписанию** включите автоматическое обновление.

4. В блоке параметров **Источник для обновления по расписанию** выберите один из следующих вариантов использования источников обновлений:

   - **Серверы обновлений "Лаборатории Касперского"** – для загрузки обновлений с серверов обновлений "Лаборатории Касперского".

   - **Сервер администрирования Kaspersky Security Center** – для загрузки обновлений с Сервера администрирования Kaspersky Security Center (этот вариант доступен, если добавлена функциональность взаимодействия программы с Kaspersky Security Center).

5. Задайте параметры расписания для запуска обновления. Для этого выполните следующие действия:

   a. В раскрывающемся списке **Периодичность** укажите, когда будет происходить обновление. Выберите один из следующих вариантов: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.

   b. В зависимости от выбранного варианта задайте значения параметров, которые уточняют время запуска обновления.

6. Нажмите на кнопку **Сохранить параметры**.

Просмотр сведений об установке обновлений

Вы можете просматривать общие и подробные сведения об установке обновлений.

Общие сведения об установленных обновлениях

Общие сведения содержат информацию о датах и времени выпуска установленных обновлений баз и программных модулей.

Чтобы просмотреть общие сведения об установленных обновлениях,

на странице веб-интерфейса программы выберите раздел **О программе**.

Подробные сведения об установке обновлений

Подробные сведения содержат информацию о запусках процессов установки обновлений. Программа сохраняет следующие подробные сведения:

- дата и время запуска процесса обновления;
- режим запуска обновления;
- дата и время выпуска баз и программных модулей, установленных в процессе обновления (при успешном обновлении);
- информация об ошибке (если обновление завершилось неудачно);
- список обновленных баз и программных модулей.

Подробные сведения об установке обновлений сохраняются в журнале сообщений программы.

Перезапуск сервисов на узлах после установки обновления библиотеки OpenSSL

Если на узлах с установленными компонентами программы была выполнена установка обновления библиотеки OpenSSL, на этих узлах требуется перезапустить сервисы, обеспечивающие работу компонентов программы. Перезапуск сервисов на узлах сенсоров выполняется автоматически. При необходимости перезапуска сервисов на узле Сервера программа выводит уведомления об этом на странице веб-интерфейса Сервера. В этом случае для перезапуска сервисов вы можете перезагрузить компьютер Сервера или инициировать перезапуск на странице веб-интерфейса.

Уведомления о необходимости перезапуска сервисов на узле Сервера выводятся в списке уведомлений о проблемах в работе программы, а также в разделе **Параметры** → **Обновление**.

Инициировать перезапуск сервисов Сервера на странице веб-интерфейса могут только пользователи с ролью Администратор.

Чтобы перезапустить сервисы на узле Сервера с использованием веб-интерфейса Сервера:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Обновление**.
3. В уведомлении **Требуется перезапуск** нажмите на кнопку **Перезапустить Сервер**.

   Начнется процесс перезапуска сервисов. До окончания перезапуска Сервер программы недоступен для подключений. Во время перезапуска сервисов на странице веб-интерфейса программы отображается специальный раздел **Обслуживание программы**.

Разделение доступа к функциям программы

В Kaspersky Industrial CyberSecurity for Networks вы можете разграничивать доступ пользователей к функциям программы в зависимости от задач пользователей.

Для доступа к программе могут использоваться следующие учетные записи:

- созданные в программе учетные записи пользователей;
- учетные записи пользователей Kaspersky Security Center, для которых настроена технология единого входа (SSO).

Подключения к Серверу под другими учетными записями, а также анонимные подключения, невозможны.

Для учетных записей, имеющих доступ к программе, не требуется регистрация в качестве учетных записей операционной системы компьютера Сервера.

Первую учетную запись пользователя программы требуется создать при начальной настройке Kaspersky Industrial CyberSecurity for Networks. После этого вы можете создавать дополнительные учетные записи, от имени которых будут выполняться действия в программе.

В зависимости от того, к какому компоненту выполнено подключение через веб-интерфейс, пользователю доступны следующие наборы функций:

- функции программы при подключении к Серверу;
- функции программы при подключении к сенсору.

При подключении к Серверу программа предоставляет доступ к функциям в зависимости от роли пользователя, который выполнил подключение.

Об учетных записях пользователей программы

Для разграничения доступа к функциям программы реализована модель управления доступом на основе ролей (Role Based Access Control, RBAC). Роль учетной записи пользователя программы определяет набор доступных пользователю действий. Для учетных записей пользователей программы предусмотрены следующие роли:

- Администратор.

  Пользователь с ролью Администратор обладает правами доступа, которые позволяют использовать все функции управления работой программы, мониторинга и просмотра сведений. Также этому пользователю доступны функции управления учетными записями, созданными в программе.

- Оператор.

  Пользователь с ролью Оператор обладает правами доступа только для мониторинга и просмотра сведений.

Первой учетной записи пользователя, созданной при начальной настройке программы, назначается роль Администратор.

При добавлении следующих учетных записей вы можете назначать им нужные роли. В программе можно создать до 100 учетных записей пользователей программы (без учета пользователей, для которых настроена технология единого входа из Kaspersky Security Center).

При подключении к Серверу пользователь получает права доступа, соответствующие роли его учетной записи. Если во время работы пользователя, созданного в программе, его роль была изменена другим пользователем (которому назначена роль Администратор), права доступа подключенного пользователя обновляются в онлайн-режиме. Например, пользователь, подключившийся к Серверу с ролью Администратор, потеряет права доступа к функциям управления программой после назначения роли Оператор для его учетной записи.

Вы можете управлять учетными записями пользователей, которые были созданы в программе, в разделе **Параметры** → **Пользователи** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Функции программы, доступные при подключении к Серверу через веб-интерфейс

В этой статье приведены функции программы, доступные пользователям при подключении к Серверу через веб-интерфейс (см. таблицу ниже).

Доступные функции программы в зависимости от роли пользователя

Функция программы	Администратор	Оператор
Контроль состояния программы при подключении через веб-интерфейс	✓	✓
Просмотр сообщений программы	✓	✓
Включение и выключение аудита действий пользователей	✓	
Просмотр записей аудита действий пользователей	✓	
Просмотр сведений об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах	✓	✓

Функция программы	Администратор	Оператор
Запуск проверки целостности модулей программы при подключении к Серверу через веб-интерфейс	✓	
Управление параметрами развертывания на узлах	✓	
Просмотр информации о добавленном лицензионном ключе	✓	✓
Добавление лицензионного ключа	✓	
Удаление лицензионного ключа	✓	
Настройка автоматического обновления	✓	
Запуск обновления вручную	✓	
Просмотр сведений об установке обновлений	✓	✓
Просмотр сведений об учетных записях пользователей программы	✓	
Создание учетной записи пользователя программы	✓	
Изменение роли учетной записи пользователя программы	✓	
Удаление учетной записи пользователя программы	✓	
Изменение пароля учетной записи	✓	✓
Просмотр таблицы устройств	✓	✓
Просмотр сведений об устройстве	✓	✓
Выбор источников для контроля уязвимостей устройств	✓	
Настройка адресных пространств	✓	
Добавление устройств вручную	✓	
Объединение устройств	✓	
Удаление устройств	✓	
Изменение статусов устройств	✓	
Формирование дерева групп устройств	✓	
Автоматическая группировка устройств по заданному критерию	✓	
Распределение устройств по группам вручную	✓	
Установка и удаление меток для устройств	✓	
Изменение сведений об устройстве	✓	
Добавление, изменение и удаление пользовательских полей для устройства	✓	
Удаление пользователей устройств	✓	
Удаление исполняемых файлов устройств	✓	
Назначение эталонной конфигурации устройства	✓	
Сравнение сохраненных конфигураций устройства	✓	✓
Просмотр правил адресных пространств	✓	✓
Просмотр подсетей адресных пространств	✓	✓
Просмотр сведений об устройствах с IP-адресами из выбранных подсетей	✓	✓
Настройка контроля процесса	✓	
Мониторинг значений параметров технологического процесса	✓	✓
Просмотр правил контроля взаимодействий в таблице разрешающих правил	✓	✓
Создание правил контроля взаимодействий вручную	✓	
Изменение параметров правила контроля взаимодействий	✓	
Включение и выключение правил контроля взаимодействий	✓	
Удаление правил контроля взаимодействий	✓	

Функция программы	Администратор	Оператор
Включение и выключение наборов правил обнаружения вторжений	✓	
Загрузка и замена пользовательских наборов правил обнаружения вторжений	✓	
Удаление пользовательских наборов правил обнаружения вторжений	✓	
Управление параметрами хранения записей журналов в базе данных	✓	
Управление параметрами сохранения трафика в базе данных	✓	
Управление параметрами сохранения файлов дампа трафика	✓	
Управление параметрами хранения файлов отчетов	✓	
Изменение уровней ведения журналов работы процессов	✓	
Настройка совместной работы с EPP-приложениями	✓	
Управление действиями по реагированию	✓	
Включение и настройка функциональности взаимодействия с Kaspersky Security Center	✓	
Управление коннекторами	✓	
Добавление и удаление типов коннекторов	✓	
Управление заданиями аудита настроек и уязвимостей	✓	
Получение отчетов по заданиям аудита настроек и уязвимостей	✓	✓
Просмотр общих сведений о выполнении запусков заданий аудита настроек и уязвимостей	✓	✓
Управление параметрами хранения для запусков заданий аудита настроек и уязвимостей	✓	
Управление наборами правил для заданий аудита настроек и уязвимостей	✓	
Управление заданиями контроля конфигураций	✓	
Просмотр общих сведений о выполнении запусков заданий контроля конфигураций	✓	✓
Управление заданиями активных опросов устройств	✓	
Просмотр общих сведений о выполнении запусков заданий активных опросов	✓	✓
Управление секретами с учетными данными для удаленных подключений	✓	
Настройка типов событий	✓	
Изменение базовой оценки для типа риска	✓	
Управление параметрами хранения рисков	✓	
Экспорт политики безопасности в файл	✓	✓
Импорт политики безопасности из файла	✓	
Очистка текущей политики безопасности	✓	
Мониторинг системы в онлайн-режиме	✓	✓
Работа с картой сетевых взаимодействий	✓	✓
Перемещение узлов и групп в другие группы на карте сетевых взаимодействий	✓	
Загрузка трафика при работе с картой сетевых взаимодействий	✓	
Просмотр сведений о сетевом сеансе	✓	✓
Загрузка трафика сетевых сеансов	✓	
Формирование топологической карты	✓	
Просмотр подробных сведений об объектах топологической карты	✓	✓
Мониторинг событий и инцидентов	✓	✓
Управление отчетами и шаблонами отчетов	✓	
Формирование отчетов вручную	✓	✓

Функция программы	Администратор	Оператор
Экспорт отчетов в файл	✓	✓
Контроль рисков	✓	✓

Просмотр сведений об учетных записях пользователей программы

При подключении к Серверу через веб-интерфейс вы можете просматривать сведения об учетных записях, созданных в программе. Сведения об учетных записях пользователей Kaspersky Security Center, для которых настроена технология единого входа (SSO), не отображаются в программе.

Просматривать сведения об учетных записях пользователей могут только пользователи с ролью Администратор.

Чтобы просмотреть сведения об учетных записях пользователей программы:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Пользователи**.

   На вкладке **Пользователи** отобразятся карточки пользователей, содержащие имена и роли пользователей программы.

Создание учетной записи пользователя программы

Создать учетную запись пользователя программы могут только пользователи с ролью Администратор.

Чтобы создать учетную запись пользователя программы:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Пользователи**.
3. Добавьте новую карточку пользователя. Для этого нажмите на карточку со знаком +.

   Появится новая карточка пользователя, внутри которой отобразятся поля для ввода учетных данных и выбора роли учетной записи нового пользователя.

4. В поле для ввода имени пользователя введите имя пользователя, учетную запись которого вы хотите создать.

   Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, точку, символы _ и -.

   Имя учетной записи пользователя должно удовлетворять следующим требованиям:

   - является уникальным в списке имен пользователей программы (регистр символов не учитывается);
   - содержит 3–20 символов;
   - начинается с буквы;
   - заканчивается любым поддерживаемым символом, кроме точки.

5. В полях для ввода пароля введите пароль, который вы хотите задать для учетной записи пользователя.

   Пароль должен удовлетворять следующим требованиям:

   - содержит от 8 до 256 символов ASCII;
   - содержит одну или несколько прописных букв латинского алфавита;
   - содержит одну или несколько строчных букв латинского алфавита;
   - содержит одну или несколько цифр;
   - содержит не более трех одинаковых символов подряд.

6. В раскрывающемся списке выберите нужную роль пользователя: **Администратор** или **Оператор**.

7. Нажмите на кнопку **Сохранить**.

В карточке пользователя отобразится значок с именем учетной записи пользователя и назначенная ему роль.

Изменение роли учетной записи пользователя программы

При подключении к Серверу через веб-интерфейс вы можете изменять роли учетных записей, созданных в программе. Этот способ изменения ролей недоступен для учетных записей пользователей Kaspersky Security Center, для которых настроена технология единого входа (SSO).

Изменять роли учетных записей могут только пользователи с ролью Администратор.

Пользователь с ролью Администратор может изменить роль любой учетной записи пользователя, кроме роли своей учетной записи.

Чтобы изменить роль учетной записи пользователя программы:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Пользователи**.

3. Нажмите на кнопку **Изменить** в карточке пользователя, роль которого вы хотите изменить.

   Карточка пользователя перейдет в режим редактирования параметров учетной записи.

4. В раскрывающемся списке выберите нужную роль учетной записи пользователя: **Администратор** или **Оператор**.

5. Нажмите на кнопку **Сохранить**.

   В карточке пользователя отобразится значок с именем пользователя и назначенная роль для его учетной записи.

Удаление учетной записи пользователя программы

При подключении к Серверу через веб-интерфейс вы можете удалять учетные записи, созданные в программе. Этот способ удаления недоступен для учетных записей пользователей Kaspersky Security Center, для которых настроена технология единого входа (SSO).

Удалить учетную запись пользователя программы могут только пользователи с ролью Администратор.

Пользователь с ролью Администратор может удалить любую учетную запись, кроме своей учетной записи.

Чтобы удалить учетную запись пользователя программы:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Пользователи**.

3. Нажмите на кнопку **Удалить** в карточке пользователя, которого вы хотите удалить.

   Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **ОК**.

Изменение пароля учетной записи

После подключения к Серверу через веб-интерфейс вы можете изменить пароль своей учетной записи, под которой выполнено подключение. Изменение пароля пользователя на странице веб-интерфейса Kaspersky Industrial CyberSecurity for Networks доступно только для учетной записи, созданной в программе. Этот способ изменения пароля недоступен для учетных записей пользователей Kaspersky Security Center, для которых настроена технология единого входа (SSO).

Рекомендуется изменять пароль в следующих случаях:

- выполнено первое подключение после создания учетной записи в программе;
- текущий пароль скомпрометирован;
- нужно выполнить регулярную смену пароля в соответствии с требованиями информационной безопасности на предприятии.

Чтобы изменить пароль своей учетной записи:

1. На странице веб-интерфейса Kaspersky Industrial CyberSecurity for Networks откройте меню пользователя:

   - Если меню свернуто, нажмите на кнопку .
   - Если меню развернуто, нажмите на кнопку справа от имени текущего пользователя.

2. В меню пользователя выберите пункт **Изменить пароль**.

   Появится окно **Изменение пароля**.

3. В поле **Текущий пароль** введите ваш текущий пароль.

4. В полях **Новый пароль** и **Новый пароль (повторно)** введите новый пароль.

   Новый пароль должен удовлетворять условиям, перечисленным в окне **Изменение пароля**. В процессе ввода пароля автоматически отмечаются выполненные условия.

5. Нажмите на кнопку **Изменить**. Кнопка доступна после ввода текущего и нового паролей и выполнения всех требований к новому паролю.

Новый пароль потребуется при следующем подключении к Серверу через веб-интерфейс.

Настройка контроля активов

Kaspersky Industrial CyberSecurity for Networks позволяет контролировать активы предприятия, представленные устройствами промышленной сети. Устройства идентифицируются программой по MAC- и/или IP-адресам. Программа может получать сведения об устройствах следующими способами:

- при обработке трафика, поступающего через точки мониторинга;
- при обработке данных, поступающих от EPP-приложений.

Для контроля активов в программе формируется таблица устройств. Таблица заполняется с учетом адресных пространств, настроенных в программе.

Программа может автоматически получать сведения об устройствах. Автоматическое получение и обновление сведений об устройствах поддерживается для таких сведений, которые программа может определить (например, адресная информация устройства).

Для обнаружения активности устройств и автоматического обновления сведений должны быть включены соответствующие методы технологии Контроль активов. При необходимости вы можете вручную указать значения конкретных сведений и выключить их автоматическое обновление, чтобы зафиксировать текущие значения (например, категорию устройства, если текущая заданная категория отличается от той, которая определяется автоматически).

Некоторые сведения об устройствах требуется указать вручную, для них не предусмотрено автоматическое обновление. Такие сведения позволяют сохранить в таблице устройств специфическую информацию, а также добавить отсутствующие критерии для упорядочивания и фильтрации устройств. В частности, с помощью заданных вручную сведений вы можете распределять устройства по разным группам в дереве групп или выполнять фильтрацию и поиск по меткам устройств.

Вы можете настраивать контроль активов и изменять сведения об устройствах в разделе **Активы** на вкладке **Устройства**. Также вы можете просматривать информацию о взаимодействиях устройств и выполнять различные действия с устройствами при работе с картой сетевых взаимодействий и с топологической картой. Для удобного представления информации о взаимодействиях устройств и для обеспечения автоматической группировки устройств по подсетям вы можете сформировать список подсетей в адресном пространстве с учетом особенностей IP-адресации устройств в сети вашего предприятия.

Методы и режимы контроля активов

Для контроля активов в Kaspersky Industrial CyberSecurity for Networks применяются следующие методы:

- Обнаружение активности устройств. Этот метод позволяет отслеживать активность устройств в трафике промышленной сети по полученным MAC- и/или IP-адресам устройств.
- Обнаружение сведений об устройствах. Этот метод позволяет автоматически получать и обновлять сведения об устройствах, известных программе, на основе полученных данных из трафика или от других источников.
- Контроль проектов ПЛК. Этот метод позволяет обнаруживать в трафике информацию о проектах ПЛК, сохранять эту информацию в программе и сравнивать с ранее полученной информацией.
- Обнаружение рисков. Этот метод позволяет обнаруживать риски информационной безопасности на основе данных об устройствах и их взаимодействиях.
- Обнаружение сетевых сессий. Этот метод позволяет обнаруживать в трафике промышленной сети сетевые сеансы, создаваемые устройствами для соединений с другими устройствами.

Вы можете включать и выключать применение методов контроля активов по отдельности.

О методе обнаружения активности устройств

Для метода обнаружения активности устройств предусмотрены следующие режимы:

- Режим обучения. Этот режим предназначен для временного использования. В этом режиме программа считает разрешенными все устройства, активность которых обнаружена в трафике. Вы можете включить режим обучения только для метода обнаружения активности устройств. При этом метод обнаружения активности устройств может применяться совместно с другими методами контроля активов.
- Режим наблюдения. Этот режим предназначен для постоянного использования. В этом режиме при обнаружении активности устройств программа считает разрешенными только те из них, которым присвоен статус *Разрешенное*.

В зависимости от выбранного режима программа автоматически присваивает статусы устройствам.

В режиме обучения программа не регистрирует события при обнаружении активности устройств или при автоматическом обновлении сведений об устройствах.

Вы можете настраивать режим обучения для метода обнаружения активности устройств. Режим обучения контроля активов должен быть включен на время, достаточное для обнаружения активности нужных устройств. Это время зависит от количества устройств в промышленной сети, периодичности их работы и обслуживания. Рекомендуется включать режим обучения на время не менее одного часа. В крупных промышленных сетях для обнаружения активности всех нужных устройств режим обучения можно включить на период от одного до нескольких дней.

Обработка полученных MAC- и IP-адресов устройств выполняется со следующими особенностями:

- Для устройств, которые выполняют функции сетевого коммутатора между сегментами промышленной сети, должен быть выставлен признак маршрутизирующего устройства. Если этот признак не был определен программой автоматически, то его требуется выставить вручную. Иначе программа может не добавить в таблицу устройств те устройства, которые взаимодействуют через это маршрутизирующее устройство в разных сегментах промышленной сети. После выставления признака взаимодействующие устройства будут добавлены в таблицу устройств при появлении соответствующего трафика с их участием.

- Если в трафике обнаружен только IP-адрес устройства (IP-адрес невозможно сопоставить с каким-либо MAC-адресом), этот IP-адрес проверяется на принадлежность известным программе подсетям. Для метода обнаружения активности устройств не учитываются IP-адреса, которые принадлежат только подсетям с типом **Публичная**.

О методе обнаружения сведений об устройствах

При включенном методе обнаружения сведений об устройствах программа автоматически изменяет сведения об известных устройствах. Например, программа может обновлять название операционной системы, установленной на устройстве, по мере обнаружения уточняющих данных в трафике этого устройства.

По умолчанию автоматическое изменение включено для всех сведений. Для некоторых сведений вы можете выключать автоматическое изменение при настройке параметров устройств: при добавлении устройства вручную, при объединении устройств или при изменении сведений об устройстве.

Для автоматического получения сведений об устройствах программа может использовать:

- Встроенные *правила определения сведений об устройствах и протоколов взаимодействия устройств*.

  После установки программы используются исходные правила определения сведений об устройствах и протоколов взаимодействия устройств. Для повышения точности определения специалисты "Лаборатории Касперского" регулярно обновляют базы с наборами правил. Вы можете обновлять правила, устанавливая обновления.

- Данные от EPP-приложений, содержащие сведения об устройствах.

  Программа обрабатывает поступающие данные от EPP-приложений, в которых непосредственно содержатся сведения об устройствах (например, сведения об оборудовании).

- Данные от EPP-приложений, обработанные по правилам из набора правил с *базой данных уязвимостей Kaspersky ICS CERT для АСУ ТП*.

  Правила из набора правил с базой данных уязвимостей Kaspersky ICS CERT для АСУ ТП позволяют проводить дополнительный анализ данных, поступающих от EPP-приложений. По результатам анализа программа может косвенно определить некоторые сведения об устройствах (например, категорию устройства). Набор правил **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП** является системным набором правил аудита безопасности. Этот набор правил поставляется и обновляется вместе с обновлениями баз и программных модулей. Поэтому, чтобы использовать правила из этого набора, вам нужно установить обновления.

О регистрируемых событиях при применении методов

В режиме наблюдения программа регистрирует соответствующие события по технологии Контроль активов. В зависимости от применяемых методов, события могут регистрироваться в следующих случаях:

- обнаружение активности неизвестных устройств или устройств со статусом *Неиспользуемое*;
- автоматическое изменение сведений об устройствах;
- обнаружение операций чтения или записи проектов и блоков проектов ПЛК;
- обнаружение рисков категории Уязвимость и изменений, связанных с такими рисками.

При включенном методе контроля проектов ПЛК программа может регистрировать большое количество событий, связанных с обнаружением операций чтения и записи проектов или блоков. Как правило, большое количество событий регистрируется на начальном этапе использования метода. Для сокращения общего количества регистрируемых событий после установки программы по умолчанию метод контроля проектов ПЛК выключен. Вы можете включить этот метод в любое время.

Выбор источников данных об уязвимостях

При контроле рисков программа обнаруживает уязвимости устройств, используя сведения из базы данных известных уязвимостей. Специалисты "Лаборатории Касперского" загружают сведения об уязвимостях в базу данных из различных источников данных об уязвимостях.

По умолчанию программа обнаруживает уязвимости устройств по сведениям, загруженным в базу данных из всех источников. При необходимости вы можете выбрать нужные источники, чтобы обнаруживать уязвимости устройств по сведениям только из этих источников.

Выбирать источники для обнаружения уязвимостей устройств могут только пользователи с ролью Администратор.

Чтобы включить или выключить использование источников для обнаружения уязвимостей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Риски** откройте окно для выбора источников по кнопке **Источники уязвимостей**.
3. Включите или выключите использование источников. Список содержит все источники в базе данных известных уязвимостей.
4. Нажмите на кнопку **Применить**.

Добавление устройств вручную

Этот раздел содержит инструкции по добавлению устройств вручную. Вы можете вручную добавить новое устройство в таблицу устройств. Для добавляемого устройства требуется указать MAC- и/или IP-адрес.

MAC- и IP-адреса добавленного устройства должны быть уникальны в пределах адресного пространства, к которому относятся эти адреса. Если в программу добавлены дополнительные адресные пространства, вы можете добавлять устройства с одинаковыми адресами в разные адресные пространства.

Добавлять устройства вручную могут только пользователи с ролью Администратор.

После добавления устройства вы можете добавить параметры контроля процесса для устройства.

Добавление устройства при работе с таблицей устройств

Чтобы добавить устройство при работе с таблицей устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Активы** на вкладке **Устройства** откройте область деталей по кнопке **Добавить устройство**.
3. На вкладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.
4. На вкладке **Адресная информация** в области деталей укажите MAC- и/или IP-адреса устройства.
5. Если в программу добавлены дополнительные адресные пространства, укажите имена адресных пространств для адресов.
6. Вы можете указать несколько IP-адресов для одного сетевого интерфейса устройства. Для формирования списка IP-адресов выполните одно из следующих действий:
   - Если вы хотите добавить IP-адрес, нажмите на кнопку **Добавить IP-адрес**.
   - Если вы хотите удалить IP-адрес, нажмите на значок , который расположен справа от поля со значением IP-адреса.

7. Если устройство имеет несколько сетевых интерфейсов, сформируйте список сетевых интерфейсов устройства и укажите для них соответствующие MAC- и/или IP-адреса.

   Для этого выполните одно из следующих действий:

   - Если вы хотите добавить сетевой интерфейс, нажмите на кнопку **Добавить интерфейс**, которая расположена под группой параметров последнего сетевого интерфейса устройства.
   - Если вы хотите удалить сетевой интерфейс, нажмите на значок ×, который расположен справа от названия сетевого интерфейса устройства (при наличии двух и более сетевых интерфейсов).
   - Если вы хотите задать другое имя для сетевого интерфейса, нажмите на значок ✎, который расположен справа от текущего имени, и введите новое имя сетевого интерфейса в появившемся поле.

8. На вкладках **Параметры** и **Адресная информация** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте значки 🔒 и 🔓. На вкладке **Параметры** значки 🔒 и 🔓 расположены в левой части полей. На вкладке **Адресная информация** значки 🔒 и 🔓 расположены справа от названия сетевого интерфейса.

9. На вкладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей.

10. Нажмите на кнопку **Сохранить**.

    Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

В таблице устройств появится новое устройство со статусом *Разрешенное*.

Добавление устройства при работе с топологической картой

При работе с топологической картой вы можете добавить новое устройство в таблицу устройств.

Чтобы добавить новое устройство в таблицу устройств при работе с топологической картой:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Карта сети** на вкладке **Топологическая карта** в раскрывающемся списке **Добавить узел** выберите пункт **Новое устройство**.

   В правой части окна появится область деталей с параметрами устройства.

3. На вкладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.

4. На вкладке **Адресная информация** в области деталей укажите MAC- и/или IP-адреса устройства.

5. Если в программу добавлены дополнительные адресные пространства, укажите имена адресных пространств для адресов.

6. Вы можете указать несколько IP-адресов для одного сетевого интерфейса устройства. Для формирования списка IP-адресов выполните одно из следующих действий:

   - Если вы хотите добавить IP-адрес, нажмите на кнопку **Добавить IP-адрес**.
   - Если вы хотите удалить IP-адрес, нажмите на значок , который расположен справа от поля со значением IP-адреса.

7. Если устройство имеет несколько сетевых интерфейсов, сформируйте список сетевых интерфейсов устройства и укажите для них соответствующие MAC- и/или IP-адреса.

   Для этого выполните одно из следующих действий:

   - Если вы хотите добавить сетевой интерфейс, нажмите на кнопку **Добавить интерфейс**, которая расположена под группой параметров последнего сетевого интерфейса устройства.
   - Если вы хотите удалить сетевой интерфейс, нажмите на значок , который расположен справа от названия сетевого интерфейса устройства (при наличии двух и более сетевых интерфейсов).
   - Если вы хотите задать другое имя для сетевого интерфейса, нажмите на значок , который расположен справа от текущего имени, и введите новое имя сетевого интерфейса в появившемся поле.

8. На вкладках **Параметры** и **Адресная информация** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте значки и . На вкладке **Параметры** значки и расположены в левой части полей. На вкладке **Адресная информация** значки и расположены справа от названия сетевого интерфейса.

9. На вкладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей.

10. Нажмите на кнопку **Сохранить**.

    Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

В таблице устройств появится новое устройство со статусом *Разрешенное*.

Добавление устройства на основе узла неизвестного устройства на карте сетевых взаимодействий

При работе с картой сетевых взаимодействий вы можете добавить новое устройство в таблицу устройств на основе узла, который представляет неизвестное программе устройство.

Чтобы добавить узел неизвестного устройства в таблицу устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите нужный узел, представляющий неизвестное программе устройство.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Добавить в таблицу устройств**.

   В области деталей появятся вкладки для настройки параметров нового устройства.

4. Настройте параметры нового устройства, не изменяя MAC и/или IP-адрес, которые указаны для узла.

   Описание действий для настройки параметров см. в процедуре добавления устройства вручную при работе с таблицей устройств.

5. Нажмите на кнопку **Сохранить**.

В таблице устройств появится новое устройство со статусом *Разрешенное*. Узел на карте сетевых взаимодействий, который ранее представлял неизвестное программе устройство, будет представлять известное программе устройство.

Добавление устройства на основе неуправляемого коммутатора на топологической карте

При работе с топологической картой вы можете добавить новое устройство в таблицу устройств на основе узла, который представляет неуправляемый коммутатор.

Чтобы добавить узел неуправляемого коммутатора в таблицу устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Карта сети** на вкладке **Топологическая карта** выберите нужный узел, представляющий неуправляемый коммутатор.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Добавить в таблицу устройств**.

   В области деталей появятся вкладки для настройки параметров нового устройства.

4. Укажите MAC и/или IP-адрес устройства и настройте остальные параметры.

   Описание действий для настройки параметров см. в процедуре добавления устройства вручную при работе с таблицей устройств.

5. Нажмите на кнопку **Сохранить**.

В таблице устройств появится новое устройство со статусом *Разрешенное***.** Узел на топологической карте, который ранее представлял неуправляемый коммутатор, будет представлять известное программе устройство.

Объединение устройств

Этот раздел содержит инструкции по объединению устройств.

Если по каким-либо причинам одно устройство представлено как несколько устройств в таблице, эти устройства можно объединить в одно устройство. Объединение устройств может выполняться автоматически при включенном методе обнаружения активности устройств в режиме обучения. Также вы можете объединять устройства вручную.

Автоматическое объединение устройств происходит в случае, если программа определила связь MAC-адреса одного устройства и IP-адреса другого устройства или связь между устройствами в соответствии с результатами активного опроса или данными, полученными от EPP-приложений. При этом, если возникают конфликты заданных значений в сведениях об устройствах, в объединенном устройстве сохранятся те значения, которые были заданы для следующих устройств:

- Устройства с IP-адресом, если обнаружена связь MAC-адреса одного устройства и IP-адреса другого устройства.

  > Перед включением режима обучения (и во время работы в этом режиме) не рекомендуется изменять сведения об устройствах, для которых задан только MAC-адрес и возможно автоматическое объединение с устройствами с заданными IP-адресами.

- Устройства с IP-адресом и установленным программным компонентом Endpoint Agent, если обнаружена связь между устройствами в соответствии с данными от EPP-приложений.
- Устройства с наибольшим количеством IP-адресов.
- Устройства с наибольшим количеством адресов, если у устройств отсутствуют IP-адреса.

При объединении устройств некоторые сведения из объединяемых устройств могут не сохраниться в новом устройстве (например, содержимое динамических полей и параметров топологии). Кроме того, для объединения устройств требуется, чтобы суммарное количество сетевых интерфейсов в новом устройстве получилось не более 512.

Объединять устройства вручную могут только пользователи с ролью Администратор.

Объединение устройств при работе с таблицей устройств

Чтобы объединить устройства при работе с таблицей устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, которые вы хотите объединить.
4. Нажмите на кнопку **Объединить устройства**.

   В правой части окна появится область деталей с вкладками для настройки параметров нового устройства.

5. Проверьте и при необходимости измените параметры нового устройства:

   - На вкладке **Параметры** в области деталей все поля, содержащие разные значения в выбранных устройствах, отмечены сообщениями о конфликте значений. При этом в текстовых полях различные значения объединяются в одно значение. При необходимости включите или выключите автоматическое изменение для нужных сведений об устройстве.

   - На вкладке **Адресная информация** в области деталей MAC- и IP-адреса выбранных устройств распределяются по отдельным сетевым интерфейсам. При необходимости измените значения адресов, адресные пространства и имена сетевых интерфейсов, включите или выключите автоматическое изменение для нужных сведений об устройстве.

   - На вкладке **Пользовательские поля** в области деталей список содержит все пользовательские поля выбранных устройств.

6. Нажмите на кнопку **Объединить**.

   Откроется окно с запросом подтверждения.

7. В окне запроса нажмите на кнопку **OK**.

В таблице устройств появится новое устройство со статусом *Разрешенное*.

Объединение устройств при работе с картой сетевых взаимодействий и топологической картой

При работе с картой сетевых взаимодействий и с топологической картой вы можете объединить несколько узлов на картах в одно новое устройство для таблицы устройств.

Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

В объединении не могут участвовать узлы WAN.

Чтобы объединить устройства, представленные узлами на картах:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Карта сети**.

3. На вкладке **Карта сетевых взаимодействий** или **Топологическая карта** выберите несколько объектов, представляющих узлы и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.

   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

4. Нажмите на кнопку **Объединить устройства**.

   В правой части окна появится область деталей с вкладками для настройки параметров нового устройства.

5. Проверьте и при необходимости измените параметры нового устройства:

   - На вкладке **Параметры** в области деталей все поля, содержащие разные значения в выбранных устройствах, отмечены сообщениями о конфликте значений. При этом в текстовых полях различные значения объединяются в одно значение. При необходимости включите или выключите автоматическое изменение для нужных сведений об устройстве.

   - На вкладке **Адресная информация** в области деталей MAC- и IP-адреса выбранных устройств распределяются по отдельным сетевым интерфейсам. При необходимости измените значения адресов, адресные пространства и имена сетевых интерфейсов, включите или выключите автоматическое изменение для нужных сведений об устройстве.

   - На вкладке **Пользовательские поля** в области деталей список содержит все пользовательские поля выбранных устройств.

6. Нажмите на кнопку **Объединить**.

   Откроется окно с запросом подтверждения.

7. В окне запроса нажмите на кнопку **ОК**.

В таблице устройств появится новое устройство со статусом *Разрешенное*. На карте сети появится один объединенный узел вместо ранее выбранных нескольких узлов.

Удаление устройств

Этот раздел содержит инструкции по удалению устройств. Вы можете удалить одно или несколько устройств из таблицы устройств.

Удалять устройства могут только пользователи с ролью Администратор.

Информация об удаленных устройствах не сохраняется в программе. Если удаленные устройства снова проявят активность в промышленной сети, программа добавит их в таблицу устройств как новые устройства (со статусом *Разрешенное* или *Неразрешенное* в зависимости от текущего режима работы контроля активов).

Удаление устройств при работе с таблицей устройств

Чтобы удалить устройство при работе с таблицей устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Активы**.

3. На вкладке **Устройства** выберите устройства, которые вы хотите удалить.

4. По правой кнопке мыши откройте контекстное меню одного из выбранных устройств.

5. В контекстном меню выберите один из следующих пунктов:

   - **Удалить устройство**, если выбрано одно устройство.
   - **Удалить устройства**, если выбрано несколько устройств.

   Откроется окно с запросом подтверждения.

6. В окне запроса нажмите на кнопку **ОК**.

Удаление устройств при работе с картой сетевых взаимодействий и топологической картой

При работе с картой сетевых взаимодействий и с топологической картой вы можете удалять устройства из таблицы устройств, используя узлы на картах, представляющие известные программе устройства.

Чтобы удалить устройство при работе с картами:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Карта сети**.
3. На вкладке **Карта сетевых взаимодействий** или **Топологическая карта** выберите узел, представляющий известное программе устройство.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

5. В окне запроса нажмите на кнопку **ОК**.

Изменение статусов устройств вручную

Этот раздел содержит инструкции по изменению статуса устройств. Изменять статусы устройств могут только пользователи с ролью Администратор.

Вы можете изменить статус (выбрать один из статусов *Разрешенное*, *Неразрешенное* или *Неиспользуемое*) для одного выбранного устройства или одновременно для нескольких выбранных устройств. Если вы изменяете статус одного выбранного устройства, вы можете включить или выключить автоматическое изменение статуса этого устройства на статус Неиспользуемое.

При использовании коннекторов типа **Cisco Switch** может происходить автоматическое ограничение сетевого доступа устройств после присвоения этим устройствам статуса *Неразрешенное*. Вам нужно учитывать заданные параметры коннекторов этого типа, чтобы не допустить блокировку нужных устройств из-за изменения их статуса.

После присвоения устройству статуса *Неиспользуемое* программа может автоматически изменить статус этого устройства, если оно проявит активность. В зависимости от текущего режима работы контроля активов программа присвоит обнаруженному устройству статус *Разрешенное* или *Неразрешенное*.

Изменение статусов устройств при работе с таблицей устройств

Чтобы изменить статус одного устройства при работе с таблицей устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Активы** на вкладке **Устройства** выберите нужное устройство.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для просмотра и изменения сведений об устройстве: **Параметры**, **Адресная информация** и **Пользовательские поля**.
4. Перейдите на вкладку **Параметры**.
5. В раскрывающемся списке **Статус** выберите нужный статус устройства.
6. Включите или выключите автоматическое изменение статуса устройства на статус *Неиспользуемое*. Для этого используйте значок , расположенный в раскрывающемся списке **Статус**.

   Выключение автоматического изменения статуса может потребоваться, например, если вы хотите, чтобы статус *Разрешенное* не изменялся на статус *Неиспользуемое* для редко подключаемого устройства.
7. Нажмите на кнопку **Сохранить**.

Чтобы изменить статус нескольких устройств при работе с таблицей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите вкладку **Устройства** в разделе **Активы**.
3. В таблице устройств выберите устройства, статус которых вы хотите изменить.
4. Откройте раскрывающийся список **Изменить статус** в панели инструментов.
5. В раскрывающемся списке выберите пункт для присвоения нужного статуса.

   Откроется окно с запросом подтверждения.
6. В окне запроса нажмите на кнопку **ОК**.

Изменение статусов устройств при работе с картой сетевых взаимодействий и топологической картой

При работе с картой сетевых взаимодействий и с топологической картой вы можете изменять статусы известных программе устройств, представленных узлами на картах.

Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы изменить статус одного устройства при работе с картами:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Карта сети**.
3. На вкладке **Карта сетевых взаимодействий** или **Топологическая карта** выберите узел нужного устройства.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для просмотра и изменения сведений об устройстве: **Параметры**, **Адресная информация** и **Пользовательские поля**.
5. Перейдите на вкладку **Параметры**.
6. В раскрывающемся списке **Статус** выберите нужный статус устройства.
7. Включите или выключите автоматическое изменение статуса устройства на статус *Неиспользуемое*. Для этого используйте значок в раскрывающемся списке **Статус**.

   Выключение автоматического изменения статуса может потребоваться, например, если вы хотите, чтобы статус *Разрешенное* не изменялся на статус *Неиспользуемое* для редко подключаемого устройства.
8. Нажмите на кнопку **Сохранить**.

Чтобы изменить статус нескольких устройств при работе с картами:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Карта сети**.

3. На вкладке **Карта сетевых взаимодействий** или **Топологическая карта** выберите объекты, представляющие узлы известных программе устройств и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

4. Откройте раскрывающийся список **Изменить статус** в панели инструментов.

5. В раскрывающемся списке выберите пункт для присвоения нужного статуса.

   Откроется окно с запросом подтверждения.

6. В окне запроса нажмите на кнопку **OK**.

О распределении устройств по группам

Вы можете распределять устройства по группам, используя дерево групп устройств. Дерево групп устройств поддерживает до шести уровней вложенности.

Устройства могут быть помещены в группы любого уровня иерархии. При этом каждое устройство может быть добавлено только в одну из групп дерева.

Для дерева действует ограничение по количеству групп – не более 1000.

До включения устройства в какую-либо группу сведения об этом устройстве не содержат информацию о размещении устройства. Такое устройство относится к верхнему уровню иерархии в дереве групп. После включения устройства в группу в программе сохраняется размещение этого устройства в виде полного пути к группе в дереве групп.

Для распределения устройств по группам предусмотрены следующие способы:

- Автоматическая группировка устройств по заданному критерию.

  При такой группировке устройств программа может автоматически добавлять группы в дерево групп устройств. Группы добавляются при обнаружении устройств, в которых есть сведения, соответствующие выбранному критерию группировки. Имена для групп задаются из диапазона значений выбранного критерия (например, из названий категорий устройств при группировке по категориям).

- Распределение устройств по группам вручную.

  Вы можете вручную распределять устройства по группам, включая устройства в нужные группы и исключая из групп. При необходимости вы можете вносить изменения в дерево групп устройств, используя функции формирования дерева групп устройств вручную.

Автоматическая группировка устройств по заданному критерию

Этот раздел содержит инструкции по автоматической группировке устройств по заданному критерию. Вы можете автоматически группировать устройства в дереве групп устройств по одному из следующих критериев:

- принадлежность IP-адресов известным программе подсетям;
- категории устройств;
- производители устройств.

Выполнять автоматическую группировку устройств могут только пользователи с ролью Администратор.

Автоматическая группировка устройств по заданному критерию, начиная с верхнего уровня иерархии в дереве групп

Чтобы сгруппировать устройства автоматически по заданному критерию, начиная с верхнего уровня иерархии в дереве групп:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** нажмите на одну из следующих кнопок выбора критерия группировки в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий:
   - – для группировки устройств по подсетям;
   - – для группировки устройств по категориям;
   - – для группировки устройств по производителям.

   Откроется окно запроса для выбора варианта группировки.
3. Если требуется группировать устройства по категориям и производителям с учетом адресных пространств, в окне запроса установите флажок **Учитывать адресные пространства**.
4. Нажмите на одну из следующих кнопок в зависимости от нужного результата:
   - Если вы хотите сгруппировать устройства по подсетям, нажмите на кнопку **Сгруппировать**.
   - Если вы хотите сгруппировать устройства с учетом адресных пространств по категориям или производителям во всех группах дерева групп устройств, нажмите на кнопку **Вместе с дочерними**.
   - Если вы хотите сгруппировать устройства с учетом адресных пространств по категориям или производителям только на верхнем уровне иерархии дерева групп устройств, нажмите на кнопку **Только выбранную группу**.

Программа определит устройства, подходящие под выбранный критерий группировки, создаст группы для этих устройств и поместит устройства в эти группы.

Автоматическая группировка устройств в выбранной группе устройств

Чтобы сгруппировать устройства автоматически в выбранной группе устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите группу, в которой вы хотите автоматически сгруппировать устройства.
3. По правой кнопке мыши откройте контекстное меню.
4. В контекстном меню выберите один из следующих пунктов:
   - **По подсетям**.
   - **По категориям**.
   - **По производителям**.

   Откроется окно запроса для выбора варианта группировки.
5. Если требуется группировать устройства по категориям и производителям с учетом адресных пространств, в окне запроса установите флажок **Учитывать адресные пространства**.
6. В окне запроса нажмите на одну из следующих кнопок в зависимости от нужного результата:
   - Если вы хотите сгруппировать устройства по подсетям, нажмите на кнопку **Сгруппировать**.
   - Если вы хотите сгруппировать устройства по категориям или производителям во всех дочерних группах выбранной группы, нажмите на кнопку **Вместе с дочерними**.
   - Если вы хотите сгруппировать устройства по категориям или производителям только в выбранной группе, нажмите на кнопку **Только выбранную группу**.

   Программа определит устройства, подходящие под выбранный критерий группировки, создаст группы для этих устройств и поместит устройства в эти группы (при этом устройства в других группах не будут распределены по новым группам).

Распределение устройств по группам вручную

Этот раздел содержит инструкции по управлению размещением устройств в дереве групп вручную. Управлять размещением устройств в дереве групп могут только пользователи с ролью Администратор.

Включение одного устройства в группу

Чтобы включить одно устройство в группу при работе с таблицей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройство для добавления в группу как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. В области деталей перейдите на вкладку **Параметры**.
5. Нажмите на значок в правой части поля **Группа**.

   Появится окно **Выбор группы в дереве**.
6. В дереве групп устройств выберите нужную группу.

   Если нужная группа отсутствует в дереве, вы можете ее добавить в текущем открытом окне **Выбор группы в дереве**.
7. Нажмите на кнопку **Выбрать**.

   Путь к выбранной группе появится в поле **Группа**.
8. Нажмите на кнопку **Сохранить** в области деталей.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

Включение нескольких устройств в группу

Вы можете включить в группу несколько устройств при работе с таблицей устройств.

Также при работе с картой сетевых взаимодействий вы можете включить в группу несколько известных программе устройств, представленных узлами на карте сетевых взаимодействий. Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы включить несколько устройств в группу при работе с таблицей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, которые вы хотите включить в группу.

4. По правой кнопке мыши откройте контекстное меню.

5. В контекстном меню выберите пункт **Управление группами → Переместить в группу**.

   Появится окно **Выбор группы в дереве**.

6. В дереве групп устройств выберите нужную группу.

   Если нужная группа отсутствует в дереве, вы можете ее добавить в текущем открытом окне **Выбор группы в дереве**.

7. Нажмите на кнопку **Выбрать**.

   Путь к выбранной группе появится в столбце **Группа**.

Чтобы включить несколько устройств в группу при работе с картой сетевых взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите нужные узлы известных программе устройств и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

3. По правой кнопке мыши откройте контекстное меню.

4. В контекстном меню выберите пункт **Переместить в группу**.

   Появится окно **Выбор группы в дереве**.

5. В дереве групп устройств выберите нужную группу.

   Если нужная группа отсутствует в дереве, вы можете ее добавить в текущем открытом окне **Выбор группы в дереве**.

6. Нажмите на кнопку **Выбрать**.

   Выбранные узлы, представляющие известные программе устройства, отобразятся внутри выбранной группы.

Исключение одного устройства из группы

Чтобы исключить одно устройство из группы при работе с таблицей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройства для исключения из группы как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Изменить**.

4. В области деталей перейдите на вкладку **Параметры**.

5. В поле **Группа** удалите путь к группе с помощью значка ✕ в поле (значок отображается, если группа задана).

6. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком •.

После сохранения изменений для устройства очистится параметр **Группа** и устройство будет относиться к верхнему уровню иерархии в дереве групп.

Исключение нескольких устройств из групп

Вы можете исключить из групп несколько устройств при работе с таблицей устройств. Устройства, выбранные для исключения из групп, могут быть включены как в одну и ту же группу, так и в разные группы.

Также при работе с картой сетевых взаимодействий вы можете исключить из групп несколько известных программе устройств, представленных узлами на карте сетевых взаимодействий. Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы исключить несколько устройств из групп при работе с таблицей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Активы**.

3. На вкладке **Устройства** выберите устройства, которые вы хотите исключить из групп.

4. По правой кнопке мыши откройте контекстное меню.

5. В контекстном меню выберите пункт **Управление группами → Исключить из групп**.

   Откроется окно с запросом подтверждения.

6. В окне запроса подтвердите исключение устройств из групп.

Для всех выбранных устройств очистится параметр **Группа** и эти устройства будут относиться к верхнему уровню иерархии в дереве групп.

Чтобы исключить несколько устройств из групп при работе с картой сетевых взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите узлы в развернутых группах и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.
3. По правой кнопке мыши откройте контекстное меню.
4. В контекстном меню выберите пункт **Исключить из групп**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите исключение устройств из групп.

Для всех выбранных устройств очистится параметр **Группа** и эти устройства отобразятся вне групп.

Перемещение узлов и групп в другие группы на карте сетевых взаимодействий

Вы можете изменять размещение узлов и групп в дереве групп устройств, перетаскивая объекты на карте сетевых взаимодействий. После перемещения узлы и группы изменяют свое размещение в дереве групп устройств так же, как при включении устройств в группу и исключении устройств из групп.

Перемещать узлы и группы в другие группы могут только пользователи с ролью Администратор.

Чтобы переместить узлы и/или группы в другие группы:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** выберите нужные узлы известных программе устройств и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.
3. Наведите курсор на один из выбранных объектов (группу или узел, представляющий известное программе устройство).

4. Нажмите на клавишу **CTRL** и, удерживая ее нажатой, перетащите выбранные объекты в нужную группу (или в любое место вне групп, если вы хотите переместить выбранные объекты на верхний уровень иерархии в дереве групп).

   Откроется окно с запросом подтверждения.

5. В окне запроса подтвердите перемещение выбранных объектов.

Формирование дерева групп устройств вручную

Вы можете формировать дерево групп устройств при работе с таблицей устройств, с картой сетевых взаимодействий и топологической картой. Функции для формирования дерева доступны в окне **Формирование дерева групп** или **Выбор группы в дереве**.

Формировать дерево групп устройств могут только пользователи с ролью Администратор.

Чтобы использовать функции для формирования дерева групп устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети** выполните одно из следующих действий:

   - Откройте окно **Формирование дерева групп** по кнопке **Настроить группы**.

     Кнопка **Настроить группы** в разделе **Активы** доступна в раскрывающемся списке **Управление группами** в панели инструментов.

     Кнопка **Настроить группы** в разделе **Карта сети** доступна только на вкладке **Карта сетевых взаимодействий**.

   - Откройте окно **Выбор группы в дереве**, выполняя добавление устройств в группы. Вы также можете открыть это окно при фильтрации таблицы устройств по столбцу **Группа**.

Изменения, сделанные в дереве групп устройств в окне **Формирование дерева групп** или **Выбор группы в дереве**, применяются сразу.

Этот раздел содержит инструкции по использовании функций для формирования дерева групп устройств.

Добавление группы

Чтобы добавить группу в дерево групп устройств:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** добавьте новую группу одним из следующих способов:

   - Если дерево пустое и вы хотите добавить первую группу, нажмите на кнопку **Добавить** или на любую из клавиш **INSERT** или **ENTER**.
   - Если вы хотите добавить группу на одном уровне иерархии с имеющейся группой, выберите эту группу и нажмите на клавишу **ENTER**.
   - Если вы хотите добавить дочернюю группу к имеющейся группе, выберите эту группу и нажмите на кнопку **Добавить** или на клавишу **INSERT**.

2. В поле ввода введите имя группы.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`.

   Имя группы должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 255 символов;
   - не совпадает с именем другой группы из числа включенных в ту же родительскую группу (регистр символов не учитывается).

3. Нажмите на значок ✓ справа от поля ввода.

Переименование группы

Чтобы переименовать группу в дереве групп устройств:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** выберите группу, которую вы хотите переименовать.

2. Нажмите на кнопку **Переименовать** или на клавишу **F2**.

3. В поле ввода введите новое имя группы.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`.

   Имя группы должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 255 символов;
   - не совпадает с именем другой группы из числа включенных в ту же родительскую группу (регистр символов не учитывается).

4. Нажмите на значок ✓ справа от поля ввода.

Новое имя группы появится в сведениях об устройствах, которые добавлены в эту группу или в ее дочерние группы.

Удаление групп

При удалении группы не удаляются устройства, добавленные в эту группу. Устройства из удаленной группы переводятся на тот же уровень иерархии в дереве устройств, на котором была удаленная группа.

Чтобы удалить группу в дереве групп устройств:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** выберите группу, которую вы хотите удалить.
2. Нажмите на значок 🗑.

   Откроется окно запроса для выбора варианта удаления.

3. В окне запроса нажмите на одну из следующих кнопок в зависимости от нужного результата:

   - Если вы хотите удалить только выбранную группу и оставить ее дочерние группы, нажмите на кнопку **Только выбранную**.
   - Если вы хотите удалить выбранную группу вместе со всеми ее дочерними группами, нажмите на кнопку **Вместе с дочерними**.

   Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **ОК**.

Перемещение группы

Чтобы переместить группу в дереве групп устройств:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** выберите группу, которую вы хотите переместить.

2. Используйте значки с изображением стрелок или соответствующие им комбинации клавиш **ALT+**↓, **ALT+**↑, **ALT+**←, **ALT+**→ для перемещения группы относительно других элементов дерева. Если невозможно выполнить какую-либо операцию, значок этой операции недоступен.

Поиск групп

Вы можете найти нужные группы в дереве групп устройств с помощью поля **Поиск групп** в окне **Формирование дерева групп** или **Выбор группы в дереве**. Группы, которые удовлетворяют условиям поиска, отобразятся в дереве групп устройств. Для групп, являющихся дочерними, также отображаются их родительские группы.

Обновление дерева

Состав групп в дереве групп устройств может быть изменен на Сервере в то время, когда вы работаете с деревом (например, другим пользователем, который выполнил подключение к Серверу).

Вы можете вручную обновлять дерево с помощью значка в окне **Формирование дерева групп** или **Выбор группы в дереве**.

Установка и удаление меток для устройств

Этот раздел содержит инструкции по установке и удалении меток для устройств. Вы можете присваивать устройствам произвольные метки.

Метка устройства содержит текстовое описание, которое позволяет быстро находить или фильтровать устройства в таблице. В качестве меток вы можете сохранять любые удобные вам текстовые описания. Для устройства можно назначить до 16 меток. При этом каждое устройство может иметь свой набор меток.

Списки меток устройств отображаются в таблице устройств в столбце **Метки**. Метки сортируются в ячейке в алфавитном порядке.

Устанавливать и удалять метки для устройств могут только пользователи с ролью Администратор.

Установка меток для одного устройства

Чтобы установить метку для одного устройства:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройства для установки его метки как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Изменить**.

   В области деталей перейдите на вкладку **Параметры**.

4. В поле **Метки** введите текстовые описания, которые вы хотите использовать в качестве меток. Для разделения меток вы можете использовать клавишу **ENTER** или символ **;**.

   Вы можете использовать прописные и строчные буквы, цифры, пробел, а также следующие специальные символы: **! @ # № $ % ^ & ( ) [ ] { } ' , . - _**.

   Имя метки должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - является уникальным в списке меток устройства (регистр символов не учитывается);
   - содержит от 1 до 255 символов.

5. При необходимости скопируйте список меток с помощью ссылки **Копировать метки**. Ссылка отображается, если список меток не пустой.

6. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком **.**.

Установка меток для нескольких устройств

Вы можете установить метки для нескольких устройств при работе с таблицей устройств.

Также при работе с картой сетевых взаимодействий и с топологической картой вы можете установить метки для известных программе устройств, представленных узлами на картах. Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы установить метки для нескольких устройств при работе с таблицей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Активы**.

3. На вкладке **Устройства** выберите устройства, для которых вы хотите установить метки.

4. По правой кнопке мыши откройте контекстное меню одного из выбранных устройств.

5. В контекстном меню выберите пункт **Установить метки**.

   Появится окно **Добавление меток**.

6. В поле **Метки** введите текстовые описания, которые вы хотите использовать в качестве меток. Для разделения меток вы можете использовать клавишу **ENTER** или символ **;**.

   Вы можете использовать прописные и строчные буквы, цифры, пробел, а также следующие специальные символы: **! @ # № $ % ^ & ( ) [ ] { } ' , . - _**.

   Имя метки должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - является уникальным в списке меток устройства (регистр символов не учитывается);
   - содержит от 1 до 255 символов.

7. При необходимости скопируйте список меток с помощью ссылки **Копировать метки**. Ссылка отображается, если список меток не пустой.

8. Если вы хотите очистить текущие списки меток для выбранных устройств и указать для этих устройств только новые метки, установите флажок **Удалить существующие**.

   Если снят флажок **Удалить существующие**, на каждом устройстве останется его текущий список меток. Списки меток на всех выбранных устройствах дополнятся новыми метками. В этом случае для некоторых из выбранных устройств суммарное количество меток может превысить ограничение (до 16 меток для каждого устройства). Программа проверяет это ограничение перед добавлением новых меток.

9. Нажмите на кнопку **ОК**.

   Кнопка недоступна, если имена введенных меток не удовлетворяют требованиям или если список меток пустой и при этом снят флажок **Удалить существующие**.

Чтобы установить метки для нескольких устройств при работе с картами:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Карта сети**.

3. На вкладке **Карта сетевых взаимодействий** или **Топологическая карта** выберите нужные узлы известных программе устройств и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

4. По правой кнопке мыши откройте контекстное меню одного из выбранных объектов.

5. В контекстном меню выберите пункт **Установить метки**.

   Появится окно **Добавление меток**.

6. В поле **Метки** введите текстовые описания, которые вы хотите использовать в качестве меток. Для разделения меток вы можете использовать клавишу **ENTER** или символ **;**.

   Вы можете использовать прописные и строчные буквы, цифры, пробел, а также следующие специальные символы: **! @ # № $ % ^ & ( ) [ ] { } ' , . - _**.

   Имя метки должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - является уникальным в списке меток устройства (регистр символов не учитывается);
   - содержит от 1 до 255 символов.

7. При необходимости скопируйте список меток с помощью ссылки **Копировать метки**. Ссылка отображается, если список меток не пустой.

8. Если вы хотите очистить текущие списки меток для выбранных устройств и указать для этих устройств только новые метки, установите флажок **Удалить существующие**.

   Если снят флажок **Удалить существующие**, на каждом устройстве останется его текущий список меток. Списки меток на всех выбранных устройствах дополнятся новыми метками. В этом случае для некоторых из выбранных устройств суммарное количество меток может превысить ограничение (до 16 меток для каждого устройства). Программа проверяет это ограничение перед добавлением новых меток.

9. Нажмите на кнопку **OK**.

   Кнопка недоступна, если имена введенных меток не удовлетворяют требованиям или если список меток пустой и при этом снят флажок **Удалить существующие**.

Удаление меток для одного устройства

Чтобы удалить метку для одного устройства:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройства для удаления его метки как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.

   В области деталей перейдите на вкладку **Параметры**.
4. В поле **Метки** удалите лишние метки:

   - с помощью значка × рядом с названиями меток, если вы хотите удалить определенные метки;
   - с помощью значка × в правой части поля **Метки**, если вы хотите удалить все метки.
5. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

Очистка списков меток для нескольких устройств

Вы можете очистить списки меток для нескольких устройств при работе с таблицей устройств.

Также при работе с картой сетевых взаимодействий и с топологической картой вы можете очистить списки меток для известных программе устройств, представленных узлами на картах. Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Чтобы очистить списки меток для нескольких устройств при работе с таблицей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, для которых вы хотите очистить списки меток.
4. По правой кнопке мыши откройте контекстное меню одного из выбранных устройств.
5. В контекстном меню выберите пункт **Установить метки**.

   Появится окно **Добавление меток**.

6. Установите флажок **Удалить существующие**.
7. Нажмите на кнопку **OK**.

Чтобы очистить списки меток для нескольких устройств при работе с картами:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Карта сети**.
3. На вкладке **Карта сетевых взаимодействий** или **Топологическая карта** выберите нужные узлы известных программе устройств и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.
4. По правой кнопке мыши откройте контекстное меню одного из выбранных объектов.
5. В контекстном меню выберите пункт **Установить метки**.

   Появится окно **Добавление меток**.
6. Установите флажок **Удалить существующие**.
7. Нажмите на кнопку **OK**.

Изменение сведений об устройстве

Изменять сведения об устройстве могут только пользователи с ролью Администратор.

Чтобы изменить сведения об устройстве вручную:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Активы** на вкладке **Устройства** выберите нужное устройство.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для просмотра и изменения сведений об устройстве: **Параметры**, **Адресная информация** и **Пользовательские поля**.
4. На вкладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.
5. На вкладке **Адресная информация** в области деталей укажите MAC- и/или IP-адреса устройства.
6. Если в программу добавлены дополнительные адресные пространства, укажите имена адресных пространств для адресов.

7. Вы можете указать несколько IP-адресов для одного сетевого интерфейса устройства. Для формирования списка IP-адресов выполните одно из следующих действий:

   - Если вы хотите добавить IP-адрес, нажмите на кнопку **Добавить IP-адрес**.
   - Если вы хотите удалить IP-адрес, нажмите на значок , который расположен справа от поля со значением IP-адреса.

8. Если устройство имеет несколько сетевых интерфейсов, сформируйте список сетевых интерфейсов устройства и укажите для них соответствующие MAC- и/или IP-адреса.

   Для формирования списка сетевых интерфейсов устройства выполните одно из следующих действий:

   - Если вы хотите добавить сетевой интерфейс, нажмите на кнопку **Добавить интерфейс**, которая расположена под группой параметров последнего сетевого интерфейса устройства.
   - Если вы хотите удалить сетевой интерфейс, нажмите на значок , который расположен справа от названия сетевого интерфейса устройства (при наличии двух и более сетевых интерфейсов).
   - Если вы хотите задать другое имя для сетевого интерфейса, нажмите на значок , который расположен справа от текущего имени, и введите новое имя сетевого интерфейса в появившемся поле.

9. На вкладках **Параметры** и **Адресная информация** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте значки и . На вкладке **Параметры** значки и расположены в левой части полей. На вкладке **Адресная информация** значки и расположены справа от названия сетевого интерфейса. Для поля **Статус** включение и выключение автоматических изменений статусов устройств выполняется с помощью значка .

10. На вкладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей и их значений.

11. Нажмите на кнопку **Сохранить**.

    Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Вкладка с параметрами, требующими ввода правильных значений, отмечена значком .

После сохранения изменений в сведениях об устройстве вы можете добавить или изменить параметры контроля процесса для устройства.

Добавление, изменение и удаление пользовательских полей для устройства

Вы можете добавлять, изменять и удалять пользовательские поля со сведениями об устройствах. Пользовательские поля отображаются в области деталей при выборе устройства.

Для пользовательских полей действуют следующие ограничения:

- количество пользовательских полей для одного устройства – не более 16;
- количество символов в имени поля – не более 100;
- количество символов в значении поля – не более 1024.

Добавлять, изменять и удалять пользовательские поля могут только пользователи с ролью Администратор.

Чтобы добавить, изменить или удалить пользовательское поле:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Активы** на вкладке **Устройства** выберите нужное устройство.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для просмотра и изменения сведений об устройстве: **Параметры**, **Адресная информация** и **Пользовательские поля**.

4. Перейдите на вкладку **Пользовательские поля** и выполните одно из следующих действий:

   - Если вы хотите добавить пользовательское поле, нажмите на кнопку **Добавить пользовательское поле** и в открывшихся полях введите имя и значение для пользовательского поля.

   - Если вы хотите изменить пользовательское поле, введите новое имя и/или значение нужного пользовательского поля.

   - Если вы хотите удалить пользовательское поле, нажмите на значок ×, который расположен справа от имени пользовательского поля.

5. Нажмите на кнопку **Сохранить**.

Удаление пользователей устройств

При использовании функциональности контроля пользователей на устройствах программа может автоматически удалять неактуальные учетные записи из таблицы пользователей. Автоматически удаляются только те пользователи, сведения о которых ранее были получены от источников **Внешний источник** и **OVAL-сканирование**, но в новых поступивших данных от этих источников такие пользователи отсутствуют.

При необходимости вы можете вручную удалять неактуальные учетные записи из таблицы пользователей.

Удалять учетные записи пользователей устройств могут только пользователи с ролью Администратор.

Чтобы удалить учетные записи из таблицы пользователей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Активы** на вкладке **Пользователи** выберите учетные записи пользователей, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **OK**.

Удаление исполняемых файлов устройств

При использовании функциональности контроля запусков исполняемых файлов на устройствах программа может автоматически удалять сведения о файлах из таблицы исполняемых файлов. Автоматическое удаление происходит при достижении ограничений по количеству или времени хранения файлов.

При необходимости вы можете вручную удалять неактуальные файлы из таблицы исполняемых файлов.

Удалять исполняемые файлы устройств могут только пользователи с ролью Администратор.

Чтобы удалить файлы из таблицы исполняемых файлов:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Активы** на вкладке **Исполняемые файлы** выберите файлы, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
4. В окне запроса нажмите на кнопку **Удалить**.

Настройка адресных пространств

Kaspersky Industrial CyberSecurity for Networks контролирует устройства и их взаимодействия с учетом адресных пространств (далее также "АП"). *Адресные пространства* предназначены для распределения адресов устройств на множества по какому-либо признаку (например, по принадлежности устройств сегментам сети).

Для описания адресных пространств в программе используются списки правил и подсетей.

Правило адресного пространства – это набор параметров, определяющих условия принадлежности адресов адресному пространству. Для связывания с адресным пространством каждый MAC- или IP-адрес должен удовлетворять хотя бы одному правилу адресного пространства. При этом программа связывает адрес с тем адресным пространством, правило которого наименее обобщенно определяет условия для принадлежности этого адреса (например, если адрес явно указан в правиле).

Подсети адресного пространства используются для проверки IP-адресов, обнаруженных программой. В зависимости от типа подсети, которой принадлежит обнаруженный IP-адрес, программа может выполнять различные действия для контроля активов и контроля взаимодействий устройств.

Вы можете настраивать адресные пространства в разделе **Активы** на вкладке **Адресные пространства**. Каждое адресное пространство представлено в виде блока со сведениями об адресном пространстве. Блок состоит из заголовка и вложенных блоков с таблицами правил и подсетей. При просмотре сведений об адресных пространствах вы можете разворачивать и сворачивать содержимое блоков.

Адресное пространство **Default**

По умолчанию в программе задано одно общее адресное пространство с именем **Default**. Это адресное пространство содержит единственное правило, параметры которого настроены на связывание любых MAC- и IP-адресов с этим адресным пространством. Список подсетей адресного пространства **Default** по умолчанию содержит стандартный набор подсетей, наиболее часто используемых на предприятиях.

Вы не можете изменить правило адресного пространства **Default** и добавлять другие правила в это адресное пространство. При этом пользователи с ролью Администратор могут изменять список подсетей в этом адресном пространстве, чтобы сформировать набор подсетей с учетом особенностей IP-адресации устройств в сети вашего предприятия. Если в Kaspersky Industrial CyberSecurity for Networks поступают данные от EPP-приложений, по этим данным программа может автоматически добавлять подсети в список подсетей.

Дополнительные адресные пространства

При необходимости вы можете настроить в программе несколько адресных пространств в дополнение к адресному пространству **Default**. Для добавленных адресных пространств доступны возможности формирования произвольных правил и наборов подсетей. Адреса, удовлетворяющие условиям добавленных адресных пространств, будут связаны с этими адресными пространствами. Остальные адреса останутся связанными с адресным пространством **Default**.

Необходимость в добавлении адресных пространств может возникнуть, например, при использовании устройств с одинаковыми адресами в разных сегментах сети. В этом случае после добавления и настройки адресных пространств программа сможет различать адресную информацию по дополнительным атрибутам, которые программа добавляет к адресам в виде имен адресных пространств.

Примеры использования адресных пространств см. в Приложении.

Связи адресов и адресных пространств

При использовании нескольких адресных пространств программа добавляет атрибуты с именами адресных пространств ко всем адресам, которые указываются в объектах программы: в устройствах, рисках, правилах, событиях и прочих объектах. Атрибуты с именами адресных пространств перестают отображаться для адресов, если в программе удалены все добавленные адресные пространства (атрибуты адресных пространств остаются только для адресов в событиях и в некоторых рисках, связанных с устройствами).

Атрибуты с именами адресных пространств обозначают связи адресов и адресных пространств. За счет связей с адресными пространствами адреса становятся зависимыми от этих адресных пространств.

Установленные связи адресов и адресных пространств приводят к следующим особенностям при удалении адресного пространства: программа автоматически удаляет все адреса, связанные с удаляемым адресным пространством. Такие адреса удаляются из всех объектов программы, за исключением событий. При удалении адреса из объекта программа проверяет наличие остающихся других адресов в этом объекте, и если других адресов не остается, программа удаляет и сам объект (например, устройство).

О правилах адресных пространств

Правила адресных пространств отображаются в блоках **Правила** внутри описаний адресных пространств. Информация о правилах отображается в строке заголовка адресного пространства и в таблице правил.

Параметры правил адресных пространств отображаются в следующих столбцах таблицы:

- **Источник**.

  Тип источника поступления данных об адресной информации и список выбранных источников данных. Предусмотрены следующие типы источников данных:

  - **Точки мониторинга** – выбранные для правила точки мониторинга.
  - **Серверы интеграции** – выбранные для правила серверы интеграции (данные об адресной информации, поступившие от выбранных серверов интеграции, будут удовлетворять правилу адресного пространства).
  - **Модули активного опроса** – выбранные для правила коннекторы модулей активного опроса (данные об адресной информации, поступившие от выбранных модулей активного опроса, будут удовлетворять правилу адресного пространства).

  Конкретные источники данных требуется указывать в правилах адресных пространств после добавления в программу объектов, которые будут являться источниками. Например, коннекторы для источника данных **Модули активного опроса** нужно указывать после добавления коннекторов типа **Active poll**.

- **Уровни модели OSI**.

  Выбранные уровни сетевой модели стека сетевых протоколов OSI (Open Systems Interconnection) для правила адресного пространства. Правило можно настроить на адреса следующих уровней модели OSI:

  - **Канальный (L2)** – к этому уровню относятся MAC-адреса.
  - **Сетевой (L3)** – к этому уровню относятся IP-адреса.
  - **Канальный и сетевой (L2 и L3)** – к этому уровню относятся и MAC-, и IP-адреса.

- **VLAN ID**.

  Идентификаторы виртуальных локальных сетей (VLAN), применяемые при использовании технологии VLAN в соответствии со стандартом IEEE 802.1q. Для правила адресного пространства параметр **VLAN ID** может принимать следующие значения:

  - **Используются любые** – для сетевых взаимодействий между устройствами используется технология VLAN, при этом идентификаторы VLAN могут быть любыми.
  - **Не используются** – для сетевых взаимодействий между устройствами не используется технология VLAN.
  - **Любые или не используются** – для сетевых взаимодействий между устройствами технология VLAN либо не используется, либо используется с применением любых идентификаторов VLAN.
  - **Фиксированные значения** со списком идентификаторов VLAN – для сетевых взаимодействий между устройствами используется технология VLAN, при этом к адресному пространству относится только такая адресная информация, в которой указан один из перечисленных идентификаторов VLAN.

- **IP-адреса**.

  IP-адреса, входящие в адресное пространство. Адреса могут быть указаны по отдельности, в виде диапазонов или в формате CIDR-адреса подсети.

При просмотре таблицы правил вы можете использовать функции настройки (по значку ⚙), а также поиска.

О подсетях адресных пространств

Подсети адресных пространств отображаются в блоках **Подсети** внутри описаний адресных пространств.

Программа проверяет обнаруженные IP-адреса по спискам подсетей адресных пространств и в зависимости от принадлежности IP-адресов определенным типам подсетей может выполнять следующие действия:

- добавлять устройство с обнаруженным IP-адресом в таблицу устройств и контролировать активность этого устройства;
- отображать устройство с обнаруженным IP-адресом на карте сетевых взаимодействий и топологической карте в виде узла соответствующего типа (известное программе устройство, неизвестное или узел WAN);
- отображать соединение на карте сетевых взаимодействий, в котором одной из сторон взаимодействия является устройство с обнаруженным IP-адресом;
- проверять взаимодействия устройства с обнаруженным IP-адресом по заданным правилам (правила контроля взаимодействий, правила обнаружения вторжений и правила корреляции);
- игнорировать активность устройства с обнаруженным IP-адресом.

Параметры подсетей адресных пространств отображаются в следующих столбцах таблицы:

- **Подсеть**.

  Адрес подсети в формате записи по методу бесклассовой адресации (Classless Inter-Domain Routing, CIDR): `<базовый адрес подсети>/<количество бит в маске>`. Адреса подсетей отображаются в виде дерева, которое показывает иерархию вложенности подсетей.

- **Тип**.

  Тип подсети, определяющий ее назначение. Предусмотрены следующие типы:

  - **Частная, IT** – подсеть для устройств, относящихся к ресурсам информационных технологий (IT), например файловых серверов.
  - **Частная, OT** – подсеть для устройств, относящихся к операционным технологиям (OT), например ПЛК.
  - **Частная, DMZ** – подсеть для устройств, находящихся в сегменте сети демилитаризованной зоны (DMZ), например серверов для запросов из внешних сетей.
  - **Публичная** – подсеть, которая считается внешней (глобальной) сетью для устройств в подсетях других типов. IP-адреса из этой подсети представлены на карте сетевых взаимодействий узлом WAN.
  - **Link-local** – подсеть для сетевых взаимодействий в пределах одного сегмента локальной сети (немаршрутизируемая).

- **Диапазон**.

  Диапазон IP-адресов, входящих в подсеть.

- **Игнорировать MAC-адреса**.

  Признак включенного или выключенного режима пропуска обнаруженных MAC-адресов при создании разрешающих правил для сетевых взаимодействий с участием IP-адресов из подсети. Если режим включен, то MAC-адреса, обнаруженные вместе с IP-адресами из подсети, не будут добавляться в правила по технологии Контроль целостности сети в режиме обучения.

- **Автоматически добавлять подсети**.

  Признак включенного или выключенного режима автоматического добавления вложенных подсетей по данным от EPP-приложений. Если режим включен, программа добавляет вложенные подсети на основании данных, полученных от EPP-приложений.

При просмотре таблицы подсетей вы можете использовать функции настройки (по значку ⚙), а также фильтрации, поиска и сортировки.

Добавление адресного пространства

Вы можете добавлять в программу адресные пространства, если требуется распределять адреса устройств на множества по какому-либо признаку (например, по принадлежности устройств сегментам сети).

Максимальное количество адресных пространств в программе – 100.

Добавлять адресные пространства могут только пользователи с ролью Администратор.

Чтобы добавить адресное пространство:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** откройте область деталей по кнопке **Добавить АП**.
4. Введите имя адресного пространства.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя адресного пространства должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 255 символов;
   - не совпадает с именем другого адресного пространства (регистр символов не учитывается).

   > Рекомендуется задавать имя адресного пространства длиной не более 6-8 символов. Если имя содержит большое количество символов, адресная информация может не полностью отображаться в ячейках некоторых таблиц данных (например, в таблице устройств).

5. При необходимости введите текстовое описание адресного пространства.
6. Настройте параметры первого правила адресного пространства.
7. При необходимости добавьте и настройте дополнительные правила адресного пространства по кнопке **Добавить правило**.

   Общее количество правил в адресном пространстве не может превышать 10.

8. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

В нижней части вкладки **Адресные пространства** появится отдельный блок со сведениями о добавленном адресном пространстве.

Формирование списка подсетей для контроля активов

Этот раздел содержит информацию о функциях, доступных для формирования списка подсетей для контроля активов.

Для адресных пространств вы можете формировать списки подсетей с учетом особенностей адресации устройств в сети вашего предприятия. Этот раздел содержит инструкции по использованию функций для формирования списка подсетей.

Если в Kaspersky Industrial CyberSecurity for Networks поступают данные от EPP-приложений, программа может использовать эти данные для автоматического добавления подсетей в соответствующих адресных пространствах. Программа автоматически добавляет обнаруженные подсети, если они являются вложенными в подсети, для которых включен режим автоматического добавления подсетей.

Формировать список подсетей могут только пользователи с ролью Администратор.

Добавление подсети

Чтобы добавить подсеть:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** раскройте блок со сведениями об адресном пространстве, в которое вы хотите добавить подсеть.
4. В заголовке блока **Подсети** нажмите на значок +.

   В правой части окна веб-интерфейса появится область деталей.
5. В поле **Подсеть** введите адрес подсети в формате CIDR: `<базовый адрес подсети>/<количество бит в маске>`.
6. В раскрывающемся списке **Тип** выберите тип подсети в соответствии с ее назначением.
7. Установите в нужные положения следующие переключатели:

   - **Игнорировать MAC-адреса для правил NIC** – включает и выключает режим пропуска обнаруженных MAC-адресов при создании разрешающих правил по технологии Контроль целостности сети.

     Если режим включен, то MAC-адреса, обнаруженные вместе с IP-адресами из подсети, не будут добавляться в правила по технологии Контроль целостности сети в режиме обучения.

   - **Автоматически добавлять подсети** – включает и выключает автоматическое добавление вложенных подсетей по данным от EPP-приложений.

     Если режим включен, программа добавляет в этой подсети вложенные подсети на основании данных, полученных от EPP-приложений. Для этих вложенных подсетей по умолчанию указывается тип, выбранный для текущей подсети.
8. Нажмите на кнопку **Сохранить**.

В списке подсетей появится новая подсеть на соответствующем уровне иерархии в дереве.

Изменение параметров подсети

Чтобы изменить параметры подсети:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Активы**.

3. На вкладке **Адресные пространства** раскройте блок со сведениями об адресном пространстве, в котором вы хотите изменить параметры подсети.

4. Раскройте блок **Подсети** и выберите нужную подсеть.

   В правой части окна веб-интерфейса появится область деталей.

5. Нажмите на кнопку **Изменить**.

6. Выполните следующие действия (в зависимости от нужного результата):

   - В поле **Подсеть** введите адрес подсети в формате CIDR: `<базовый адрес подсети>/<количество бит в маске>`.

     Адрес корневой подсети недоступен для изменения.

   - В раскрывающемся списке **Тип** выберите тип подсети в соответствии с ее назначением.

     При изменении типа подсети учитывайте, что новый тип подсети может повлиять на выполняемые программой действия с IP-адресами из этой подсети. Например, при выборе типа **Публичная** на карте сетевых взаимодействий перестанут отображаться соединения с устройствами, у которых заданы IP-адреса из этой подсети.

   - Установите в нужные положения следующие переключатели:

     - **Игнорировать MAC-адреса для правил NIC** – включает и выключает режим пропуска обнаруженных MAC-адресов при создании разрешающих правил по технологии Контроль целостности сети.

       Если режим включен, то MAC-адреса, обнаруженные вместе с IP-адресами из подсети, не будут добавляться в правила по технологии Контроль целостности сети в режиме обучения.

     - **Автоматически добавлять подсети** – включает и выключает автоматическое добавление вложенных подсетей по данным от EPP-приложений.

       Если режим включен, программа добавляет в этой подсети вложенные подсети на основании данных, полученных от EPP-приложений. Для этих вложенных подсетей по умолчанию указывается тип, выбранный для текущей подсети

7. Нажмите на кнопку **Сохранить**.

Если изменен параметр **Подсеть**, для подсети может измениться уровень иерархии в дереве.

Удаление подсетей

В списке подсетей адресного пространства вы можете удалить любую подсеть, кроме корневой подсети в дереве (подсеть 0.0.0.0/0).

Чтобы удалить подсети:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** раскройте блок со сведениями об адресном пространстве, в котором вы хотите удалить подсети.
4. Раскройте блок **Подсети** и выберите подсети для удаления.

   В правой части окна веб-интерфейса появится область деталей.
5. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
6. В окне запроса подтвердите удаление подсетей.

Удаленные подсети перестанут отображаться в списке подсетей. Если удаленная подсеть содержала вложенные подсети, эти подсети останутся в списке (при этом изменится уровень иерархии этих подсетей в дереве).

Просмотр сведений об устройствах с IP-адресами из выбранных подсетей

Вы можете просмотреть сведения об устройствах, у которых заданы IP-адреса из выбранных подсетей в адресном пространстве. Сведения об устройствах выводятся в таблице устройств. В таблице устройств автоматически применяется фильтрация по адресам подсетей.

Чтобы просмотреть сведения об устройствах в таблице устройств:

1. Выберите раздел **Активы**.
2. На вкладке **Адресные пространства** раскройте блок со сведениями об адресном пространстве с нужными подсетями.
3. Раскройте блок **Подсети** и выберите подсети, для которых вы хотите просмотреть сведения об устройствах.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Показать устройства**.

Откроется вкладка **Устройства** в разделе **Активы**. В таблице устройств будет применена фильтрация по IP-адресам в адресной информации устройств.

Изменение адресного пространства

Для добавленных адресных пространств вы можете изменять имена, текстовые описания и параметры правил адресных пространств. Для адресного пространства **Default** такие изменения недоступны.

Также вы можете формировать списки подсетей для любых адресных пространств (включая список подсетей адресного пространства **Default**).

При изменении параметров правила адресного пространства требуется учитывать установленные связи этого адресного пространства и адресов, которые указаны в объектах программы: в устройствах, рисках, правилах, событиях и прочих объектах. Если в результате изменения параметров в правилах адресного пространства удаляются связи этого адресного пространства и адресов, программа автоматически удаляет такие адреса. Это может привести и к удалению самих объектов программы (например, устройств), если у этих объектов не остается других адресов.

Изменять имена, текстовые описания и параметры правил адресных пространств могут только пользователи с ролью Администратор.

Чтобы изменить имя, текстовое описание или параметры правил адресного пространства:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Активы**.

3. На вкладке **Адресные пространства** нажмите на значок в блоке со сведениями о нужном адресном пространстве.

   В правой части окна веб-интерфейса появится область деталей.

4. Выполните следующие действия (в зависимости от нужного результата):

   - Введите имя адресного пространства.

     Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

     Имя адресного пространства должно удовлетворять следующим требованиям:

     - начинается и заканчивается любым символом, кроме пробела;
     - содержит до 255 символов;
     - не совпадает с именем другого адресного пространства (регистр символов не учитывается).

     Рекомендуется задавать имя адресного пространства длиной не более 6-8 символов. Если имя содержит большое количество символов, адресная информация может не полностью отображаться в ячейках некоторых таблиц данных (например, в таблице устройств).

   - Введите описание адресного пространства.
   - Настройте параметры правил адресного пространства.
   - При необходимости добавьте и настройте дополнительные правила адресного пространства по кнопке **Добавить правило** или удалите ненужные правила с помощью значков ×.

     Общее количество правил в адресном пространстве не может превышать 10.

5. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

6. В окне запроса подтвердите изменение параметров адресного пространства.

Удаление адресного пространства

Вы можете удалять добавленные адресные пространства. Для адресного пространства **Default** возможность удаления недоступна.

При удалении адресного пространства требуется учитывать установленные связи этого адресного пространства и адресов, которые указаны в объектах программы: в устройствах, рисках, правилах, событиях и прочих объектах. Если в результате удаления адресного пространства удаляются связи этого адресного пространства и адресов, программа автоматически удаляет такие адреса. Это может привести и к удалению самих объектов программы (например, устройств), если у этих объектов не остается других адресов.

Удалять адресные пространства могут только пользователи с ролью Администратор.

Чтобы удалить адресное пространство:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Адресные пространства** нажмите на значок в блоке со сведениями об адресном пространстве, которое вы хотите удалить.

   Откроется окно с запросом подтверждения.
4. В окне запроса подтвердите удаление адресного пространства.

Настройка контроля процесса

Kaspersky Industrial CyberSecurity for Networks может контролировать технологический процесс, отслеживая параметры технологического процесса и системные команды, передаваемые в трафике промышленной сети. Программа отслеживает эти данные для устройств, представленных в таблице устройств и имеющих заданные параметры контроля процесса.

Параметры контроля процесса можно настроить для типов устройств и протоколов, поддерживаемых программой.

Для контроля технологического процесса в автоматическом режиме вы можете использовать правила контроля процесса и функциональность отслеживания системных команд. Также вы можете отслеживать параметры технологического процесса в онлайн-режиме.

Правило контроля процесса – это набор параметров, определяющих условие для значений тега. В правилах контроля процесса описываются ситуации, которые необходимо обнаруживать в трафике промышленной сети (например, превышение тегом указанного значения).

При выполнении условия, заданного в правиле, Kaspersky Industrial CyberSecurity for Networks регистрирует событие. Вы можете задать нужные параметры регистрации событий (например, заголовки событий) при настройке правил контроля процесса.

Отслеживание системных команд обеспечивает регистрацию событий обнаружения в трафике переданных системных команд. При настройке параметров контроля процесса для устройств вы можете выбрать нужные системные команды для отслеживания. Эта функциональность может использоваться независимо от правил контроля процесса.

Настраивать параметры контроля процесса для устройств, а также формировать списки контролируемых тегов и правил контроля процесса могут только пользователи с ролью Администратор. При этом возможности просмотра и экспорта данных доступны как пользователям с ролью Администратор, так и пользователям с ролью Оператор.

Вы можете формировать списки контролируемых тегов и правил контроля процесса на странице веб-интерфейса Сервера в разделе **Контроль процесса**. Параметры контроля процесса для устройств вы можете настраивать при работе с устройствами в разделах **Активы** и **Карта сети**.

Поддерживаемые устройства и протоколы

Kaspersky Industrial CyberSecurity for Networks анализирует трафик следующих типов устройств, используемых для автоматизации технологического процесса:

- Программируемые логические контроллеры (далее "ПЛК"):
  - ABB™ AC 700F, 800M;
  - ABB B&R;
  - Allen-Bradley® серий ControlLogix®, CompactLogix™;
  - AutomationDirect DirectLOGIC;
  - BECKHOFF® серий CX;
  - Emerson DeltaV серии M, серии S;
  - Emerson серии ControlWave;
  - General Electric RX3i;
  - Honeywell C300 для систем управления Experion PKS / PlantCruise;
  - Honeywell ControlEDGE серии 900;
  - IPU950;
  - Mitsubishi System Q E71;
  - OMRON серии CJ2M;
  - Schneider Electric Foxboro FCP270, FCP280;
  - Schneider Electric серии Modicon: M580, M340, Momentum;
  - Siemens SIMATIC® серий S7-200, S7-300, S7-400, S7-1200, S7-1500;
  - YCU и ELC, поддерживающие протокол YARD;
  - Yokogawa CENTUM;
  - Yokogawa ProSafe-RS;
  - ОВЕН серий ПЛК100;
  - Прософт-Системы Regul R500;
  - устройства KNX®;
  - устройства в системах управления Valmet DNA;

- устройства, поддерживающие протокол Allen-Bradley EtherNet/IP;
- устройства, поддерживающие протокол COS;
- устройства, поддерживающие протокол DTS;
- устройства, поддерживающие протокол FEU;
- устройства, поддерживающие протокол ВНИИА;
- устройства, поддерживающие протокол ПК4;
- устройства, поддерживающие протокол ПНУ20;
- устройства, поддерживающие протоколы CODESYS V2, V3;
- устройства, поддерживающие протоколы Siemens S7comm, S7comm-plus;
- устройства, поддерживающие протоколы стандарта PROFINET IO.

- Интеллектуальные электронные устройства (далее IED):
  - ABB серии Relion™: REF615, RED670, REL670, RET670;
  - General Electric серии Multilin: B30, C60;
  - MiCOM C264;
  - Schneider Electric P545;
  - Schneider Electric Sepam серии 80 NPP;
  - Siemens серии SIPROTEC™ 4: 6MD66, 7SA52, 7SJ64, 7SS52, 7UM62, 7UT63;
  - Релематика ТОР 300;
  - ЭКРА серий 200, БЭ2502, БЭ2704;
  - устройства, поддерживающие протокол DNP3;
  - устройства, поддерживающие протокол Schneider Electric UMAS;
  - устройства, поддерживающие протоколы стандарта IEC 60870: IEC 60870-5-101, IEC 60870-5-104;
  - устройства, поддерживающие протоколы стандарта IEC 61850: IEC 61850-8-1 (GOOSE, MMS), IEC 61850-9-2 (Sampled Values);
  - устройства, поддерживающие протокол Modbus TCP.

- Устройства с установленным серверным ПО:
  - FTP-сервер;
  - сервер OPC DA;
  - сервер OPC UA;
  - сервер Siemens SICAM PAS;
  - сервер TASE.2;
  - сервер с поддержкой шифрования;
  - устройства SCADA-системы АСРК.
- Устройства, относящиеся к сетевому оборудованию:
  - Moxa серии NPort;
  - устройства ввода-вывода, поддерживающие протоколы BACnet™, FTP, IEC 60870-5-101, IEC 60870-5-104, Modbus TCP, OPC DA, протокол взаимодействия устройств по технологии WMI, OPC UA Binary;
  - устройства, поддерживающие серверные команды управления по протоколу Telnet.

Дополнительно в Kaspersky Industrial CyberSecurity for Networks предусмотрены *универсальные типы* устройств для контроля процесса: **Универсальный ПЛК**, **Универсальное устройство IED** и **Универсальный шлюз**. Используя эти типы устройств, вы можете настроить в Kaspersky Industrial CyberSecurity for Networks анализ трафика для тех устройств, которые не входят в список поддерживаемых типов. Для универсальных типов устройств можно указывать любые сочетания протоколов прикладного уровня из числа поддерживаемых протоколов на устройствах, относящихся к программируемым логическим контроллерам, интеллектуальным электронным устройствам и сетевым шлюзам.

Для поддерживаемых типов устройств Kaspersky Industrial CyberSecurity for Networks анализирует взаимодействия по следующим протоколам прикладного уровня:

- ABB™ SPA-Bus;
- Allen-Bradley EtherNet/IP;
- BECKHOFF® ADS/AMS;
- BSAP;
- CODESYS V2, V3 Gateway поверх TCP и V3 Gateway поверх UDP;
- COS;
- DHCP;
- DMS для устройств ABB AC 700F;
- DNP3;
- Emerson ControlWave Designer;

- Emerson DeltaV, включая протокол обновления встроенного ПО (прошивок);
- FTP;
- General Electric EGD;
- General Electric SRTP;
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104;
- IEC 61850: GOOSE, MMS (включая MMS Reports), Sampled Values;
- INA2000;
- KNXnet/IP;
- Mitsubishi MELSEC System Q;
- MMS (ISO 9506-2);
- Modbus TCP;
- OMRON FINS;
- OPC DA, протокол взаимодействия устройств по технологии WMI;
- OPC UA Binary;
- PROFINET IO и RPC для PROFINET IO;
- Schneider Electric UMAS;
- Siemens Industrial Ethernet;
- Siemens S7comm, S7comm-plus;
- TASE.2;
- YARD;
- Yokogawa Vnet/IP;
- ВНИИА;
- Релематика BDUBus;
- ПК4;
- ПНУ20;
- модификация протокола Modbus TCP для устройств ЭКРА серии 200;
- протокол автоматизированных систем радиационного контроля (АСРК);
- протокол взаимодействия систем Siemens SICAM PAS и SICAM SCC (на базе SIMATIC WinCC®);

- протокол взаимодействия устройств AutomationDirect DirectLOGIC;
- протокол взаимодействия устройств Foxboro FCP270, FCP280;
- протокол взаимодействия устройств IPU-FEU;
- протокол взаимодействия устройств MiCOM C264;
- протокол взаимодействия устройств Valmet DNA;
- протокол начальной настройки устройств Прософт-Системы;
- протокол передачи данных DTS;
- протокол устройств с системным ПО Siemens DIGSI 4;
- протоколы взаимодействия устройств в системах управления Honeywell Experion PKS / PlantCruise;
- протоколы начальной настройки и взаимодействия устройств Moxa серии NPort;
- протоколы обнаружения и взаимодействия устройств Honeywell ControlEDGE серии 900.

Для анализа трафика и взаимодействий устройств программа использует модули обработки протоколов прикладного уровня. Модули, входящие в состав пакетов из комплекта поставки Kaspersky Industrial CyberSecurity for Networks, обеспечивают поддержку перечисленных типов устройств и протоколов прикладного уровня. Вы можете обновлять модули обработки протоколов, устанавливая обновления. При установке обновлений в программу могут быть добавлены новые модули, обеспечивающие поддержку дополнительных типов устройств и/или протоколов прикладного уровня.

Kaspersky Industrial CyberSecurity for Networks также анализирует трафик по протоколам общего применения. Список поддерживаемых протоколов общего применения см. в Приложении.

Устройства для контроля процесса

Для контроля технологического процесса вы можете использовать устройства из таблицы устройств, у которых заданы параметры контроля процесса.

В Kaspersky Industrial CyberSecurity for Networks для контроля процесса поддерживаются различные типы устройств и протоколы прикладного уровня.

Вы можете просматривать и изменять параметры контроля процесса в области деталей устройства, выбранного в разделе **Активы** или **Карта сети** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Параметры контроля процесса для устройств

Параметры контроля процесса для устройств отображаются в области деталей при выборе устройства в таблице устройств, на карте сетевых взаимодействий и на топологической карте. Если для устройства заданы параметры контроля процесса, вкладка **Контроль процесса** в области деталей содержит следующие сведения:

- **Тип устройства** – тип устройства из числа поддерживаемых типов устройств для контроля процесса.
- **Протокол** – название используемого протокола. Для каждого протокола отображаются следующие сведения:
  - **Системные команды** – основные параметры отслеживания системных команд для протокола. В поле отображается общее количество системных команд для протокола и количество отслеживаемых системных команд, при обнаружении которых программа регистрирует события.
  - Адресная информация – в зависимости от выбранного протокола содержит IP-адрес и порт, MAC-адрес или идентификатор домена (для протокола IEC 61850: GOOSE). Если в программу добавлены дополнительные адресные пространства, для адреса должно быть указано АП, к которому относится этот адрес (при этом уровни модели OSI, выбранные для правил адресного пространства, должны соответствовать адресу).
  - Дополнительные параметры в зависимости от выбранного протокола. Дополнительные параметры отображаются, если для протокола можно настроить не только системные команды и адресную информацию.

    Примеры:

    При выборе протокола Modbus TCP отображается дополнительный параметр **Обратный порядок регистров**. Параметр позволяет включить или выключить поддержку обратной последовательности регистров (машинных слов) в 32-разрядных значениях данных.

    При выборе протокола IEC 60870-5-101 отображаются следующие дополнительные параметры:

    - **Адрес ASDU два байта** – позволяет включить или выключить режим двухбайтовой адресации для блоков данных прикладного уровня (Application Service Data Unit, ASDU). Если режим выключен, используется однобайтовая адресация.
    - **Инициатор** – позволяет включить или выключить использование дополнительного байта для адреса инициатора в идентификаторе блока данных.
    - **Блок адреса канала (байт)** – количество байт в блоке адреса канального уровня.
    - **Блок адреса объекта (байт)** – количество байт в блоке адреса объекта информации.

Вы можете добавлять параметры контроля процесса для устройств следующими способами:

- автоматически;
- вручную;
- путем импорта из внешних проектов.

Об автоматическом определении параметров контроля процесса для устройств

Kaspersky Industrial CyberSecurity for Networks может автоматически определять параметры контроля процесса для устройств и сохранять эти параметры в сведениях об устройствах. Определение параметров выполняется путем анализа обнаруженных в трафике протокольных команд для устройств, участвующих в технологическом процессе.

Программа автоматически добавляет или изменяет параметры контроля процесса для устройств, которые добавлены в таблицу устройств. Добавление устройств в таблицу также может происходить автоматически, если для контроля активов включен метод обнаружения активности устройств.

Автоматически добавленные параметры контроля процесса считаются *системными*. Программа может изменять эти параметры, если в трафике обнаружены протокольные команды с обновленной информацией о параметрах.

Параметры контроля процесса, добавленные пользователем вручную, считаются *пользовательскими*. Программа не изменяет пользовательские параметры контроля процесса. Если пользователь вручную изменит системные параметры контроля процесса, эти параметры также становятся пользовательскими.

Автоматическое определение параметров контроля процесса для устройств выполняется при использовании метода обнаружения устройств для контроля процесса по технологии Контроль технологического процесса. Вы можете включать и выключать применение метода.

Для автоматического определения параметров контроля процесса в программе используются модули обработки протоколов прикладного уровня. После установки программы используются исходные модули, обеспечивающие определение основных параметров для ряда устройств и протоколов из числа поддерживаемых типов устройств и протоколов. Вы можете обновлять модули обработки протоколов, устанавливая обновления.

Добавление параметров контроля процесса для устройства вручную

Вы можете вручную добавить параметры контроля процесса для устройства при работе с таблицей устройств, картой сетевых взаимодействий или с топологической картой. Добавленные параметры контроля процесса для устройства считаются пользовательскими. Пользовательские параметры не изменяются при автоматическом определении параметров контроля процесса для устройств.

Добавлять параметры контроля процесса могут только пользователи с ролью Администратор.

Чтобы добавить параметры контроля процесса для устройства:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети** выберите нужное устройство.

   В разделе **Карта сети** вы можете выбрать нужное устройство как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.

3. В правом верхнем углу области деталей нажмите на значок ⋮ и выберите пункт **Параметры контроля процесса → Добавить**.

   Появится окно **Добавление параметров контроля процесса**.

4. Настройте параметры контроля процесса:

   a. Выберите тип устройства.

   b. Выберите протокол, по которому осуществляется взаимодействие с устройством в рамках технологического процесса.

   c. При необходимости измените параметры отслеживания системных команд по выбранному протоколу. По умолчанию отслеживаются все системные команды, кроме тех, которые часто возникают при нормальной работе устройства.

   d. Если для выбранного протокола требуется настроить другие параметры (например, адресную информацию для взаимодействия с устройством), укажите нужные значения в появившихся полях.

   e. Если вы хотите дополнительно указать другой протокол (поддерживаемый для выбранного типа устройства) или другую комбинацию параметров для ранее выбранного протокола (в случае использования нескольких подключаемых модулей в составе одного устройства), добавьте параметры для этого протокола по ссылке **Добавить протокол**.

5. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

На вкладке **Контроль процесса** в области деталей появится отдельный блок с заданными параметрами.

Изменение параметров контроля процесса для устройства

Если для устройства добавлены параметры контроля процесса, вы можете вручную изменить эти параметры при работе с таблицей устройств, с картой сетевых взаимодействий или топологической картой. После сохранения изменений параметры контроля процесса для устройства считаются пользовательскими. Пользовательские параметры не изменяются при автоматическом определении параметров контроля процесса для устройств.

Изменять параметры контроля процесса могут только пользователи с ролью Администратор.

Чтобы изменить параметры контроля процесса для устройства:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети** выберите нужное устройство.

   В разделе **Карта сети** вы можете выбрать нужное устройство как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.

3. В правом верхнем углу области деталей нажмите на значок ⋮ и выберите пункт **Параметры контроля процесса → Изменить**.

   Появится окно **Изменение параметров контроля процесса**.

4. Настройте параметры контроля процесса. Вы можете изменить параметры по отдельности (например, изменить параметры отслеживания системных команд для протокола) или заново настроить все параметры в том же порядке, как при добавлении параметров контроля процесса.

   При изменении параметров, которые используются в ранее созданных тегах, программа автоматически удаляет эти теги и связанные с ними правила контроля процесса. Например, если вы удаляете протокол, то после сохранения параметров программа удалит все теги, в которых были указаны устройство и удаленный протокол (в том числе будут удалены и правила контроля процесса, связанные с этими тегами).

5. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

На вкладке **Контроль процесса** в области деталей обновятся сведения в блоке с заданными параметрами.

Выбор отслеживаемых системных команд

Вы можете настроить отслеживание в трафике системных команд, переданных и полученных устройствами для контроля процесса.

В Kaspersky Industrial CyberSecurity for Networks к системным командам относятся как команды управления (например, START PLC), так и системные сообщения, связанные с функционированием устройств или содержащие результаты анализа пакетов (например, REQUEST NOT FOUND). Для классификации системных команд в Kaspersky Industrial CyberSecurity for Networks предусмотрены категории, перечисленные в Приложении.

При обнаружении отслеживаемой системной команды Kaspersky Industrial CyberSecurity for Networks регистрирует событие по технологии Контроль системных команд. Для регистрации используется системный тип события, которому присвоен код 4000002602. Вы можете настроить параметры для этого типа события.

Настраивать отслеживание системных команд для устройств могут только пользователи с ролью Администратор.

Чтобы настроить отслеживание системных команд для устройства:

1. В разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети** выберите нужное устройство, для которого заданы параметры контроля процесса.

   В разделе **Карта сети** вы можете выбрать устройство как на карте сетевых взаимодействий, так и на топологической карте.

   Если параметры контроля процесса не заданы для устройства, добавьте параметры.

2. В правом верхнем углу области деталей нажмите на значок ⋮ и выберите пункт **Параметры контроля процесса → Изменить**.

   Появится окно **Изменение параметров контроля процесса**.

3. Для первого протокола укажите нужные системные команды. Для этого раскройте список **Системные команды** под полем **Протокол** и установите флажки у тех системных команд, которые вы хотите отслеживать. После выбора системных команд нажмите на кнопку **OK**.

4. Если в параметрах контроля процесса дополнительно указан другой протокол (или тот же протокол, но с другой адресной информацией), выберите системные команды, которые будут отслеживаться при взаимодействиях по этому протоколу. Для этого используйте раскрывающийся список **Системные команды** под полем с названием этого протокола. Аналогичным образом настройте отслеживание системных команд для всех остальных указанных протоколов устройства.

5. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

На вкладке **Контроль процесса** в области деталей обновятся сведения в блоке с заданными параметрами.

Очистка параметров контроля процесса, заданных для устройства

Вы можете очистить параметры контроля процесса, заданные для устройства, при работе с таблицей устройств, с картой сетевых взаимодействий или с топологической картой.

При очистке параметров контроля процесса, заданных для устройства, программа автоматически удаляет все теги, которые были созданы для этого устройства. Также вместе с тегами удаляются и связанные с ними правила контроля процесса.

Выполнять очистку параметров контроля процесса для устройств могут только пользователи с ролью Администратор.

Чтобы очистить параметры контроля процесса для устройства:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети** выберите нужное устройство.

   В разделе **Карта сети** вы можете выбрать нужное устройство как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.

3. В правом верхнем углу области деталей нажмите на значок ⋮ и выберите пункт **Параметры контроля процесса → Удалить**.

   Откроется окно с запросом подтверждения.

4. В окне запроса подтвердите удаление параметров.

Блок с параметрами контроля процесса будет удален с вкладки **Контроль процесса** в области деталей.

Импорт конфигураций устройств и тегов из внешних проектов

Вы можете импортировать в Kaspersky Industrial CyberSecurity for Networks конфигурации параметров контроля процесса для устройств (далее также "конфигурации устройств") и теги из файлов, представляющих внешние проекты. *Внешними проектами* для Kaspersky Industrial CyberSecurity for Networks считаются проекты с данными об устройствах и тегах, сохраненные средствами других систем (например, в системе SCADA).

Для импорта файлы внешних проектов должны быть упакованы в ZIP-архив (кроме файлов некоторых проектов, содержимое которых представляет собой ZIP-архив). Вы можете импортировать конфигурации устройств и тегов только из файлов поддерживаемых типов внешних проектов.

Вы можете обновлять и дополнять поддерживаемые типы проектов, устанавливая обновления.

Чтобы импортировать конфигурации устройств и тегов из внешнего проекта:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** в панели инструментов, которая расположена над таблицей устройств, откройте раскрывающийся список **Импорт**.
4. В раскрывающемся списке выберите пункт с нужным типом проекта.

   На экране появится окно **Импортируется <тип проекта>**.
5. В поле **Файл для импорта** укажите файл проекта с помощью кнопки **Обзор**.
6. Выберите нужный вариант действий с имеющимися конфигурациями устройств и тегами. Для этого нажмите на одну из следующих кнопок:

   - **Добавить** – импортируемые конфигурации устройств и теги будут добавлены к имеющимся конфигурациям устройств и тегам.
   - **Заменить** – при импорте удаляются имеющиеся конфигурации устройств и теги, связанные с теми устройствами, для которых импортируются новые конфигурации и теги (при этом не удаляются теги, для которых есть пользовательские правила контроля процесса).
7. Подтвердите импорт с помощью кнопки **Продолжить**.

   Запустится процесс импорта данных. Сведения о выполнении операции импорта отображаются в списке фоновых операций. По окончании процесса импортированные конфигурации устройств и теги будут доступны для загрузки в таблице устройств и в таблице тегов.
8. Если вы хотите просмотреть отчет о результатах импорта, выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции импорта.

   c. Нажмите на кнопку **Вывести отчет**.

Поддерживаемые типы проектов для импорта

Импорт конфигураций устройств и тегов поддерживается из файлов данных, представляющие следующие типы проектов:

- Проект универсального формата.

  Этот тип проекта может быть получен из любых источников путем преобразования и сохранения данных в текстовых файлах с разделителями в формате CSV. Сведения о составе файлов в проекте универсального формата см. в Приложении.

- Файл конфигурации AC 800M для сервера OPC.

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами ABB AC 800M.

- Проект Control Builder M.

  Этот тип проекта может быть получен с помощью программного обеспечения ABB Control Builder M.

- Архив с конфигурацией устройств COS.

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами, поддерживающими протокол COS.

  > Файлы конфигурации устройств не содержат сетевые IP-адреса, которые используются этими устройствами. Поэтому после добавления устройств из файлов конфигурации вам потребуется проверить сведения об устройствах в программе и при необходимости вручную задать правильные IP-адреса для этих устройств.

- Проект DeltaV.

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами Emerson DeltaV.

- Проект DirectSOFT6.

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами DirectLOGIC.

- Список тегов ABB Freelance 2016 Engineering.

  Этот тип проекта может быть получен с помощью программного обеспечения ABB Freelance 2016 Engineering.

- Проект для устройств IEC 61850.

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами, поддерживающими протоколы стандарта IEC 61850.

  > Для импорта поддерживаются типы файлов SCD, CID и ICD, подготовленные в соответствии со стандартом IEC 61850-6. Дополнительные сведения о возможностях программы в части обработки и контроля конфигураций, сохраненных в этих файлах, см. в Приложении.

- Проект RSLogix 5000® (представленный CSV- или ACD-файлом).

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами RSLogix 5000.

  > При импорте CSV-файла проекта RSLogix 5000 программа игнорирует структурные и пользовательские типы тегов в этом проекте. Если вы хотите добавить в программу такие теги, вы можете использовать для импорта ACD-файл проекта RSLogix 5000 или включить обнаружение неизвестных тегов, чтобы добавить теги из трафика.

- Проект SICAM PAS V7 (представленный TXT-файлом описания или PXD-файлом).

  Этот тип проекта может быть получен с помощью программного обеспечения Siemens SICAM PAS версии 7.

- Проект TIA Portal V12/V13.

  Этот тип проекта может быть получен с помощью программного обеспечения Siemens TIA Portal версий 12 или 13.

- Проект Schneider Electric Unity.

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами Schneider Electric серии Modicon. Проект может быть представлен ZEF- или XEF-файлами (при этом если проект представлен ZEF-файлом, то этот файл не нужно упаковывать в ZIP-архив для импорта).

  > При импорте проекта Schneider Electric Unity добавляемым устройствам назначаются имена файлов, из которых они были импортированы. Вы можете вручную задать нужные имена этим устройствам при изменении сведений об устройствах.

- Проект WinCC (в том числе WinCC OA, WinCC flexible).

  Этот тип проекта может быть получен с помощью программного обеспечения Siemens SIMATIC WinCC, WinCC OA, WinCC flexible.

- Файл конфигурации YARD.

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами, поддерживающими протокол YARD.

- CSV-файл экспорта CIMPLICITY.

  Этот тип проекта может быть получен с помощью программного обеспечения CIMPLICITY.

- Файл конфигурации Valmet DNA.

  Этот тип проекта может быть получен с помощью программного обеспечения Valmet DNA.

- XML-файл конфигурации EGD.

  Этот тип проекта может быть получен путем экспорта конфигурации для обмена данными по протоколу General Electric EGD.

- SIG-файл проекта ControlWave.

  Этот файл входит в состав проекта, который используют устройства Emerson серии ControlWave.

- Проект Honeywell Control Builder.

  Этот тип проекта может быть получен с помощью программного обеспечения Honeywell Control Builder.

- Проект PcVue V10/V11.

  Этот тип проекта может быть получен с помощью программного обеспечения PcVue версий 10 или 11.

- CSV-файл экспорта Proficy.

  Этот тип проекта может быть получен с помощью программного обеспечения Proficy.

- Проект с файлами экспорта Foxboro IACC.

  Этот тип проекта может быть получен с помощью программного обеспечения Foxboro IACC.

- Файл конфигурации ПНУ20.

  Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами, поддерживающими протокол ПНУ20.

- Файлы формата CSV.

  Этот тип проекта может быть получен из любых источников в виде файлов в формате CSV.

Теги

Тег – это параметр технологического процесса, передаваемый в промышленной сети (например, контролируемая температура). Значения тегов передаются и принимаются устройствами по определенным протоколам.

Вы можете добавлять теги в программу следующими способами:

- вручную;
- автоматически при обнаружении неизвестных тегов;
- при импорте из внешних проектов.

Добавление тега возможно при следующих условиях:

- В таблице устройств есть устройство, к которому относится добавляемый тег.
- Для устройства заданы параметры контроля процесса, в которых указан протокол добавляемого тега.

После добавления тега в программу этот тег может быть использован в правилах контроля процесса. В соответствии с условиями, заданными в правилах контроля процесса, программа будет регистрировать соответствующие события, в которых могут сохраняться полученные значения тега.

Для контроля значений тега при мониторинге параметров технологического процесса не требуется добавлять этот тег в правила контроля процесса.

Вы можете просматривать и изменять теги в разделе **Контроль процесса** на вкладке **Теги**.

Об обнаружении неизвестных тегов

Kaspersky Industrial CyberSecurity for Networks может анализировать трафик для обнаружения и сохранения информации о неизвестных тегах. Неизвестными считаются теги, отсутствующие в таблице тегов.

Программа добавляет обнаруженный тег в таблицу тегов, если выполнены условия для добавления тега. Если не выполнено одно из условий, обнаруженный тег игнорируется (например, если в параметрах контроля процесса для устройства не указан протокол, к которому относится тег).

Получение из трафика информации о неизвестных тегах выполняется с помощью метода обнаружения неизвестных тегов по технологии Контроль технологического процесса. Вы можете включать и выключать применение метода.

При использовании метода обнаружения неизвестных тегов возможно некоторое снижение производительности модулей обработки протоколов прикладного уровня. Поэтому по умолчанию после установки программы обнаружение неизвестных тегов выключено. Рекомендуется включать метод обнаружения неизвестных тегов на время, достаточное для обнаружения всех тегов, которые могут относиться к устройствам с заданными параметрами контроля процесса. После добавления обнаруженных тегов в таблицу рекомендуется выключить этот метод.

Обнаружение неизвестных тегов поддерживается для следующих протоколов:

- Allen-Bradley EtherNet/IP;
- BACnet;
- BSAP;
- CODESYS V3 Gateway;
- DMS для устройств ABB AC 700F;
- DNP3;
- Emerson DeltaV;
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104;
- Modbus TCP;
- OPC DA;
- OPC UA Binary;
- Schneider Electric UMAS;
- Siemens S7comm;
- TASE.2;
- Yokogawa Vnet/IP;

- ПНУ20;
- протокол взаимодействия устройств Foxboro FCP270, FCP280.

Добавление тега вручную

Добавлять теги вручную могут только пользователи с ролью Администратор.

Чтобы вручную добавить новый тег:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На вкладке **Теги** откройте область деталей по кнопке **Добавить тег**.
4. Откройте окно выбора устройств по ссылке **Выбрать устройство**.
5. В окне выбора устройств выберите устройство, для которого вы хотите создать тег, и нажмите на кнопку **ОК**.

   Окно выбора устройств содержит таблицу, в которой можно настраивать отображение и порядок столбцов, выполнять фильтрацию, поиск и сортировку аналогично таблице устройств в разделе **Активы**.
6. Выберите протокол, который указан в параметрах контроля процесса для выбранного устройства. Требуется выбрать протокол, в котором поддерживается передача тегов.

   Если нужный протокол отсутствует, вы можете настроить параметры контроля процесса и указать нужный протокол. Для открытия окна настройки используйте кнопку справа от поля для выбора протокола. Настройка параметров контроля процесса выполняется аналогично, как при добавлении или изменении параметров при работе в таблице устройств.
7. При необходимости измените имя тега. По умолчанию задано имя по шаблону: **Tag <значение счетчика тегов устройства>**.

   Вы можете использовать буквы латинского алфавита, цифры, пробел, а также следующие специальные символы: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. Имя тега должно начинаться и заканчиваться любым допустимым символом, кроме пробела.
8. Настройте другие параметры тега.

   Для тега должны быть указаны обязательные параметры (например, имя тега, тип данных). Также в зависимости от выбранного протокола и типа данных для настройки могут быть доступны дополнительные параметры (например, единица измерения, пределы масштабирования).
9. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

В таблице тегов появится новый тег.

Изменение параметров тега

Изменять параметры тегов могут только пользователи с ролью Администратор.

Чтобы изменить параметры тега:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На вкладке **Теги** выберите нужный тег.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. При необходимости измените имя тега.

   Вы можете использовать буквы латинского алфавита, цифры, пробел, а также следующие специальные символы: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. Имя тега должно начинаться и заканчиваться любым допустимым символом, кроме пробела.
6. Настройте другие параметры тега.

   Для тега должны быть указаны обязательные параметры (например, имя тега, тип данных). Также в зависимости от выбранного протокола и типа данных для настройки могут быть доступны дополнительные параметры (например, единица измерения, пределы масштабирования).
7. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

Добавление тегов в список избранных

Если вы хотите составить список наиболее важных тегов и быстро переходить к этому списку (например, для просмотра текущих значений этих тегов), вы можете добавлять теги в список избранных. Теги можно произвольно добавлять в список избранных и удалять из него. Количество тегов в списке избранных не ограничивается.

Для отображения списка избранных тегов вы можете использовать фильтрацию по столбцу **В избранных** при просмотре таблицы тегов.

По умолчанию созданный тег не добавлен в список избранных.

Чтобы добавить теги в список избранных:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На вкладке **Теги** выберите теги, которые вы хотите добавить в список избранных.
4. По правой кнопке мыши откройте контекстное меню одного из выбранных тегов.
5. В контекстном меню выберите пункт **Добавить в список избранных**.

В таблице тегов для всех выбранных тегов в столбце **В избранных** отобразится признак **Да**.

Чтобы удалить теги из списка избранных:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На вкладке **Теги** выберите теги, которые вы хотите удалить из списка избранных.
4. По правой кнопке мыши откройте контекстное меню одного из выбранных тегов.
5. В контекстном меню выберите пункт **Удалить из списка избранных**.

В таблице тегов для всех выбранных тегов в столбце **В избранных** отобразится признак **Нет**.

Удаление тегов

Удалять теги могут только пользователи с ролью Администратор.

Чтобы удалить теги:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На вкладке **Теги** выберите теги, которые вы хотите удалить.
4. В панели инструментов, которая расположена над таблицей тегов, нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление тегов.

Правила контроля процесса

Для контроля значений тегов в программе могут использоваться следующие правила контроля процесса:

- Правила с заданными условиями. Эти правила содержат условия для отслеживания значений тегов. Каждое правило может содержать условие одного из предусмотренных типов. Если выполнено заданное в правиле условие, программа регистрирует событие. Параметры регистрируемого события также задаются в правиле.
- Правила с Lua-скриптами. Эти правила содержат описания алгоритмов для проверки значений тегов. Алгоритмы составляются на языке программирования Lua с использованием функций и переменных для Lua-скриптов. При срабатывании алгоритма в правиле с Lua-скриптом программа регистрирует событие (параметры регистрируемого события задаются в правиле). Если вы используете Lua-скрипты для правил контроля процесса, то вы можете применить *глобальный Lua-скрипт*, в котором инициализируются глобальные переменные и функции Lua. Эти глобальные переменные и функции вы можете указать в Lua-скрипте любого правила. По умолчанию глобальный Lua-скрипт пустой и не содержит исполняемый код. В программе может существовать только один глобальный Lua-скрипт.

Программа применяет правила контроля процесса при использовании метода контроля процесса по правилам по технологии Контроль технологического процесса. Вы можете включать и выключать применение метода.

Правила контроля процесса могут быть включены или выключены. Включенные правила применяются при анализе трафика. Выключенные правила не применяются и не учитываются.

Программа может автоматически создавать правила контроля процесса с заданными условиями при работе контроля процесса в режиме обучения.

Вы можете просматривать и изменять правила контроля процесса в разделе **Контроль процесса** на вкладке **Правила**.

Правила с заданными условиями для значений тегов

Для контроля значений тегов вы можете использовать правила контроля процесса, в которых заданы условия для значений тегов. Каждое правило может содержать условие одного из предусмотренных типов. Правило может быть связано только с одним тегом. При этом для тега можно создать до 20 правил с различными типами условий.

Правила с заданными условиями могут быть созданы автоматически программой при работе контроля процесса в режиме обучения. Также вы можете вручную создавать и изменять правила с заданными условиями для значений тегов.

Для правила контроля процесса вы можете выбрать один из следующих типов условий:

- **Значение изменилось** – значение контролируемого тега изменилось целиком или в определенном бите.

  Если выключен режим контроля определенного бита значения, с этим условием можно контролировать значение тегов любого типа. При этом вы можете указать количество сохраняемых (разрешенных) значений тега, при обнаружении которых не будет регистрироваться событие. Для правила можно указать количество сохраняемых значений от 1 до 10 (сохраняемые значения будут обновляться по мере обнаружения новых значений). По умолчанию сохраняется только последнее значение.

  Если включен режим контроля определенного бита значения, с этим условием можно контролировать только теги типов int и unsigned int. Для контроля вам нужно указать порядковый номер отслеживаемого бита в теге (целое число в диапазоне, который соответствует типу данных выбранного тега: от 1 до 8, 16, 32 или 64).

- **Тег отсутствует** – контролируемый тег не обнаружен в отслеживаемом трафике в течение заданного времени.

  С этим условием можно контролировать теги любого типа.

- **Обнаружение** – контролируемый тег обнаружен в отслеживаемом трафике.

  С этим условием можно контролировать теги любого типа.

- **В диапазоне** – значение контролируемого тега входит в границы указанного диапазона.

  С этим условием можно контролировать только теги типов int и float.

  Вы можете задать значения для нижней и/или верхней границ диапазона. Заданные значения для границ могут быть включены в диапазон или исключены из него.

- **Вне диапазона** – значение контролируемого тега выходит за границы указанного диапазона.

  С этим условием можно контролировать только теги типов int и float.

  Вы можете задать значения для нижней и/или верхней границ диапазона. Заданные значения для границ могут быть включены в диапазон или исключены из него.

- **Равно** – значение контролируемого тега равно одному из заданных значений целиком или в определенном бите.

  Если выключен режим контроля определенного бита значения, с этим условием можно контролировать значение тегов типов int, bool и string. Вы можете задать от 1 до 10 значений для сравнения.

  Если включен режим контроля определенного бита значения, с этим условием можно контролировать только теги типов int и unsigned int. Для контроля вам нужно указать порядковый номер отслеживаемого бита в теге (целое число в диапазоне, который соответствует типу данных выбранного тега: от 1 до 8, 16, 32 или 64) и значение бита для сравнения (в виде одного из двух целых чисел: ноль или единица).

- **Не равно** – значение контролируемого тега не равно одному из заданных значений целиком или в определенном бите.

  Если выключен режим контроля определенного бита значения, с этим условием можно контролировать значение тегов типов int, bool и string. Вы можете задать от 1 до 10 значений для сравнения.

  Если включен режим контроля определенного бита значения, с этим условием можно контролировать только теги типов int и unsigned int. Для контроля вам нужно указать порядковый номер отслеживаемого бита в теге (целое число в диапазоне, который соответствует типу данных выбранного тега: от 1 до 8, 16, 32 или 64) и значение бита для сравнения (в виде одного из двух целых чисел: ноль или единица).

- **Нарушение монотонного изменения** – значение контролируемого тега нарушает последовательность монотонного возрастания или убывания значений.

  С этим условием можно контролировать только теги типов int и float.

Для правил, контролирующих значения тегов, вам нужно учитывать особенности обработки программой значений, представленных денормализованными числами (числа малого порядка, приближенные к нулю – например, 2.22507e-308 в случае представления данного значения с двойной точностью). Программа преобразует денормализованные числа в нулевые значения.

Для любого условия вы можете выбрать операции, при выполнении которых программа будет контролировать значения тега. Предусмотрены следующие варианты контроля в зависимости от операций с тегом:

- **Контроль при чтении тега** – значение проверяется при чтении тега из устройства.

- **Контроль при записи тега** – значение проверяется при записи тега в устройство.

Правила с Lua-скриптами

Для описания алгоритмов проверки значений тегов в правилах контроля процесса могут использоваться скрипты на языке программирования Lua. Lua-скрипты предоставляют возможности не только для проверки значений тегов, но и для добавления различных сведений в регистрируемые события и журналы работы процессов.

Lua-скрипт должен состоять из одной или нескольких функций. Имена функций должны быть уникальны среди всех правил с Lua-скриптами. Функция, с помощью которой отслеживаются значения тегов, называется *триггерной функцией*. Для регистрации события триггерная функция должна возвращать значение `true`.

Если в скрипте указана переменная, она должна быть инициализирована либо в самом скрипте (для применения только в этом скрипте), либо в отдельном глобальном скрипте (для применения во всех правилах с Lua-скриптами). Глобальный скрипт также может содержать вспомогательные функции, которые можно использовать в правилах с Lua-скриптами.

Триггерная функция вызывается при изменении значения какого-либо тега, используемого в функции. Впервые функция вызывается при получении всех значений тегов, используемых в функции.

Для получения значений тега в коде функции используется запись вида:

```
tag'основные_параметры_тега[:имя_поля][@модификатор]'[.направление_передачи]
```

где:

- `основные_параметры_тега` – обязательные параметры, идентифицирующие тег в программе. Основные параметры представлены следующими параметрами из таблицы тегов:
  - **Устройство**.

    Этот параметр отделяется от следующего символом `:`
  - **Имя тега**.

    Этот параметр отделяется от следующего символом `/`
  - **Идентификатор тега**.
- `имя_поля` – имя поля в структуре полей тега, представленной параметром **Структурные значения** в таблице тегов. Если поле является вложенным в другие поля, его имя указывается вместе с именами всех родительских полей, разделенных двоеточием. Если параметр `имя_поля` не указан, проверяется значение, которое является основным в структуре полей тега.

- `модификатор` – определяет режим представления и получения данных. Предусмотрены следующие модификаторы:

  - `type` – в качестве значения передается название типа данных полученного значения.

  - `str` – полученное значение преобразуется в строковый тип.

  - `loc` – в качестве значения передается закрепленное локализованное название для полученного значения (если локализованное название отсутствует, полученное значение преобразуется в строковый тип).

  - `ts` – для получения метки времени последнего обновления значения тега (время UTC в микросекундах с 1970.01.01). Модификатор не применяется для полей.

  Если модификатор не указан, передается само полученное значение. При этом тип данных значения не меняется.

- `направление_передачи` – задает направление передачи полученного значения. Направление передачи может быть задано одним из следующих параметров:

  - `r` – значение получено при чтении из устройства.

  - `w` – значение получено при записи в устройство.

  - `rw` – любое направление полученного значения.

  Если направление передачи не задано, то передается значение, полученное с любого направления.

  Пример:
  ```
  tag'BayController:BayControllerQ.T1MMXU1.PhV.phsA/73:cVal:mag:f'
  ```

  где:

  - `BayController` – имя устройства.
  - BayControllerQ.T1MMXU1.PhV.phsA – имя тега.
  - 73 – идентификатор тега.
  - cVal:mag:f – имя поля вместе с именами родительских полей.

Записи для получения значений тегов могут использоваться в составе выражений (например, присвоение значений переменным или сравнение значений).

Для выполнения различных действий с помощью Lua-скрипта вы можете использовать *вспомогательные функции*, поддерживаемые Сервером. Имена вспомогательных функций начинаются с символа подчеркивания `_`.

Основные вспомогательные функции для добавления сведений через Lua-скрипты:

- Функция добавления параметров для использования их в качестве дополнительных переменных в событиях:

  `_AddEventParam('имя_параметра', значение_параметра)`

  Имя и значение параметра могут быть заданы произвольно. Для использования параметра и его значения в событиях этот параметр должен быть указан в параметрах типа события в виде `$extra.<имя_параметра>`.

- Функции для добавления записей в журнал работы процесса, в котором выполняется Lua-скрипт (обычно это процесс, имя которого начинается со слова `Filter`). В журнал вносится запись, заданная аргументом функции (переменной или константой):

  - Для создания записи с уровнем *Ошибки*:

    `_WriteErrorLog(аргумент_функции)`

  - Для создания записи с уровнем *Важные*:

    `_WriteWarningLog(аргумент_функции)`

  - Для создания записи с уровнем *Инфо*:

    `_WriteInfoLog(аргумент_функции)`

  - Для создания записи с уровнем *Отладка*:

    `_WriteDebugLog(аргумент_функции)`

  - Для создания записи с уровнем *Отладка*, которая может содержать несколько аргументов функции:

    `print(аргумент_функции1, аргумент_функции2,…)`

    Переменные или константы, заданные аргументами функции, разделяются в записи журнала символом табуляции.

  Записи в журнале не создаются, если уровень записи ниже уровня ведения журнала, установленного для процесса.

Режим обучения правилам контроля процесса

В режиме обучения правилам контроля процесса программа автоматически формирует правила контроля процесса с условиями для значений тегов. Для формирования правил программа анализирует в трафике значения только тех тегов, которые добавлены в таблицу тегов.

Правила контроля процесса, которые были автоматически добавлены в режиме обучения, называются *системными*. У этих правил параметр **Источник** содержит значение **Система**. При автоматическом создании системных правил параметру **Оценка события** присваивается значение по умолчанию – 6.0.

Правила, созданные вручную, называются *пользовательскими*. У этих правил параметр **Источник** содержит значение **Пользователь**. Если в системное правило внесены изменения вручную, это правило также становится пользовательским.

Правилам, добавленным в режиме обучения, программа присваивает статус *Выключено*. Если системное правило было обновлено в режиме обучения, это правило остается с тем же статусом, с которым оно было до обновления: *Включено* или *Выключено*.

В режиме обучения правилам контроля процесса при их добавлении или обновлении программа задает для каждого из правил одно из следующих условий:

- **Не равно**.

  Это условие задается при добавлении правила, если для обнаруженного значения тега не найдено другое системное правило, или при получении до десяти различных значений тега (кроме тегов с типом данных bool или float).

- **Вне диапазона**.

  В правиле выполняется замена на это условие, если получено новое значение для тега с типом данных float или если получено более десяти различных значений для тега с типом данных int.

- **Нарушение монотонного изменения**.

  В правиле выполняется замена на это условие, если обнаруженные значения тега изменялись только в сторону возрастания или только в сторону убывания. Замена на это условие выполняется в правилах для тегов с типом данных int или float по окончании режима обучения.

Также в режиме обучения программа удаляет системные правила контроля процесса в следующих случаях:

- если правило создано для тега с типом данных bool и обнаруженное и сохраненное значения не совпадают (сравнения выполняются только для первых десяти обнаруженных значений, остальные игнорируются);

- если правило создано для тега с типом данных string и получено более десяти различных значений.

Вы можете настраивать режим обучения метода контроля процесса по правилам.

Режим обучения правилам контроля процесса должен быть включен на время, достаточное для обнаружения всех возможных значений нужных тегов. Это время зависит от интенсивности появления тегов в трафике, периодичности работы устройств в промышленной сети и других особенностей технологического процесса. Рекомендуется включать режим обучения на время не менее одного часа. В крупных промышленных сетях для накопления данных в максимальном объеме режим обучения можно включить на период от одного до нескольких дней.

Просмотр таблицы правил контроля процесса

Таблица правил контроля процесса отображается в разделе **Контроль процесса** на вкладке **Правила**. В таблице представлены общие параметры правил, а также тегов и устройств, к которым относятся правила.

Параметры правил отображаются в следующих столбцах таблицы:

- **ID правила**.

  Уникальный идентификатор правила.

- **Группа устройств**.

  Имя группы, в которую помещено связанное с тегом устройство (содержит имя самой группы и имена всех ее родительских групп в дереве групп устройств).

- **Устройство**.

  Имя связанного с тегом устройства.

- **Протокол**.

  Название протокола, по которому передается тег.

- **Имя тега**.

  Заданное имя тега, для которого создано правило.

- **Правило**.

  Заданное имя правила.

- **Описание правила**.

  Заданное описание правила.

- **Статус**.

  Текущий статус правила (*Включено* или *Выключено*).

- **Создано**.

  Дата и время создания правила.

- **Изменено**.

  Дата и время последнего изменения правила.

- **Тип условия**.

  Название выбранного типа условия для правила.

- **Заголовок события**.

  Заголовок события, регистрируемого при срабатывании правила.

- **Оценка события**.

  Оценка события, регистрируемого при срабатывании правила. События оцениваются по шкале от 0.0 до 10.0.

- **Описание события**.

  Описание события, регистрируемого при срабатывании правила.

- **Источник**.

  Сведения об источнике правила.

При просмотре таблицы правил вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Создание правила контроля процесса с параметрами условий

Для создания правил контроля процесса с параметрами условий предусмотрены следующие варианты:

- создание нового правила для тега;

- создание дополнительного правила на основе имеющегося правила.

Чтобы создать новое правило для тега:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Контроль процесса**.

3. На вкладке **Теги** выберите тег, для которого вы хотите создать правило контроля процесса.

   В правой части окна веб-интерфейса появится область деталей.

4. В правом верхнем углу области деталей нажмите на кнопку **Создать правило**.

   Откроется вкладка **Правила** с областью деталей создаваемого правила контроля процесса.

5. Выполните следующие действия:

   a. С помощью переключателя **Включить** задайте статус правила: *Включено* или *Выключено*.

   b. Введите имя и описание правила.

      Вы можете использовать буквы латинского алфавита, цифры, пробел, а также следующие специальные символы: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. Имя правила должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

   c. Выберите тип условия и настройте параметры в зависимости от выбранного типа.

   d. Настройте параметры регистрации события при срабатывании правила (заголовок, описание и оценка события, параметры сохранения трафика).

6. Нажмите на кнопку **Сохранить**.

Чтобы создать дополнительное правило контроля процесса на основе имеющегося правила:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Контроль процесса**.

3. На вкладке **Правила** выберите правило, на основе которого вы хотите создать другое правило для того же самого тега.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Создать другое правило**.

   Появится область деталей создаваемого правила контроля процесса. Для нового правила будут указаны сведения об устройстве, протоколе и теге, полученные из параметров выбранного правила.

5. Выполните следующие действия:

   a. С помощью переключателя **Включить** задайте статус правила: *Включено* или *Выключено*.

   b. Введите имя и описание правила.

   c. Выберите тип условия и настройте параметры в зависимости от выбранного типа.

   d. Настройте параметры регистрации события при срабатывании правила (заголовок, описание и оценка события, параметры сохранения трафика).

6. Нажмите на кнопку **Сохранить**.

Создание правила контроля процесса с Lua-скриптом

Чтобы создать правило с Lua-скриптом:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Контроль процесса**.

3. На вкладке **Правила** откройте область деталей по кнопке **Добавить Lua-скрипт**.

4. Выполните следующие действия:

   a. С помощью переключателя **Включить** задайте статус правила: *Включено* или *Выключено*.

   b. Введите имя и описание правила.

   c. Если вы хотите задать скрипт из шаблона, в области деталей нажмите на кнопку **Использовать шаблон Lua**, в открывшемся окне выберите нужный шаблон и нажмите на кнопку **Применить**.

   d. В поле **Lua-скрипт для правила** введите код скрипта на языке Lua.

      В поле ввода скрипта отображаются имена функций и комментарии, загруженные из шаблона. Вы можете формировать скрипт, изменяя и дополняя шаблонные строки. При вводе текста рядом с курсором автоматически появляются подсказки или доступные для выбора значения (например, подходящие имена устройств и тегов при вводе параметров, идентифицирующих тег).

      Если код скрипта не помещается в поле **Lua-скрипт для правила**, вы можете открыть отдельное окно для отображения кода с помощью кнопки .

   e. Настройте параметры регистрации события при срабатывании правила (заголовок, описание и оценка события, параметры сохранения трафика).

5. Нажмите на кнопку **Сохранить**.

Изменение параметров правила контроля процесса

Чтобы изменить параметры правила контроля процесса:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На вкладке **Правила** выберите правило, которое вы хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Измените нужные параметры. Для изменения параметров вам доступны те же действия, что и при создании правил контроля процесса с параметрами условий или с Lua-скриптами.

Создание, просмотр и изменение глобального Lua-скрипта

Переменные и функции, заданные в глобальном Lua-скрипте могут использоваться в правилах с Lua-скриптами.

Создать и изменить глобальный Lua-скрипт для правил контроля процесса могут только пользователи с ролью Администратор. При этом просматривать содержимое глобального Lua-скрипта могут как пользователи с ролью Администратор, так и пользователи с ролью Оператор.

Чтобы создать или изменить глобальный Lua-скрипт:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На вкладке **Правила** откройте окно редактирования глобального Lua-скрипта по кнопке **Глобальный Lua-скрипт**.
4. Введите код скрипта на языке Lua.
5. Нажмите на кнопку **Сохранить**.

Удаление правил контроля процесса

Чтобы удалить правила контроля процесса:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.

3. На вкладке **Правила** выберите правила, которые вы хотите удалить.

4. Нажмите на кнопку **Удалить**. Если кнопка не отображается в панели инструментов, нажмите на кнопку ⋮ и выберите нужный пункт в открывшемся меню.

   Откроется окно с запросом подтверждения.

5. В окне запроса подтвердите удаление правил.

Настройка контроля взаимодействий

Kaspersky Industrial CyberSecurity for Networks может отслеживать сетевые взаимодействия устройств в промышленной сети. Для определения разрешенных и неразрешенных сетевых взаимодействий используются *правила контроля взаимодействий*. Все обнаруженные сетевые взаимодействия, которые не удовлетворяют действующим правилам контроля взаимодействий, считаются неразрешенными. При обнаружении неразрешенных взаимодействий программа регистрирует соответствующие события.

Правило контроля взаимодействий может относиться к одной из следующих технологий:

- Контроль целостности сети – правило описывает сетевое взаимодействие устройств, использующих заданный набор протоколов и параметров соединения.
- Контроль системных команд – правило описывает контролируемые системные команды при взаимодействии между устройствами по одному из поддерживаемых протоколов для контроля процесса.

Правило контроля взаимодействий содержит следующую информацию о взаимодействии:

- стороны, принимающие участие в сетевом взаимодействии;
- разрешенный протокол или системные команды.

Сетевые взаимодействия между устройствами определяются по MAC- и/или IP-адресам устройств. Если в программу добавлены дополнительные адресные пространства, вы можете настраивать правила контроля взаимодействий для адресов нужных адресных пространств.

При анализе сетевых взаимодействий по технологии Контроль целостности сети программа дополнительно проверяет IP-адреса в этих взаимодействиях на принадлежность известным подсетям. Проверка IP-адресов выполняется для всех взаимодействий IPv4. Программа проверяет каждое взаимодействие на соответствие правилам по технологии Контроль целостности сети (и регистрирует соответствующее событие в случае необходимости), только если такое взаимодействие должно контролироваться согласно таблице ниже.

Подсети IP-адресов, между которыми контролируются взаимодействия

Подсеть отправителя	Подсеть получателя				
	Частная, IT	Частная, OT	Частная, DMZ	Публичная	Link-local
Частная, IT	нет	да	нет	нет	да
Частная, OT	да	да	да	да	да
Частная, DMZ	нет	да	нет	нет	да
Публичная	нет	да	нет	нет	да
Link-local	да	да	да	да	нет

Пример

При контроле взаимодействий по технологии Контроль целостности сети программа проверяет все взаимодействия, в которых в качестве получателей или отправителей сетевых пакетов определены IP-адреса из подсетей с типом **Частная, OT**. Программа не проверяет взаимодействия, в которых в качестве получателей сетевых пакетов определены IP-адреса из подсетей с типом **Частная, DMZ**, а в качестве отправителей определены IP-адреса из подсетей с типом **Частная, IT**.

Технология Контроль системных команд применяется независимо от того, какой подсети принадлежат IP-адреса отправителей и получателей сетевых пакетов с системными командами.

Правила контроля взаимодействий могут быть включены или выключены.

По умолчанию после создания правило включено и применяется для разрешения описанных взаимодействий. При обнаружении взаимодействий, описанных во включенных правилах, программа не регистрирует события.

Выключенные правила предназначены для описания нежелательных сетевых взаимодействий. В режиме обучения для технологий контроля взаимодействий выключенные правила предотвращают автоматическое создание новых включенных правил, описывающих те же сетевые взаимодействия. В режиме наблюдения выключенные правила не учитываются.

Программа обрабатывает правила контроля взаимодействий по технологиям Контроль целостности сети и Контроль системных команд, если включено применение этих технологий. Для этих технологий вы также можете настраивать режим обучения.

Для создания списка правил контроля взаимодействий предусмотрены следующие способы:

- автоматическое формирование правил в режиме обучения;
- автоматическое формирование правил при импорте конфигураций из внешний проектов;
- создание правил вручную.

Вы можете настраивать правила контроля взаимодействий в разделе **Разрешающие правила** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks. Раздел содержит таблицу с правилами контроля взаимодействий по технологиям Контроль целостности сети и Контроль системных команд. Также в этой таблице правил могут быть представлены созданные разрешающие правила для событий.

События, регистрируемые по технологиям Контроль целостности сети и Контроль системных команд, относятся к системным типам событий.

Вы можете просматривать события контроля взаимодействий в таблице зарегистрированных событий. События, регистрируемые по технологии Контроль целостности сети, имеют уровень критичности *Высокий*. Событиям, регистрируемым по технологии Контроль системных команд, присваивается уровень критичности в зависимости от заданного уровня критичности для обнаруженной системной команды.

Режим обучения для технологий контроля взаимодействий

В режиме обучения для технологий контроля взаимодействий программа выполняет следующие действия:

- Если включено применение технологии Контроль целостности сети, программа формирует правила по этой технологии. Правила формируются для всех взаимодействий IPv4, которые должны контролироваться согласно таблице подсетей IP-адресов для контроля взаимодействий. При обнаружении сетевых взаимодействий, которые удовлетворяют выключенным правилам, регистрируются события по технологии Контроль целостности сети. Для регистрации используется системный тип события, которому присвоен код 4000002601.

- Если включено применение технологии Контроль системных команд, программа формирует правила по этой технологии. При обнаружении системных команд, которые удовлетворяют выключенным правилам, регистрируются события обнаружения неразрешенных системных команд по технологии Контроль системных команд. Для регистрации используется системный тип события, которому присвоен код 4000002602.

При формировании правил по технологиям контроля взаимодействий добавляются новые правила, полученные в результате анализа сетевых взаимодействий и системных команд в трафике промышленной сети. Для этих правил параметр **Источник** содержит значение **Система**. Если вы вручную измените параметры правила, параметр **Источник** примет значение **Пользователь**.

Сетевые взаимодействия, обнаруженные при анализе трафика, проверяются на соответствие текущим правилам контроля взаимодействий. Если обнаруженное взаимодействие не соответствует ни одному правилу, программа создает новое правило. Событие обнаружения взаимодействия в этом случае не регистрируется. При создании нового правила программа включает его и добавляет значения параметров на основании полученных данных о сетевом взаимодействии.

Если обнаруженное взаимодействие соответствует только выключенному правилу, программа регистрирует событие по технологии, соответствующей этому правилу. В этом случае новое правило не создается.

В процессе обучения программа может оптимизировать список правил контроля взаимодействий. Оптимизация заключается в объединении двух и более частных правил в одно общее правило либо в удалении частных правил при наличии общего правила. В оптимизации участвуют правила, для которых выполняются следующие условия:

- правила включены;

- параметр **Источник** содержит значение **Система**;

- правила относятся к одной технологии.

Объединение правил при оптимизации происходит, если полученное общее правило будет соответствовать только обнаруженным сетевым взаимодействиям и никаким другим. Например, после обнаружения системной команды при взаимодействии двух устройств было создано одно правило контроля взаимодействий. Затем была обнаружена другая системная команда при взаимодействии этих же устройств. В этом случае в результате оптимизации останется одно общее правило, описывающее обе системные команды при сетевом взаимодействии этих устройств.

Во время работы в режиме обучения программа периодически выполняет оптимизацию правил для соответствующей технологии контроля взаимодействий. Периодичность оптимизации – один раз в минуту. Оптимизация выполняется, если в трафике промышленной сети обнаружены новые взаимодействия. Для поддержания таблицы правил в актуальном состоянии требуется обновлять правила.

После выключения режима обучения оптимизация выполняется еще один раз.

Оптимизация правил контроля взаимодействий после выключения режима обучения может выполняться с задержкой. Длительность задержки зависит от интенсивности поступления данных в программу и может составлять до трех минут. В течение этого времени рекомендуется не вносить изменения в правила по технологиям Контроля целостности сети и Контроля системных команд, созданные в режиме обучения.

Режим обучения для технологий контроля взаимодействий должен быть включен на время, достаточное для получения всех необходимых данных о сетевых взаимодействиях. Это время зависит от количества устройств в промышленной сети, периодичности их работы и обслуживания. Рекомендуется включать режим обучения на время не менее одного часа. В крупных промышленных сетях, для накопления данных в максимальном объеме, режим обучения можно включить на период от одного до нескольких дней.

Режим наблюдения для технологий контроля взаимодействий

В режиме наблюдения для технологий контроля взаимодействий программа выполняет следующие действия:

- Если включено применение технологии Контроль целостности сети, программа проверяет сетевые взаимодействия устройств на соответствие правилам по этой технологии. При обнаружении сетевых взаимодействий, для которых отсутствуют включенные правила, регистрируются события обнаружения неразрешенных взаимодействий по технологии Контроль целостности сети. Для регистрации используется системный тип события, которому присвоен код 4000002601.

- Если включено применение технологии Контроль системных команд, программа проверяет сетевые взаимодействия устройств на соответствие правилам по этой технологии. При обнаружении системных команд, для которых отсутствуют включенные правила, регистрируются события обнаружения неразрешенных системных команд по технологии Контроль системных команд. Для регистрации используется системный тип события, которому присвоен код 4000002602.

Правила, относящиеся к разным технологиям, применяются независимо друг от друга. Поэтому чтобы разрешить использование системной команды, в таблице разрешающих правил должны быть созданы правила (автоматически или вручную) и для этой системной команды, и для сетевого пакета, в котором она передается.

Автоматическое формирование правил контроля взаимодействий в режиме обучения

В режиме обучения Kaspersky Industrial CyberSecurity for Networks автоматически формирует правила контроля взаимодействий. Программа создает новое правило, если обнаруженное сетевое взаимодействие не соответствует ни одному правилу в таблице разрешающих правил.

При создании правила программа задает значения параметров, полученные из трафика и относящиеся к обнаруженному сетевому взаимодействию.

Если создается правило по технологии Контроль целостности сети для взаимодействия, в котором IP-адрес одной из сторон принадлежит известной программе подсети, то программа может не добавить в параметры правила MAC-адреса, обнаруженные вместе с этим IP-адресом. Обнаруженные MAC-адреса для IP-адресов подсети добавляются в случае, если в параметрах подсети выключен режим пропуска MAC-адресов с помощью переключателя **Игнорировать MAC-адреса для правил NIC**.

В режиме обучения программа может автоматически создавать правила контроля взаимодействий, разрешающие отправку системных команд для Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes. Эти правила нужны для удобного совместного использования программ в рамках комплексного решения Kaspersky Industrial CyberSecurity. Для автоматического создания правил перед включением режима обучения требуется включить компонент Проверка целостности проекта ПЛК на компьютерах с установленной программой Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes в этой же промышленной сети. Подробную информацию о включении компонента см. в справочной системе Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes.

Автоматическое формирование правил контроля взаимодействий при импорте конфигураций из внешних проектов

Kaspersky Industrial CyberSecurity for Networks автоматически формирует правила контроля взаимодействий при импорте конфигураций из проекта для устройств IEC 61850. Программа создает новые правила на основе информации об устройствах в импортируемой конфигурации.

После загрузки проекта Kaspersky Industrial CyberSecurity for Networks проверяет в трафике соответствие данных, передаваемых между устройствами, импортированной конфигурации. Если Kaspersky Industrial CyberSecurity for Networks обнаруживает несоответствия в трафике, программа регистрирует события.

Если в импортируемой конфигурации определены протоколы и параметры соединения для взаимодействия устройств, программа создает правило по технологии Контроль целостности сети. При обнаружении сетевых взаимодействий, которые удовлетворяют выключенным правилам, программа регистрирует события по технологии Контроль целостности сети.

Если в импортируемой конфигурации определены системные команды, используемые при взаимодействии между устройствами, программа создает правило по технологии Контроль системных команд. При обнаружении системных команд, которые удовлетворяют выключенным правилам, программа регистрирует обнаружения неразрешенных системных команд по технологии Контроль системных команд.

Для правил, созданных при импорте конфигураций из проекта для устройств IEC 61850, параметр **Источник** содержит значение **Система**. Если вы вручную измените параметры правила, параметр **Источник** примет значение **Пользователь**.

Просмотр правил контроля взаимодействий в таблице разрешающих правил

Правила контроля взаимодействий отображаются в таблице разрешающих правил в разделе **Разрешающие правила** веб-интерфейса программы. К правилам контроля взаимодействий относятся правила следующих типов:

- NIC – правила по технологии Контроль целостности сети.
- CC – правила по технологии Контроль системных команд.

Параметры правил контроля взаимодействий отображаются в следующих столбцах таблицы:

- **ID правила**.

  Уникальный идентификатор правила.

- **Статус** (значок ◐).

  Текущий статус правила (*Включено* или *Выключено*).

- **Тип правила**.

  Для правил контроля взаимодействий – технология, к которой относится правило (NIC или CC). Для правил, выключающих регистрацию событий, указан тип EVT.

- **Протоколы/Команды**.

  Для правил, относящихся к технологии Контроль целостности сети (тип NIC) или выключающих регистрацию событий (тип EVT) – набор используемых протоколов. Для правил, относящихся к технологии Контроль системных команд (тип CC) – протокол и системные команды. Протоколы, которые определяются программой по содержимому сетевых пакетов, выделены курсивом.

- **Сторона 1**.

  Имя устройства / адресная информация одной из сторон сетевого взаимодействия. Отображение адресов и портов адресной информации можно включать и выключать с помощью следующих параметров: **MAC-адрес**, **IP-адрес**, **Номер порта**. Если в программу добавлены дополнительные адресные пространства, можно включать и выключать отображение имен адресных пространств с помощью следующих параметров:

  - **АП для MAC-адресов** – адресные пространства, к которым относятся MAC-адреса в правиле контроля взаимодействий. Параметр может содержать имена только тех АП, в которых есть правила адресных пространств с выбранным уровнем модели OSI **Канальный (L2)**.

  - **АП для IP-адресов** – адресные пространства, к которым относятся IP-адреса в правиле контроля взаимодействий. Параметр может содержать имена только тех АП, в которых есть правила адресных пространств с выбранным уровнем модели OSI **Сетевой (L3)**.

- **Сторона 2**.

  Имя устройства / адресная информация другой стороны сетевого взаимодействия. Отображение адресной информации можно настраивать аналогично, как для столбца **Сторона 1**.

- **Комментарий**.

  Дополнительная информация о правиле.

- **Создано**.

  Дата и время создания правила.

- **Изменено**.

  Дата и время последнего изменения правила.

- **Правило в событии**.

  Имя правила контроля процесса или обнаружения вторжений, которое должно быть указано в событии (для правил типа EVT).

- **Точка мониторинга**.

  Имя точки мониторинга, которое должно быть указано в событии (для правил типа EVT).

- **Тип события**.

  Идентификатор и заголовок типа события (для правил типа EVT).

- **Источник**.

  Сведения об источнике правила.

При просмотре таблицы правил вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Создание правил контроля взаимодействий вручную

Этот раздел содержит инструкции для создания правила контроля взаимодействий вручную.

Создание правила контроля взаимодействия с изначально пустыми значениями параметров или со значениями из шаблона

Чтобы создать правило контроля взаимодействия с изначально пустыми значениями параметров или со значениями из шаблона:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Разрешающие правила** откройте область деталей по кнопке **Добавить правило**.
3. Если вы хотите задать значения параметров из шаблона, в области деталей нажмите на кнопку **Использовать шаблон**, в открывшемся окне выберите нужный шаблон и нажмите на кнопку **Применить**.
4. В области деталей выберите тип правила, соответствующий нужной технологии контроля взаимодействий:
   - Если вы хотите создать правило по технологии Контроль целостности сети, нажмите на кнопку **NIC**.
   - Если вы хотите создать правило по технологии Контроль системных команд, нажмите на кнопку **CC**.

5. В поле **Протокол** укажите протокол для взаимодействия устройств.

   При выборе поля **Протокол** откроется окно с таблицей поддерживаемых протоколов, отображаемых в виде дерева стека протоколов. Вы можете управлять отображением элементов дерева с помощью кнопок **+** и **-** рядом с названиями протоколов, которые содержат протоколы следующих уровней.

   При необходимости воспользуйтесь поисковой строкой над таблицей, чтобы найти нужные протоколы.

   Чтобы указать протокол, выполните следующие действия:

   a. В таблице протоколов выберите протокол, который вы хотите указать для правила. Для выбора нужного протокола нажмите на кнопку, которая отображается в левом столбце таблицы протоколов.

      Для правила по технологии Контроль целостности сети вы можете выбрать любой протокол, отображаемый в таблице поддерживаемых протоколов. Для правила по технологии Контроль системных команд вы можете выбрать только протокол из числа поддерживаемых протоколов для контроля процесса.

   b. Нажмите на кнопку **OK**.

   Если выбран протокол, который программа может определять по содержимому сетевых пакетов, ниже поля **Протокол** появится пояснение об этом.

6. Если для правила выбрана технология Контроль системных команд, в поле **Команды** укажите нужные системные команды.

   При выборе поля **Команды** открывается окно со списком системных команд, доступных для выбранного протокола. Чтобы указать команды, выполните следующие действия:

   a. В списке системных команд установите флажки напротив тех команд, которые нужно разрешить. Если требуется разрешить все команды, вы можете либо установить все флажки, либо снять все флажки для всех команд.

   b. Нажмите на кнопку **OK**.

7. При необходимости введите дополнительную информацию о правиле в поле **Комментарий**.

8. В блоках параметров **Сторона 1** и **Сторона 2** укажите доступную для изменения адресную информацию для сторон сетевого взаимодействия. В зависимости от выбранного протокола (или набора протоколов), адресная информация может содержать MAC-адрес, IP-адрес и/или номер порта. Если в программу добавлены дополнительные адресные пространства, вы можете указать имена адресных пространств для адресов.

   Для автоматического заполнения адресной информации стороны сетевого взаимодействия вы можете выбрать известные программе устройства. Для этого выполните следующие действия:

   a. Откройте окно выбора устройств по ссылке **Указать адреса устройств**.

   b. В окне выбора устройств установите флажки напротив тех устройств, которые вы хотите использовать.

      Окно выбора устройств содержит таблицу, в которой можно настраивать отображение и порядок столбцов, выполнять фильтрацию, поиск и сортировку аналогично таблице устройств в разделе **Активы**.

   c. В окне выбора устройств нажмите на кнопку **OK**.

9. В области деталей нажмите на кнопку **Сохранить**.

   Программа проверит текущий состав правил контроля взаимодействий.

10. Если среди правил контроля взаимодействий присутствует включенное правило, в котором совпадают все параметры, отобразится предупреждение о наличии совпадающего правила. В этом случае закройте предупреждение и измените параметры создаваемого правила.

11. Если среди правил контроля взаимодействий присутствует включенное правило с более общими параметрами, отобразится предупреждение о наличии общего правила. При наличии общего правила новое частное правило не будет использоваться в программе. Предупреждение будет содержать запрос на сохранение нового частного правила. Для создания нового правила с заданными параметрами подтвердите решение в окне запроса (например, если вы хотите потом удалить общее правило).

    Новое правило будет добавлено в таблицу разрешающих правил.

12. Если среди правил контроля взаимодействий присутствуют включенные правила с более частными параметрами, отобразится предупреждение о наличии более частных правил. После появления общего правила частные правила не будут использоваться в программе. Предупреждение будет содержать запрос на удаление частных правил. Для удаления частных правил подтвердите решение в окне запроса.

    Если в таблице правил присутствуют выключенные правила с более частными или совпадающими параметрами, программа удаляет эти правила из списка. При удалении этих правил программа не отображает запрос.

13. Если для нового правила по технологии Контроль системных команд отсутствует включенное правило, которое разрешает сетевое взаимодействие между устройствами, отобразится запрос на создание соответствующего правила по технологии Контроль целостности сети. В этом случае рекомендуется создать дополнительное правило вместе с текущим создаваемым правилом. Для этого подтвердите решение в окне запроса и выполните действия по созданию нового правила по технологии Контроль целостности сети.

Создание правила контроля взаимодействия на основе имеющегося правила

Чтобы создать правило контроля взаимодействия на основе имеющегося правила:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Разрешающие правила** выберите правило, на основе которого вы хотите создать новое правило.

3. По правой кнопке мыши откройте контекстное меню.

4. В контекстном меню выберите пункт **Копировать правило**.

    В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила. Для параметров нового правила будут заданы значения, полученные из параметров выбранного правила.

5. Измените нужные параметры. Для этого выполните пункты 4–9, описанные в процедуре создания правила с изначально пустыми значениями параметров.

Создание правила на основе события, зарегистрированного по технологии Контроль целостности сети или Контроль системных команд

Чтобы создать правило контроля взаимодействия на основе события, зарегистрированного по технологии Контроль целостности сети или Контроль системных команд:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **События**.

3. В таблице зарегистрированных событий выберите событие, на основе которого вы хотите создать правило контроля взаимодействий.

   В правой части окна веб-интерфейса появится область деталей.

4. В области деталей нажмите на кнопку **Создать разрешающее правило**.

   В окне браузера откроется раздел **Разрешающие правила**. В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила. Для параметров нового правила будут заданы значения, полученные из сохраненных сведений о событии.

5. При необходимости измените параметры нового правила. Для этого выполните пункты 4–9, описанные в процедуре создания правила с изначально пустыми значениями параметров. Если изменять параметры нового правила не требуется, сохраните правило с помощью кнопки **Сохранить**.

Изменение параметров правила контроля взаимодействий

Вы можете изменять параметры включенного правила контроля взаимодействий. Для выключенных правил возможность изменения недоступна.

Чтобы изменить параметры правила контроля взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Разрешающие правила** выберите нужное правило типа NIC или CC для изменения параметров.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Изменить**.

4. Измените нужные параметры.

Включение и выключение правил контроля взаимодействий

Правилам контроля взаимодействий могут быть присвоены статусы *Включено* или *Выключено*. По умолчанию после создания правила включены.

Вы можете выключить те правила, которые не должны использоваться при работе технологий контроля взаимодействий в режиме наблюдения.

Чтобы изменить статус правил контроля взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Разрешающие правила** выберите правила контроля взаимодействий, для которых вы хотите изменить статус.
3. Включите или выключите правила с помощью кнопок **Включить** и **Выключить**. Каждая из этих кнопок отображается, если среди выбранных правил есть правила, с которыми можно выполнить соответствующую операцию.

   Если выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000, программа не проверяет статус правил. В этом случае в области деталей отображаются обе кнопки для изменения состояния правил.

Удаление правил контроля взаимодействий

Вы можете выборочно удалить одно или несколько правил контроля взаимодействий. Удаленные правила перестают действовать при работе технологий контроля взаимодействий как в режиме наблюдения, так и в режиме обучения.

Чтобы удалить правила контроля взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Разрешающие правила**.
3. В таблице правил выберите правила контроля взаимодействий, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения. В зависимости от состояния выбранных правил, в запросе будут предложены следующие варианты действий:

   - Если все выбранные правила включены, программа предлагает удалить выбранные правила, выключить их или отменить операцию. Это условие не проверяется, если выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000.
   - Если среди выбранных правил присутствуют выключенные правила или выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000, программа предлагает удалить выбранные правила или отменить операцию.
5. В окне запроса подтвердите удаление правил.

Настройка обнаружения вторжений

Для обнаружения вторжений в трафике промышленной сети вы можете использовать правила обнаружения вторжений и дополнительные методы обнаружения вторжений по встроенным алгоритмам. При обнаружении в трафике признаков атак Kaspersky Industrial CyberSecurity for Networks регистрирует события по технологии Обнаружение вторжений.

Настройка правил и методов обнаружения вторжений выполняется при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс. Список правил обнаружения вторжений отображается в разделе **Обнаружение вторжений**.

Настройка параметров регистрации событий обнаружения вторжений выполняется в разделе **Параметры → Типы событий**.

Вы можете просмотреть события обнаружения вторжений в таблице зарегистрированных событий.

Правила обнаружения вторжений

Правило обнаружения вторжений описывает аномалию трафика, которая может быть признаком атаки в промышленной сети. Правила содержат условия, по которым система обнаружения вторжений анализирует трафик.

Правила обнаружения вторжений хранятся на Сервере и сенсорах.

Программа применяет правила обнаружения вторжений при использовании метода обнаружения вторжений по правилам. Вы можете включать и выключать применение метода.

Правила обнаружения вторжений группируются в наборы правил по каким-либо признакам. Например, правила могут быть сгруппированы по их назначению и входить в набор, предназначенный для обнаружения определенных видов вторжений. Вы можете использовать следующие типы наборов правил:

- Системные наборы правил. Эти наборы правил поставляются "Лабораторией Касперского" и предназначены для обнаружения признаков наиболее часто встречающихся атак или нежелательной сетевой активности. Системные наборы правил доступны сразу после установки программы. Вы можете обновлять системные наборы правил, устанавливая обновления.

- Пользовательские наборы правил. Эти наборы правил пользователь самостоятельно загружает в программу. Для загрузки нужно использовать файлы, в которых содержатся структуры данных, задающие правила обнаружения вторжений. Файлы для загрузки должны находиться в одной директории и иметь расширение rules. Имена пользовательских наборов правил совпадают с именами файлов, из которых были загружены эти наборы правил.

Программа поддерживает применение не более чем 50 000 правил суммарно во всех загруженных наборах правил. Ограничение количества загруженных наборов правил – не более 100.

Правила, загружаемые из пользовательских наборов правил, могут содержать такие условия для анализа трафика, по которым программа будет регистрировать слишком большое количество событий срабатывания этих правил. В этом случае вам нужно учитывать, что регистрация слишком большого количества событий может повлиять на производительность системы обнаружения вторжений.

Наборы правил обнаружения вторжений могут быть включены или выключены. Правила из включенного набора применяются при анализе трафика, если включен метод обнаружения вторжений по правилам. Если набор правил выключен, правила из этого набора не применяются.

При загрузке набора правил программа выполняет проверку содержащихся в нем правил. Если в проверяемых правилах обнаружены ошибки, программа блокирует применение таких правил. Если обнаружены ошибки во всех правилах набора или набор не содержит правил, программа выключает этот набор правил.

Сведения о наборах правил и обнаруженных ошибках вы можете просмотреть в разделе **Обнаружение вторжений**.

При обнаружении в трафике условий, заданных в правиле из включенного набора, программа регистрирует событие срабатывания правила. Для регистрации используются системные типы событий, которым присвоены следующие коды:

- 4000003000 – для события при срабатывании правила из системного набора правил;
- 4000003001 – для события при срабатывании правила из пользовательского набора правил.

Пользовательские наборы правил могут содержать правила, полученные из других систем обнаружения и предотвращения вторжений. При обработке таких правил программа не выполняет заданные в них действия, применяющиеся по отношению к сетевым пакетам (например, действия `drop` и `reject`). В результате срабатывания правил обнаружения вторжений в Kaspersky Industrial CyberSecurity for Networks выполняется только регистрация событий.

Значения оценок событий Kaspersky Industrial CyberSecurity for Networks соответствуют значениям приоритетов в правилах обнаружения вторжений (см. таблицу ниже).

Соответствие приоритетов правил и значений оценок событий

Значения приоритетов в правилах обнаружения вторжений	Значения оценок событий Kaspersky Industrial CyberSecurity for Networks
4 и более	2.5
3	4.5
2	6.5
1	9

Дополнительные методы обнаружения вторжений

Для обнаружения вторжений вы можете применять следующие дополнительные методы:

- Обнаружение признаков подмены адресов в ARP-пакетах (ARP-спуфинг).

  Если включено обнаружение признаков подмены адресов в ARP-пакетах, Kaspersky Industrial CyberSecurity for Networks проверяет указываемые адреса в ARP-пакетах и обнаруживает признаки атак низкого уровня типа "человек посередине" (Man in the middle, MITM). Этот тип атак в сетях с использованием протокола ARP характеризуется наличием в трафике поддельных ARP-сообщений.

  При обнаружении признаков подмены адресов в ARP-пакетах программа регистрирует события по технологии Обнаружение вторжений. Для регистрации используются системные типы событий, которым присвоены следующие коды:

  - 4000004001 – для события обнаружения нескольких ARP-ответов, которые не связаны с ARP-запросами;
  - 4000004002 – для события обнаружения нескольких ARP-запросов с одного MAC-адреса разным получателям.

- Обнаружение аномалий в протоколе TCP.

  Если включено обнаружение аномалий в протоколе TCP, Kaspersky Industrial CyberSecurity for Networks проверяет TCP-сегменты потока данных в поддерживаемых протоколах прикладного уровня.

  При обнаружении пакетов, содержащих перекрывающиеся TCP-сегменты с различающимся содержимым, программа регистрирует событие по технологии Обнаружение вторжений. Для регистрации используется системный тип события, которому присвоен код 4000002701.

- Обнаружение аномалий в протоколе IP.

  Если включено обнаружение аномалий в протоколе IP, Kaspersky Industrial CyberSecurity for Networks проверяет фрагментированные IP-пакеты.

  При обнаружении ошибок сборки IP-пакетов программа регистрирует события по технологии Обнаружение вторжений. Для регистрации используются системные типы событий, которым присвоены следующие коды:

  - 4000005100 – для события обнаружения конфликта данных при сборке IP-пакета (IP fragment overlapped);
  - 4000005101 – для события обнаружения IP-пакета с превышением максимально допустимого размера (IP fragment overrun);
  - 4000005102 – для события обнаружения IP-пакета с размером начального фрагмента меньше ожидаемого (IP fragment too small);
  - 4000005103 – для события обнаружения несоответствия фрагментов IP-пакета (mis-associated fragments).

- Обнаружение атак подбора и сканирования.

  Если включено обнаружение атак подбора и сканирования, Kaspersky Industrial CyberSecurity for Networks проверяет статистику сетевой активности с целью выявления признаков атак подбора учетных данных, отказа в обслуживании, сканирования, подмены сетевых сервисов и других аномалий.

  Метод использует встроенные правила. При срабатывании правил программа регистрирует событие по технологии Обнаружение вторжений. Для регистрации используется системный тип события, которому присвоен код 4000003002.

Вы можете включать и выключать применение методов. Применять дополнительные методы обнаружения вторжений можно независимо от наличия и состояния правил обнаружения вторжений. Для проверки по дополнительным методам используются встроенные алгоритмы.

Включение и выключение наборов правил обнаружения вторжений

Наборам правил обнаружения вторжений могут быть присвоены статусы *Включено* или *Выключено*. Если набор правил выключен, все правила этого набора не используются при обнаружении вторжений.

При включении или выключении выбранных наборов правил на всех компьютерах с установленными компонентами программы (Сервере и сенсорах) выполняется перезапуск системы обнаружения вторжений. Перезапуск необходим для применения изменений.

Изменять состояния наборов правил обнаружения вторжений могут только пользователи с ролью Администратор.

Чтобы изменить статус наборов правил обнаружения вторжений:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Обнаружение вторжений** выберите наборы правил, для которых вы хотите изменить статус.
3. По правой кнопке мыши откройте контекстное меню.

4. В контекстном меню выберите один из следующих пунктов:

   - **Включить**, если вы хотите включить все выключенные наборы правил из числа выбранных.
   - **Выключить**, если вы хотите выключить все включенные наборы правил из числа выбранных.
   - **Поменять статусы выбранных наборов правил**, если для всех выбранных наборов правил вы хотите одновременно инвертировать их статусы. Этот вариант позволяет быстрее включить и выключить выбранные наборы правил с разными статусами на всех компьютерах с установленными компонентами программы (так как для применения изменений будет выполнен только один перезапуск системы обнаружения вторжений на этих компьютерах).

   Откроется окно с запросом подтверждения.

5. В окне запроса нажмите на кнопку **ОК**.

Загрузка и замена пользовательских наборов правил обнаружения вторжений

Вы можете загрузить в программу наборы правил обнаружения вторжений из файлов. Для загрузки в программу файлы с описаниями правил обнаружения вторжений должны находиться в одной папке и иметь расширение rules. Имена файлов не должны содержать следующие символы: `\ / : * ? , " < > |`.

После загрузки из файла правила обнаружения вторжений сохраняются в программе в качестве пользовательского набора правил. Имя набора правил совпадает с именем файла, из которого этот набор был загружен.

> При загрузке наборов правил из файлов текущие пользовательские наборы правил удаляются из таблицы и заменяются новыми. При этом системные наборы правил (для которых в столбце **Источник** указано значение **Система**) не удаляются из таблицы.

Загружать пользовательские наборы правил обнаружения вторжений могут только пользователи с ролью Администратор.

Чтобы загрузить и заменить пользовательские наборы правил обнаружения вторжений:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Обнаружение вторжений**.
3. По ссылке **Заменить все пользовательские правила** в панели инструментов вызовите окно для выбора папки с файлами правил обнаружения вторжений.
4. При появлении окна запроса нажмите на кнопку **ОК**.
5. В стандартном окне используемого браузера выберите папку, в которой содержатся нужные файлы, и нажмите на кнопку пересылки файлов из этой папки.

   В таблице с наборами правил отобразятся новые пользовательские наборы правил. Для этих наборов правил в столбце **Источник** будет указано значение **Пользователь**. Все наборы правил, в которых не обнаружены ошибки, будут включены.

6. Проверьте наличие ошибок в правилах загруженных наборов правил.

   Сведения об обнаруженных ошибках отображаются в столбце **Правила**. При отсутствии ошибок отображается статус *OK*. Если набор правил содержит ошибки, вы можете просмотреть подробные сведения о них по ссылке **Подробнее**.

7. При необходимости измените статусы наборов правил (в том числе тех наборов, для которых отображается статус *Ошибки в некоторых правилах*).

Удаление пользовательских наборов правил обнаружения вторжений

Вы можете удалить все пользовательские наборы правил обнаружения вторжений, которые были загружены в программу из файлов. Возможность выборочного удаления пользовательских наборов правил недоступна. Если вы хотите использовать в программе только некоторые из имеющихся наборов правил, вы можете скопировать файлы с этими наборами в отдельную папку и заменить все пользовательские наборы правил на наборы правил из этой папки.

Удалять пользовательские наборы правил обнаружения вторжений могут только пользователи с ролью Администратор.

Чтобы удалить пользовательские наборы правил обнаружения вторжений:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Обнаружение вторжений**.

3. Запустите удаление пользовательских наборов правил по ссылке **Удалить все пользовательские правила** в панели инструментов.

   Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **ОК**.

Все пользовательские наборы правил обнаружения вторжений будут удалены из таблицы.

Управление журналами

Этот раздел содержит информацию об управлении журналами Kaspersky Industrial CyberSecurity for Networks.

Управлять журналами Kaspersky Industrial CyberSecurity for Networks могут только пользователи с ролью Администратор.

Управление параметрами хранения журналов в базе данных Сервера

Вы можете изменить параметры хранения записей журналов в базе данных Сервера.

Чтобы изменить параметры хранения журналов в базе данных Сервера:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку Сервера.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров Сервера.
5. На вкладке **Общие** настройте следующие параметры в блоках параметров **События**, **Записи аудита** и **Сообщения программы**:

   a. С помощью параметра **Макс. объем** задайте ограничение занимаемого объема для хранения записей. Вы можете выбрать единицу измерения для указанного значения: **МБ** или **ГБ**.

   При изменении значения параметра обратите внимание на оцениваемое максимальное количество записей для указанного объема. Также вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.

   b. При необходимости с помощью параметра **Время хранения (дней)** включите ограничение на минимальное время хранения записей и укажите нужное количество дней для хранения.
6. Нажмите на кнопку **Сохранить**.

Управление параметрами сохранения трафика в базе данных Сервера

Программа может сохранять трафик, полученный на момент регистрации событий. Трафик сохраняется в базе данных Сервера при регистрации событий, для которых включено сохранение трафика. Также программа может сохранять трафик в базе данных Сервера непосредственно при запросе на загрузку трафика, используя временные файлы дампа трафика.

Программа сохраняет данные о трафике блоками. Если блок трафика относится к нескольким событиям (когда события регистрируются в коротком промежутке времени), этот блок трафика не дублируется в базе данных.

Чтобы изменить параметры сохранения трафика в базе данных Сервера:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку Сервера.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров Сервера.
5. На вкладке **Общие** перейдите к блоку параметров **Трафик для событий** и задайте ограничение занимаемого объема для хранения трафика с помощью параметра **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.
6. Нажмите на кнопку **Сохранить**.

Управление параметрами сохранения файлов дампа трафика

Программа сохраняет трафик, полученный через точки мониторинга, в виде файлов дампа трафика. Эти файлы используются программой для анализа поступающего трафика. Также с помощью этих файлов вы можете выполнять следующие действия в программе:

- загрузка трафика, поступившего на точки мониторинга узлов;
- загрузка трафика при работе с картой сетевых взаимодействий;
- загрузка трафика сетевых сеансов;
- загрузка трафика для событий (файлы дампа трафика позволяют загрузить трафик для событий, даже если в соответствующих типах событий выключено сохранение трафика).

Файлы дампа трафика размещаются в хранилищах на узлах с установленными компонентами программы. На каждом узле может использоваться как внутреннее хранилище узла (созданное автоматически при установке компонента программы), так и внешнее хранилище, если оно подключено на узле.

Программа хранит файлы дампа трафика временно. По мере поступления трафика программа автоматически удаляет из хранилищ самые старые файлы дампа трафика, если общий объем файлов приближается к ограничению, заданному для хранилища.

Для каждого узла вы можете настроить параметры сохранения трафика во внутреннем хранилище. Вы также можете подключить внешнее хранилище на узле и настроить параметры сохранения трафика во внешнем хранилище.

Чтобы настроить параметры сохранения файлов дампа трафика во внутреннем хранилище узла:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку нужного узла.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров узла.
5. На вкладке **Общие** при необходимости включите фильтрацию в блоке **Фильтрация сохраняемого трафика** и введите выражение для фильтрации с использованием технологии BPF (Berkley Packet Filter) по адресным параметрам в сетевых пакетах.

   Фильтрация позволяет сократить объем сохраняемого трафика за счет отбрасывания сетевых пакетов, не удовлетворяющих фильтру. Однако при использовании фильтрации вам нужно учитывать, что программа может получать в отфильтрованном трафике не все данные, необходимые для качественного анализа трафика. Вам нужно настроить фильтрацию таким образом, чтобы в файлах дампа трафика сохранялись все сетевые пакеты, которые требуются для анализа трафика в соответствии с функциональностью программы.
6. Перейдите к блоку параметров **Файлы дампа трафика** и задайте ограничение занимаемого объема для хранения файлов дампа трафика с помощью параметра **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать объем и скорость поступления входящего трафика, а также, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.
7. Нажмите на кнопку **Сохранить**.

Включение и выключение аудита действий пользователей

Вы можете включать и выключать аудит действий пользователей программы.

По умолчанию аудит действий пользователей включен.

Чтобы включить или выключить аудит действий пользователей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Аудит**.
3. Включите или выключите аудит действий пользователей с помощью переключателя **Аудит действий пользователей** в панели инструментов.
4. Дождитесь применения изменений. До завершения перевода в другое состояние переключатель недоступен.

Изменение уровней ведения журналов работы процессов

На узлах с установленными компонентами программы выполняются служебные процессы, которые могут сохранять данные о своей работе в журналах в локальных директориях. Вы можете управлять сохранением данных в журналах работы следующих процессов программы:

- На компьютере, который выполняет функции Сервера:
  - EntityManager.
  - Filter.
  - KisClient.
  - NetworkDumper.
  - ProductServer.
  - Watchdog.
  - WebServer.
- На компьютере, который выполняет функции сенсора:
  - EntityManager.
  - Filter.
  - NetworkDumper.
  - Watchdog.

Для каждого процесса вы можете задать один из следующих уровней ведения журнала:

- **Выкл**. В журнале не сохраняются данные о работе процесса.
- **Ошибки**. В журнале сохраняются только данные об ошибках, возникших в работе процесса.
- **Важные**. В журнале сохраняются данные уровня **Ошибки** и данные, на которые нужно обратить внимание.
- **Инфо**. В журнале сохраняются данные уровня **Важные** и информация справочного характера.
- **Отладка**. В журнале сохраняются данные уровня **Инфо** и все данные о работе процесса, которые могут потребоваться в процессе отладки программы (например, сведения о производительности процесса).

Необходимость изменить уровни ведения журналов может возникнуть, например, при обращении в Службу технической поддержки.

Изменять уровни ведения журналов могут только пользователи с ролью Администратор.

Чтобы изменить уровни ведения журналов для процессов Kaspersky Industrial CyberSecurity for Networks:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Ведение журналов**.
3. Измените уровни ведения журналов в зависимости от нужного результата:
   - Если вы хотите задать одинаковый уровень ведения журналов для всех процессов на всех узлах, нажмите на заголовок столбца с названием нужного уровня.
   - Если вы хотите задать одинаковый уровень ведения журналов для всех процессов на одном из узлов, нажмите на ячейку столбца с названием нужного уровня в строке с именем узла.
   - Если вы хотите для одного процесса задать уровень ведения журнала, отличающийся от заданных уровней для других процессов, раскройте список процессов нужного узла в столбце **Узлы и процессы** и нажмите на ячейку столбца с названием нужного уровня в строке с именем процесса.
4. Дождитесь применения изменений (до применения изменений отображается индикатор выполнения).

Настройка совместной работы с EPP-приложениями

Kaspersky Industrial CyberSecurity for Networks может получать и обрабатывать данные, которые поступают от приложений "Лаборатории Касперского", выполняющих функции защиты рабочих станций и серверов. Эти приложения входят в состав системы защиты конечных устройств (англ. Endpoint Protection Platform, EPP) и устанавливаются на конечные устройства внутри IT-инфраструктуры организации.

Передачу данных от EPP-приложений осуществляют программные компоненты *Endpoint Agent*. В зависимости от используемого EPP-приложения функции Endpoint Agent может выполнять следующее программное обеспечение:

- Программа Kaspersky Endpoint Agent. Эта программа устанавливается на рабочие станции и серверы в IT-инфраструктуре организации дополнительно к используемому EPP-приложению, которое поддерживает Kaspersky Endpoint Agent (например, Kaspersky Industrial CyberSecurity for Nodes).
- Программные модули, встроенные в EPP-приложение. Программные модули, выполняющие функции Endpoint Agent, встроены в Kaspersky Industrial CyberSecurity for Linux Nodes тех версий, с которыми поддерживается работа Kaspersky Industrial CyberSecurity for Networks в режиме интеграции.

С использованием полученных данных от EPP-приложений Kaspersky Industrial CyberSecurity for Networks позволяет выполнять различные действия на устройствах с Endpoint Agent.

Для установки соединений с Kaspersky Endpoint Agent на устройствах с устаревшими операционными системами (например, Windows 7) в Kaspersky Industrial CyberSecurity for Networks могут использоваться устаревшие и потенциально уязвимые протоколы и алгоритмы шифрования. Если в вашей сети отсутствуют устройства с устаревшими операционными системами или с такими устройствами не требуется устанавливать соединения, рекомендуется выключить использование устаревших и потенциально уязвимых протоколов и алгоритмов шифрования в Kaspersky Industrial CyberSecurity for Networks. Для получения дополнительной информации вы можете обратиться в Службу технической поддержки.

Максимальное количество компьютеров, от которых поддерживается получение и обработка данных от EPP-приложений – 1000.

Данные от компьютеров с программными компонентами Endpoint Agent поступают в Kaspersky Industrial CyberSecurity for Networks через *серверы интеграции*. Функции сервера интеграции может выполнять любой узел с установленным компонентом Kaspersky Industrial CyberSecurity for Networks (Сервер или сенсор). Для интеграции с Endpoint Agent вам нужно добавить серверы интеграции на те узлы, которые будут получать данные от компьютеров с Endpoint Agent.

Функции сервера интеграции на узле Kaspersky Industrial CyberSecurity for Networks реализует сервис интеграции с EPP-приложениями – kics4net-epp-proxy. Пакет для установки этого сервиса входит в комплект поставки Kaspersky Industrial CyberSecurity for Networks.

При поступлении данных от Endpoint Agent на сервер интеграции программа может выполнять следующие действия:

- регистрировать события по технологии EPP (события защиты рабочих станций и серверов);
- добавлять в таблицу устройств те устройства, на которых установлены EPP-приложения (а также устройства, с которыми были двусторонние взаимодействия этих устройств);
- обновлять в таблице устройств сведения об устройствах, на которых установлены EPP-приложения (например, версия операционной системы, сведения о модели или производителе);
- отображать на узлах карты сетевых взаимодействий и топологической карты специальные значки, обозначающие наличие EPP-приложений и состояния подключения этих приложений;
- отображать на карте сетевых взаимодействий соединения, в которых одной из сторон взаимодействия является устройство с установленным EPP-приложением (при этом для отображения сведений о таких соединениях приоритет имеют данные, полученные из трафика от точек мониторинга);
- контролировать оборудование на устройствах;
- регистрировать сетевые сеансы.

С помощью программных компонентов Endpoint Agent вы можете выполнять следующие действия при работе с Kaspersky Industrial CyberSecurity for Networks:

- сканирования устройств в рамках заданий аудита настроек и уязвимостей и заданий контроля конфигураций;
- запускать действия по реагированию при регистрации событий по технологии EPP, если для этих событий построены цепочки развития угроз в Endpoint Agent.

Компьютеры с Endpoint Agent устанавливают защищенные соединения с серверами интеграции по протоколу HTTPS. Для обеспечения безопасности соединений используются сертификаты, выданные Сервером Kaspersky Industrial CyberSecurity for Networks. В соединениях могут использоваться следующие сертификаты:

- Сертификат сервера интеграции. Этот сертификат проверяет компьютер с Endpoint Agent при каждой установке соединения. Соединение не устанавливается до успешного завершения проверки сертификата.
- Сертификат клиента. Этот сертификат используется для аутентификации клиентов сервера интеграции, которыми являются компьютеры с Endpoint Agent. Один и тот же сертификат клиента может использоваться несколькими компьютерами с Endpoint Agent. По умолчанию сервер интеграции не выполняет проверку сертификатов клиентов, но вы можете ее включить для усиления защиты соединений.

Доставка сертификатов и открытых ключей на компьютеры с Endpoint Agent выполняется с помощью Kaspersky Security Center. Для загрузки этих данных в Kaspersky Security Center используется файл свертки, который нужно создать в Kaspersky Industrial CyberSecurity for Networks после добавления сервера интеграции.

Настраивать получение данных от EPP-приложений могут только пользователи с ролью Администратор.

Сценарий подготовки к получению данных от EPP-приложений

Сценарий подготовки к получению данных от EPP-приложений состоит из следующих этапов:

1. **Установка EPP-приложений на компьютеры контролируемой сети**

   На этом этапе вам нужно установить приложения "Лаборатории Касперского", выполняющие функции защиты рабочих станций и серверов (EPP-приложения). EPP-приложения требуется установить на все компьютеры, данные о которых вы хотите получать в Kaspersky Industrial CyberSecurity for Networks. Эти компьютеры должны находиться либо вне промышленной сети (трафик которой контролируется через точки мониторинга), либо иметь дополнительное подключение к другой сети, в которую входит один из узлов с установленным компонентом Kaspersky Industrial CyberSecurity for Networks (например, к выделенной сети Kaspersky Industrial CyberSecurity). Если функции программного компонента Endpoint Agent для EPP-приложений выполняет программа Kaspersky Endpoint Agent, эту программу также требуется установить на соответствующие компьютеры.

   > В текущей версии Kaspersky Industrial CyberSecurity for Networks поддерживает получение и обработку данных только при работе в режиме интеграции с Kaspersky Industrial CyberSecurity for Nodes или Kaspersky Industrial CyberSecurity for Linux Nodes. Версии указанных программ, с которыми поддерживается работа в режиме интеграции, см. в статье Аппаратные и программные требования.

2. **Добавление серверов интеграции для узлов Kaspersky Industrial CyberSecurity for Networks**

   На этом этапе выполняются процедуры добавления серверов интеграции на узлы, к которым будут подключаться компьютеры с программным компонентом Endpoint Agent. Сетевые взаимодействия узлов с этими компьютерами возможны только через сетевые интерфейсы, не используемые в качестве точек мониторинга. При этом для серверов интеграции не настраиваются конкретные сетевые интерфейсы и IP-адреса, поскольку для внешнего подключения к серверу интеграции может использоваться любой из доступных сетевых интерфейсов и IP-адресов компьютера.

3. **Создание файлов свертки для клиентов серверов интеграции**

   На этом этапе вам нужно создать и скачать файлы свертки, в которых программа сохраняет сертификаты и ключи для подключений клиентов к серверам интеграции. Каждый файл свертки представляет собой архив, содержащий следующие данные:

   - Открытый ключ сертификата сервера интеграции.
   - Сертификат для клиентов сервера интеграции (с закрытым ключом). Этот сертификат добавляется, если на сервере интеграции включена проверка сертификатов клиентов. Сертификат и ключ сохраняются в зашифрованном виде с использованием пароля, указанного при создании файла свертки.

4. **Загрузка данных для подключения к серверам интеграции на компьютеры клиентов**

Этот этап реализуется с использованием Kaspersky Security Center. Клиентами для серверов интеграции Kaspersky Industrial CyberSecurity for Networks являются компьютеры с программным компонентом Endpoint Agent. Вам нужно загрузить сертификаты и/или ключи из файлов свертки на Сервер администрирования Kaspersky Security Center с помощью плагина управления Endpoint Agent. После этого вам нужно создать политики в Kaspersky Security Center для загрузки данных на компьютеры с Endpoint Agent. Сведения о работе с данными и создании политик см. в документации Kaspersky Endpoint Agent или в документации Kaspersky Industrial CyberSecurity for Linux Nodes.

Для каждого сервера интеграции должна быть создана как минимум одна политика, содержащая следующие данные для загрузки на компьютеры клиентов:

- Открытый ключ сертификата сервера интеграции.
- IP-адрес для подключения к серверу интеграции. Вы можете указать любой из доступных IP-адресов узла с сервером интеграции (IP-адреса можно просмотреть при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс в разделе **Параметры → Серверы подключений** на вкладке **Серверы интеграции**). По умолчанию для подключения используется порт 8081.
- Сертификат для клиентов сервера интеграции (с закрытым ключом). Этот сертификат добавляется, если на сервере интеграции включена проверка сертификатов клиентов.

5. **Включение серверов интеграции**

   Этот этап выполняется после применения политик и загрузки данных на компьютеры с Endpoint Agent. На этом этапе вам нужно включить все серверы интеграции, на которые будут передаваться данные от EPP-приложений. При включении сервера интеграции на узле активируется сервис kics4net-epp-proxy.

В результате выполнения сценария Kaspersky Industrial CyberSecurity for Networks начнет получать и обрабатывать данные от EPP-приложений.

Добавление сервера интеграции

Чтобы добавить сервер интеграции:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры → Серверы подключений**.
3. На вкладке **Серверы интеграции** откройте область деталей по ссылке **Добавить сервер интеграции с Endpoint Agent**.
4. В раскрывающемся списке **Узел** выберите узел с установленным компонентом программы (Сервером или сенсором), на который требуется добавить сервер интеграции.

   Вы можете выбрать только тот узел, на который еще не добавлен сервер интеграции.
5. При необходимости включите проверку сертификатов для аутентификации клиентов с помощью переключателя **Проверять сертификаты клиентов**.

6. Если вы включили проверку сертификатов клиентов, создайте один или несколько сертификатов для клиентов сервера интеграции. Для создания сертификата нажмите на кнопку **Создать новый сертификат**. При необходимости вы можете удалить лишние сертификаты из списка с помощью значка 🗑, который расположен справа от поля с отпечатком сертификата.

   Если вы создали несколько сертификатов клиентов, вы сможете выбирать нужный сертификат при создании файла свертки.

7. Нажмите на кнопку **Сохранить**.

Создание файла свертки для клиентов сервера интеграции

После добавления сервера интеграции или после изменения его параметров вам нужно создать и скачать файл свертки для клиентов этого сервера.

Чтобы создать новый файл свертки для клиентов сервера интеграции:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Серверы подключений**.

3. На вкладке **Серверы интеграции** выберите сервер, для клиентов которого вы хотите создать новый файл свертки.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Получить файл свертки для клиентов**.

5. Если для сервера интеграции включена проверка сертификатов клиентов, откроется окно **Генерация нового файла свертки**. Выполните следующие действия:

   a. В раскрывающемся списке **Сертификат для клиентов** выберите нужный сертификат, который будет использоваться для аутентификации клиентов сервера интеграции.

   b. Укажите пароль для доступа к выбранному сертификату. С использованием заданного пароля будет зашифрован сертификат в файле свертки коннектора.

   c. Нажмите на кнопку **Создать файл свертки**.

Сервер Kaspersky Industrial CyberSecurity for Networks сформирует новый файл свертки для клиентов выбранного сервера интеграции, после чего браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Содержимое полученного файла свертки вам нужно загрузить на компьютеры клиентов сервера интеграции. Загрузка выполняется с помощью политик Сервера администрирования Kaspersky Security Center. В политиках Kaspersky Security Center нужно указать IP-адрес для подключения к серверу интеграции (для этого вы можете использовать один из доступных IP-адресов, указанных в области деталей выбранного сервера интеграции).

Создание и настройка политик Kaspersky Security Center выполняются в процессе настройки интеграции с EPP-приложением. Сведения о настройке интеграции см. в документации Kaspersky Endpoint Agent или в документации Kaspersky Industrial CyberSecurity for Linux Nodes.

Таблица серверов интеграции

Таблица серверов интеграции отображается в разделе **Параметры → Серверы подключений** на вкладке **Серверы интеграции**. В этой таблице отображаются сведения о серверах интеграции, добавленных на узлах с установленными компонентами программы.

Таблица серверов интеграции содержит следующие сведения:

- **Имя узла** – имя узла с установленным компонентом программы.
- **IP-адреса** – список IP-адресов на всех сетевых интерфейсах узла (для серверов интеграции не настраиваются конкретные сетевые интерфейсы и IP-адреса, поскольку для внешнего подключения к серверу интеграции может использоваться любой из доступных сетевых интерфейсов и IP-адресов компьютера).
- **Запросов в секунду** – среднее количество успешно обработанных запросов, поступивших от клиентов на сервер интеграции.
- **Статус** – текущий статус сервера интеграции.
- **Проверка сертификата клиента** – признак включенной или выключенной проверки сертификатов клиентов (если проверка выключена, ячейка таблицы пустая).

Включение и выключение сервера интеграции

Серверы интеграции могут быть включены или выключены. По умолчанию после создания сервер интеграции выключен, поэтому данные от клиентов этого сервера не обрабатываются в Kaspersky Industrial CyberSecurity for Networks.

Чтобы включить или выключить сервер интеграции:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры → Серверы подключений**.
3. На вкладке **Серверы интеграции** выберите сервер, который вы хотите включить или выключить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Включить** или **Выключить**.

Изменение параметров сервера интеграции

При изменении параметров сервера интеграции вы можете заменить сертификат для самого сервера интеграции, а также включить или выключить проверку сертификатов клиентов и изменить список сертификатов для клиентов.

Чтобы изменить параметры сервера интеграции:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Серверы подключений**.
3. На вкладке **Серверы интеграции** выберите сервер, для клиентов которого вы хотите изменить параметры.

   В правой части окна веб-интерфейса появится область деталей.
4. Если вы хотите заменить (выпустить новый) сертификат для самого сервера интеграции, нажмите на кнопку **Перевыпустить сертификат**.

   После замены сертификата сервера интеграции его старый сертификат становится недействительным.
5. Если вы хотите включить или выключить проверку сертификатов для аутентификации клиентов, используйте переключатель **Проверять сертификаты клиентов**.
6. Если проверка сертификатов клиентов включена и вы хотите изменить список сертификатов для клиентов, используйте кнопку **Создать новый сертификат** и/или значок , который расположен справа от поля с отпечатком сертификата.
7. Нажмите на кнопку **Сохранить**.

Если для сервера интеграции выпущен новый сертификат или созданы новые сертификаты клиентов, вам нужно снова создать и скачать файл свертки для отправки данных об этих сертификатах на компьютеры клиентов.

Удаление сервера интеграции

Чтобы удалить сервер интеграции:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Серверы подключений**.
3. На вкладке **Серверы интеграции** выберите сервер, который вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.

Управление действиями по реагированию в Kaspersky Industrial CyberSecurity for Networks

Если в Kaspersky Industrial CyberSecurity for Networks настроена совместная работа с EPP-приложениями, вы можете вручную запускать следующие действия по реагированию на устройствах:

- **Изолировать устройство от сети**.

  После включения сетевой изоляции устройства программный компонент Endpoint Agent разрывает все активные и блокирует все новые сетевые соединения TCP/IP на устройстве, кроме следующих соединений:

  - соединения, указанные в исключениях из сетевой изоляции в Endpoint Agent;
  - соединения, инициированные службами EPP-приложения, совместимого с Endpoint Agent;
  - соединения, инициированные службами Endpoint Agent;
  - соединения, инициированные Агентом администрирования Kaspersky Security Center.

  Сетевая изоляция устройства действует до отключения сетевой изоляции в Kaspersky Industrial CyberSecurity for Networks. Если сетевая изоляция не отключена вручную, она будет отключена автоматически через 9 999 часов с момента включения.

- **Запретить запуск**.

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

  Запрет запуска выполняется с уведомлением пользователя о сработавшем правиле запрета запуска. Если пользователь устройства не закроет всплывающее уведомление, то оно закроется автоматически через 60 секунд после появления.

- **Поместить на карантин**.

  Карантин – это специальное локальное хранилище на устройстве с программным компонентом Endpoint Agent, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства.

  На компьютере с программой Kaspersky Endpoint Agent локальное хранилище карантина по умолчанию 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 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 Endpoint Agent. Восстановление объектов из карантина также выполняется на защищаемых устройствах.

Действия по реагированию позволяют предотвратить или минимизировать последствия обнаруженных угроз со стороны устройств в промышленной сети.

Возможность запуска действий по реагированию доступна для устройств с программным компонентом Endpoint Agent. При запуске действия по реагированию Kaspersky Industrial CyberSecurity for Networks передает информацию об этом в Endpoint Agent. Программный компонент Endpoint Agent выполняет полученную команду и отправляет оповещение о ее выполнении в Kaspersky Industrial CyberSecurity for Networks.

После выполнения запущенного действия по реагированию и устранения угрозы со стороны устройства вы можете запускать соответствующее обратное действие. Для перечисленных действий по реагированию предусмотрены следующие обратные действия:

- **Отключить сетевую изоляцию**.
- **Отключить запрет запуска**.
- **Восстановить из карантина**.

Kaspersky Industrial CyberSecurity for Networks регистрирует запущенные действия по реагированию и соответствующие им обратные действия. Зарегистрированные действия отображаются в разделе **События** на вкладке **Действия по реагированию**.

Вы можете запускать действия по реагированию, выбирая для этого нужные события, устройства или зарегистрированные и выполненные предыдущие действия по реагированию. Доступные для запуска действия зависят от выбранного объекта. Например, если вы выбрали устройство с программным компонентом Endpoint Agent, вам доступна только возможность управления сетевой изоляцией этого устройства. Остальные действия по реагированию доступны при других условиях (например, действия **Запретить запуск** и **Поместить на карантин** доступны при выборе события, которое связано с устройством, и для события построена цепочка развития угрозы в Endpoint Agent).

Запускать действия по реагированию и соответствующие им обратные действия могут только пользователи с ролью Администратор.

Запуск действий по реагированию при работе с событиями

Вы можете запускать действия по реагированию на устройстве, используя зарегистрированное событие, которое связано с этим устройством. Для запуска действия по реагированию событие должно быть связано с устройством, на котором есть программный компонент Endpoint Agent и завершена подготовка к получению данных от EPP-приложения.

При работе с событиями вы можете запускать следующие действия по реагированию:

- **Изолировать устройство от сети** – для любого события, если оно связано с устройством с Endpoint Agent.
- **Запретить запуск**, **Поместить на карантин** – для события по технологии EPP, если для этого события построена цепочка развития угрозы в Endpoint Agent и при этом в цепочке развития угрозы есть событие активности с объектом обнаружения угрозы и типом **Создание файла** или **Запуск процесса**. Для таких событий вы также можете запускать действие **Изолировать устройство от сети**.

Для событий, являющихся инцидентами EDR, вы можете запускать действия **Запретить запуск** и **Поместить на карантин** как для объекта обнаружения угрозы, так и для объектов, указанных в других событиях активности с типом **Создание файла** или **Запуск процесса**.

Чтобы изолировать от сети устройство, связанное с событием:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите нужное событие в разделе **События** на вкладке **События и инциденты**.

   Вы можете выбрать как событие, которое является инцидентом EDR, так и любое событие, связанное с устройством с программным компонентом Endpoint Agent.

   В правой части окна веб-интерфейса появится область деталей.

3. В области деталей откройте раскрывающийся список **Реагирование на угрозы** и выберите пункт **Изолировать устройство от сети**.

   Откроется окно с запросом подтверждения.

4. В окне запроса подтвердите запуск действия по реагированию.

Программа зарегистрирует новое действие по реагированию. Сведения о выполнении этого действия вы можете просмотреть в разделе **События** на вкладке **Действия по реагированию**.

Чтобы запретить выполнение объекта обнаружения угрозы или поместить этот объект на карантин:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите нужное событие в разделе **События** на вкладке **События и инциденты**.

   Вы можете выбрать событие, которое является инцидентом EDR и при этом в цепочке развития угрозы есть событие активности с объектом обнаружения угрозы и типом **Создание файла** или **Запуск процесса**.

   В правой части окна веб-интерфейса появится область деталей.

3. В области деталей откройте раскрывающийся список **Реагирование на угрозы** и выберите нужный пункт:

   - **Запретить запуск** – если вы хотите запретить выполнение объекта обнаружения угрозы.
   - **Поместить на карантин** – если вы хотите поместить на карантин объект обнаружения угрозы.

   Откроется окно с запросом подтверждения.

4. В окне запроса подтвердите запуск действия по реагированию.

Программа зарегистрирует новое действие по реагированию. Сведения о выполнении этого действия вы можете просмотреть в разделе **События** на вкладке **Действия по реагированию**.

*Чтобы запретить выполнение или поместить на карантин объект, указанный в любом событии активности с типом **Создание файла** или **Запуск процесса** в цепочке развития угрозы:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите нужное событие в разделе **События** на вкладке **События и инциденты**.

   Вы можете выбрать событие, которое является инцидентом EDR.

   В правой части окна веб-интерфейса появится область деталей.

3. В области деталей перейдите на вкладку **Все события активности** и выберите нужное событие активности.

   Вы можете выбрать любое событие активности с типом **Создание файла** или **Запуск процесса**. Ключевое событие активности (с объектом обнаружения угрозы) отмечено значком **Обнаружение**.

4. В открывшемся окне деталей события активности нажмите на нужную кнопку:

   - **Запретить запуск** – если вы хотите запретить выполнение объекта, указанного в выбранном событии активности.
   - **Поместить на карантин** – если вы хотите поместить на карантин объект, указанный в выбранном событии активности.

   Откроется окно с запросом подтверждения.

5. В окне запроса подтвердите запуск действия по реагированию.

Программа зарегистрирует новое действие по реагированию. Сведения о выполнении этого действия вы можете просмотреть в разделе **События** на вкладке **Действия по реагированию**.

Запуск действий по реагированию при работе с устройствами

Вы можете запускать на устройстве действие по реагированию **Изолировать устройство от сети** и соответствующее ему обратное действие **Отключить сетевую изоляцию**. Для управления сетевой изоляцией на устройстве должен быть программный компонент Endpoint Agent и должна быть завершена подготовка к получению данных от EPP-приложения.

Чтобы запустить действие по реагированию для устройства:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите устройство в разделе **Активы** на вкладке **Устройства** или в разделе **Карта сети**.

   В разделе **Карта сети** вы можете выбрать устройство для запуска действия как на карте сетевых взаимодействий, так и на топологической карте.

   В правой части окна веб-интерфейса появится область деталей.

3. В области деталей откройте раскрывающийся список **Реагирование на угрозы** и выберите нужный пункт:

   - **Изолировать устройство от сети** – если вы хотите изолировать выбранное устройство от сети.
   - **Отключить сетевую изоляцию** – если вы хотите отключить сетевую изоляцию устройства, для которого ранее было запущено действие **Изолировать устройство от сети**.

   Пункты в раскрывающемся списке **Реагирование на угрозы** доступны, если на устройстве есть программный компонент Endpoint Agent.

   Откроется окно с запросом подтверждения.

4. В окне запроса подтвердите запуск действия по реагированию.

Программа зарегистрирует новое действие по реагированию. Сведения о выполнении этого действия вы можете просмотреть в разделе **События** на вкладке **Действия по реагированию**.

Запуск действий по реагированию при работе с зарегистрированными действиями по реагированию

Если в Kaspersky Industrial CyberSecurity for Networks было запущено действие по реагированию (при работе с событиями или при работе с устройствами), вы можете запустить соответствующее обратное действие в разделе **События** на вкладке **Действия по реагированию**. Например, если для устройства запущено действие **Изолировать устройство от сети**, при работе с зарегистрированными действиями вы можете запустить действие **Отключить сетевую изоляцию** для этого устройства.

После регистрации обратного действия вы можете его использовать для следующего запуска действия по реагированию в отношении того же устройства или объекта. Например, если снова нужно изолировать устройство от сети после отключения сетевой изоляции.

Для зарегистрированных действий **Отключить запрет запуска** и **Восстановить из карантина** в качестве обратного действия вы можете запустить как действие **Запретить запуск**, так и действие **Поместить на карантин**.

Чтобы запустить действие по реагированию, обратное по отношению к зарегистрированному действию:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите нужное действие в разделе **События** на вкладке **Действия по реагированию**.

   В правой части окна веб-интерфейса появится область деталей.
3. В области деталей нажмите на кнопку запуска обратного действия. Например, если вы выбрали действие **Изолировать устройство от сети**, для запуска обратного действия нажмите на кнопку **Отключить сетевую изоляцию**.

   Откроется окно с запросом подтверждения.
4. В окне запроса подтвердите запуск действия по реагированию.

Программа зарегистрирует новое действие по реагированию.

Просмотр таблицы действий по реагированию

Таблица действий по реагированию отображается в разделе **События** на вкладке **Действия по реагированию**. В таблице представлены действия по реагированию, зарегистрированные при запуске действий по реагированию в Kaspersky Industrial CyberSecurity for Networks.

Параметры действий по реагированию отображаются в следующих столбцах таблицы:

- **ID**.

  Уникальный идентификатор зарегистрированного действия.
- **Начало**.

  Дата и время запуска действия.

- **Завершение**.

  Дата и время выполнения действия или получения подтверждения о выполнении действия. Если подтверждение о выполнении действия не поступило в программу, отображается дата и время завершения времени ожидания на выполнение действия.

- **Тип действия**.

  Тип зарегистрированного действия. Предусмотрены следующие типы:

  - **Изолировать устройство от сети**.
  - **Запретить запуск**.
  - **Поместить на карантин**.
  - **Отключить сетевую изоляцию**.
  - **Отключить запрет запуска**.
  - **Восстановить из карантина**.

- **Статус**.

  Статус выполнения действия. Предусмотрены следующие статусы:

  - **Ожидание** – команда на выполнение действия еще не отправлена.
  - **Выполняется** – действие находится в процессе выполнения.
  - **Успешно** – действие завершено успешно.
  - **Неуспешно** – при выполнении действия произошла ошибка или действие отменено из-за истечения времени на получение подтверждения.

- **Устройство**.

  Имя устройства, для которого или на котором запущено действие.

- **Заголовок события**.

  Заголовок события, если запуск действия был выполнен при работе с событием.

- **Тип объекта**.

  Тип объекта, для которого было запущено действие.

- **Объект**.

  Имя объекта, для которого запущено действие.

При просмотре таблицы действий по реагированию вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Удаление действий по реагированию

Вы можете удалять зарегистрированные действия по реагированию. При этом невозможно удалять действия со статусом *Выполняется*.

> Перед удалением действия по реагированию программа проверяет текущий статус этого действия. Однако в процессе удаления действия и после удаления действия программа не контролирует выполнение операций по этому действию на устройстве и не отменяет выполнение операций, если они уже начались. Вследствие этого действие по реагированию может быть выполнено на устройстве, даже если на момент удаления это действие было со статусом **Ожидание**.

При удалении зарегистрированного действия не отменяется результат выполненного действия на устройстве. Например, если удалено успешно завершенное действие **Изолировать устройство от сети**, сетевая изоляция устройства продолжится после удаления действия. Для отключения сетевой изоляции должно быть запущено действие **Отключить сетевую изоляцию**.

Чтобы удалить действие по реагированию:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите нужное действие в разделе **События** на вкладке **Действия по реагированию**.
3. Нажмите на кнопку **Удалить действие**.

   Откроется окно с запросом подтверждения.
4. В окне запроса подтвердите удаление действия.

Управление коннекторами

Этот раздел содержит информацию об управлении коннекторами в Kaspersky Industrial CyberSecurity for Networks. *Коннекторы* – это специальные программные модули, которые обеспечивают обмен данными с Kaspersky Industrial CyberSecurity for Networks и могут предоставлять возможности выполнения управляющих действий в самой программе или с помощью программы.

Коннекторы расширяют функциональность программы для взаимодействия со сторонними системами, в том числе с Kaspersky Security Center. В зависимости от своего функционального назначения, коннекторы могут передавать данные в сторонние системы (например, передавать события, сообщения программы и записи аудита в SIEM-систему) или обеспечивать получение данных от сторонних систем (например, для регистрации в программе событий по технологии Внешние системы). Также в программе могут использоваться коннекторы для проведения активных опросов устройств.

Для взаимодействия программы с Kaspersky Security Center используется специальный коннектор **Kaspersky Security Center Connector**. Этот коннектор создается в программе по умолчанию и не может быть удален. Для работы коннектора требуется добавить на Сервер Kaspersky Industrial CyberSecurity for Networks функциональность взаимодействия программы с Kaspersky Security Center.

Компьютеры, на которых работают программные модули коннекторов, называется *узлами размещения коннекторов*. В качестве узла размещения коннектора вы можете использовать любой компьютер, имеющий сетевой доступ к компьютеру Сервера программы (в том числе узлы с установленными компонентами программы, включая и компьютер самого Сервера).

Функциональные возможности коннектора зависят от выбранного *типа коннектора*. Вы можете выбрать нужный тип коннектора при добавлении коннектора в программу. По умолчанию в программу встроены следующие типы коннекторов:

- **Syslog**

  Этот тип коннектора предоставляет возможности отправки данных на сервер Syslog.

  При добавлении коннектора типа **Syslog** (или при изменении параметров) вам нужно настраивать не только общие параметры коннектора, но также и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Адрес сервера Syslog.
  - Порт сервера Syslog.
  - Протокол передачи данных.

- **SIEM**

  Этот тип коннектора предоставляет возможности отправки данных на сервер SIEM-системы.

  При добавлении коннектора типа **SIEM** (или при изменении параметров) вам нужно настраивать не только общие параметры коннектора, но также и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Адрес сервера SIEM-системы.
  - Порт сервера SIEM-системы.
  - Протокол передачи данных.

- **Generic**

  Этот тип коннектора предоставляет возможности подключения приложений, использующих Kaspersky Industrial CyberSecurity for Networks API.

- **Email**

  Этот тип коннектора предоставляет возможности отправки данных в сообщениях электронной почты.

  При добавлении коннектора типа **Email** (или при изменении параметров) вам нужно настраивать не только общие параметры коннектора, но также и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Адрес, указываемый в качестве отправителя сообщений электронной почты.
  - Адреса получателей сообщений электронной почты.
  - Темы сообщений электронной почты для событий, сообщений программы и записей аудита.
  - Шаблоны текстовых описаний для событий, сообщений программы, записей аудита, описаний сетевых взаимодействий и для всего письма с уведомлениями. Шаблоны составляются с использованием переменных.
  - Тема и текст письма для сообщения электронной почты о достижении максимального количества отправленных уведомлений.
  - Максимальное количество отправляемых сообщений электронной почты в сутки.
  - Максимальное количество уведомлений в каждом сообщении. Определяет максимальное количество зарегистрированных уведомлений одного типа (событий, сообщений программы или записей аудита), которые можно поместить в одно сообщение электронной почты. Если зарегистрированных уведомлений больше, то формируется дополнительное сообщение электронной почты (в пределах суточного ограничения).

- **Active poll**

  Этот тип коннектора предоставляет возможности активного опроса устройств в рамках заданий контроля конфигураций и заданий активных опросов.

  При добавлении коннектора типа **Active poll** (или при изменении параметров) вам нужно настраивать не только общие параметры коннектора, но также и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Методы проведения активных опросов, которые будут доступны пользователю программы при использовании коннектора.
  - Диапазоны разрешенных и запрещенных IP-адресов устройств, по которым будет разрешено и запрещено проведение активных опросов. Адрес `0.0.0.0` соответствует всем возможным IP-адресам. Если какой-либо адрес входит в диапазон как разрешенных, так и запрещенных IP-адресов, то Kaspersky Industrial CyberSecurity for Networks отнесет его к запрещенным IP-адресам.
  - Имена адресных пространств, для устройств которых будет разрешено проведение активных опросов. Если требуется, вы можете выбрать адресные пространства для IP-адресов в поле **Адресное пространство L3** и для MAC-адресов в поле **Адресное пространство L2**.

    При выборе адресного пространства, отличающегося от адресного пространства **Default**, вам нужно добавить новое правило для этого адресного пространства (или изменить имеющееся правило). В правиле должен быть указан коннектор, для которого выбрано это адресное пространство. Настройка параметров правил выполняется при изменении адресного пространства.

- **KUMA**

  Этот тип коннектора предоставляет возможности интеграции с программным решением Kaspersky Unified Monitoring and Analysis Platform (далее также KUMA). Программные модули для коннекторов данного типа поставляются отдельно от Kaspersky Industrial CyberSecurity for Networks. С помощью коннектора данного типа вы можете отправлять в KUMA сведения об устройствах и рисках, а также применять в KUMA команды на изменение статусов устройств. После добавления коннектора требуется настроить интеграцию в KUMA (создать подключение к Kaspersky Industrial CyberSecurity for Networks). Взаимодействие коннектора KUMA с Сервером выполняется с использованием Kaspersky Industrial CyberSecurity for Networks API.

  Коннектор KUMA обеспечивает интеграцию в части отправки сведений об устройствах и рисках и применения команд на изменение статусов устройств. Для отправки событий в KUMA вы можете добавить в Kaspersky Industrial CyberSecurity for Networks коннектор типа **Syslog** или **SIEM** и указать для этого коннектора данные для подключения к серверу KUMA. После добавления коннектора требуется настроить коллектор на стороне KUMA.

- **Cisco Switch**

  Этот тип коннектора предоставляет возможности автоматического управления сетевым доступом устройств с использованием сетевых коммутаторов Cisco.

  При добавлении коннектора типа **Cisco Switch** (или при изменении параметров) вам нужно настраивать не только общие параметры коннектора, но также и дополнительные параметры, сгруппированные в блоке **Детали**:

  - Имя коммутатора, которое будет указываться в событиях программы о выполненных действиях с помощью коннектора.
  - Адресная информация для подключения коннектора к сетевому коммутатору: IP-адрес и SSH-порт.
  - Учетные данные для установки SSH-соединения с сетевым коммутатором.
  - Открытый ключ, используемый для проверки совпадения с полученным открытым ключом сетевого коммутатора перед установкой SSH-соединения с целью защиты от подмены этого устройства в сети (если значение пустое, то проверка не выполняется).
  - Используемый метод для ограничения сетевого доступа устройств. Предусмотрены методы создания правил блокировки в списках контроля доступа коммутатора по MAC-адресам (MAC ACL), по IP-адресам (IP ACL), а также с отключением Ethernet-портов, к которым подключены устройства.

    Для использования метода отключения Ethernet-портов вам нужно настроить конфигурацию подключений к сетевому коммутатору таким образом, чтобы исключить соединение нескольких устройств через один порт. Иначе при отключении Ethernet-порта для блокировки одного устройства, сетевой доступ будет также заблокирован для всех устройств, которые соединены с сетью через этот порт.

  - Параметр сброса правил блокировки при изменении метода ограничения сетевого доступа (если параметр включен, при изменении метода сбрасываются правила, которые ранее были заданы для блокировки устройств).
  - Параметр исключения сетевых устройств для применения метода ограничения сетевого доступа (если параметр включен, метод не применяется к устройствам категорий **Сетевое устройство**, **Брандмауэр**, **Коммутатор**, **Виртуальный коммутатор**, **Маршрутизатор**, **Виртуальный маршрутизатор**, **Wi-Fi**).
  - Параметр применения правил блокировки только к новым устройствам (если параметр включен, метод применяется только к тем неразрешенным устройствам, для которых зарегистрировано событие

обнаружения нового устройства с кодом типа события 4000005003).

- Длительность интервала времени между запросами данных о наличии устройств со статусами *Разрешенное* и *Неразрешенное* в таблице устройств.

- Параметр отправки уведомлений о заблокированных устройствах при перезапуске коннектора (если параметр включен, после включения или перезапуска коннектора на Сервер отправляется список устройств, для которых ранее были применены ограничения сетевого доступа).

При необходимости в программу можно добавлять другие типы коннекторов, которые будут обеспечивать обмен данными или предоставлять возможности выполнения управляющих действий при взаимодействии программы с другими сторонними системами.

Для соединений коннекторов с Сервером используются определенные порты и протоколы.

Подключение сторонней системы через коннектор выполняется от имени одного из пользователей программы. Для каждого коннектора рекомендуется использовать отдельную учетную запись пользователя. За счет этого вам будет удобнее анализировать действия, которые выполнялись через коннекторы, по записям аудита.

Таблицы коннекторов и типов коннекторов отображаются в разделе **Параметры** → **Коннекторы** веб-интерфейса программы. Управлять коннекторами и типами коннекторов могут только пользователи с ролью Администратор.

Максимальное количество коннекторов в программе – 20. Максимальное количество типов коннекторов – 100.

Об управляемых и неуправляемых коннекторах

В программе могут использоваться управляемые и неуправляемые коннекторы.

Коннектор является *управляемым*, если для его программных модулей доступны функции автоматической регистрации и запуска после добавления коннектора, а также функции управления этими модулями при включении и выключении коннектора и при его удалении. Узлами размещения управляемых коннекторов могут быть только узлы с установленными компонентами программы.

Неуправляемый коннектор не предоставляет функции управляемого коннектора. Регистрацию такого коннектора, а также запуск, остановку и удаление его программных модулей требуется выполнять вручную на узле размещения коннектора. При включении и выключении неуправляемого коннектора программа соответственно разрешает и запрещает взаимодействие с коннектором на стороне Сервера.

Безопасность соединений коннекторов с Сервером программы обеспечивается с использованием сертификатов. Сертификаты для коннекторов создаются при добавлении коннекторов в программу. Для программных модулей управляемых коннекторов программа автоматически передает созданные сертификаты. При добавлении неуправляемого коннектора (или при добавлении управляемого коннектора с включенным режимом игнорирования функций управляемого коннектора) сертификат для программных модулей этого коннектора требуется загрузить вручную с помощью файла свертки. При необходимости заменить (выпустить новый) сертификат для такого коннектора вам нужно создать новый файл свертки и использовать этот файл для загрузки нового сертификата. Замена сертификатов управляемых коннекторов возможна только путем удаления и повторного добавления этих коннекторов.

Об отправке событий, сообщений программы и записей аудита в сторонние системы

Вы можете настроить отправку событий, сообщений программы или записей аудита (далее также "зарегистрированные уведомления") в стороннюю систему с помощью коннекторов. Для типов коннекторов **Syslog**, **SIEM**, **Email** и **Kaspersky Security Center Connector** возможность отправки зарегистрированных уведомлений включена по умолчанию. Для типа коннектора **KUMA** возможность отправки зарегистрированных уведомлений доступна при наличии установленных программных модулей. При использовании других типов коннекторов, добавленных в программу, эта возможность доступна в зависимости от заданных параметров для этих типов коннекторов.

Параметры отправки зарегистрированных уведомлений настраиваются для каждого коннектора. При настройке типов событий вы можете выбрать нужные типы событий для передачи через коннекторы. При создании коннектора или при изменении его параметров вы можете включить или выключить отправку всех сообщений программы и всех записей аудита через этот коннектор.

Некоторые типы коннекторов предоставляют возможность ограничения объема передаваемых данных. Ограничение действует в течение суток, начиная с нуля часов в часовом поясе Сервера. Вы можете задать ограничение объема передаваемых данных для следующих системных типов коннекторов:

- **Email**. Для этого типа коннектора можно задать максимальное количество сообщений электронной почты о новых зарегистрированных уведомлениях и максимальное количество зарегистрированных уведомлений в каждом сообщении. Если отправлено максимальное количество сообщений электронной почты, получателям отправляется ещё одно сообщение о превышении максимального количества. После этого новые сообщения не будут отправляться до конца текущих суток.

- **Kaspersky Security Center Connector**. Для этого типа коннектора можно задать максимальное количество передаваемых зарегистрированных уведомлений. Если зарегистрированных уведомлений больше, в Kaspersky Security Center не отправляются остальные уведомления, регистрируемые до конца текущих суток.

Передача событий, содержащих сведения о нескольких сетевых взаимодействиях, выполняется со следующей особенностью. При отправке через коннектор **Kaspersky Security Center Connector** каждое такое событие учитывается как один элемент. Однако в процессе отправки событие преобразуется в несколько зарегистрированных уведомлений: по одному уведомлению на каждое сетевое взаимодействие. Поэтому список зарегистрированных уведомлений для коннектора **Kaspersky Security Center Connector** может содержать больше уведомлений, чем задано параметром, который определяет максимальное количество уведомлений.

Содержание и порядок сведений о зарегистрированных уведомлениях, которые передаются через коннекторы типов **Syslog** и **SIEM**, могут отличаться в этих системах от содержания и порядка сведений, отображаемых на страницах веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Сообщения электронной почты, отправляемые через коннектор **Email**, формируются раздельно для каждого типа зарегистрированных уведомлений. То есть для отправки событий, сообщений программы и записей аудита формируются разные сообщения электронной почты.

Об автоматическом управлении сетевым доступом устройств с помощью коннекторов типа Cisco Switch

Вы можете настроить автоматическое управление сетевым доступом устройств с помощью коннекторов типа **Cisco Switch**. Коннекторы этого типа соединяются с сетевыми коммутаторами и отправляют на эти коммутаторы команды, добавляющие или удаляющие правила блокировки (ограничения) сетевого доступа для устройств, которые подключены к коммутаторам.

Управление сетевым доступом устройств осуществляется в зависимости от их статусов. Коннектор создает на сетевом коммутаторе правила блокировки для устройств со статусом *Неразрешенное* и удаляет такие правила после присвоения устройствам статуса *Разрешенное*.

Каждый коннектор может устанавливать соединение только с одним сетевым коммутатором.

Ограничение сетевого доступа с помощью коннектора типа **Cisco Switch** выполняется для тех устройств, в сведениях о которых указаны их MAC-адреса. Также эти MAC-адреса должны храниться в ARP-таблице сетевого коммутатора. То есть, устройства с этими MAC-адресами должны быть подключены к сетевому коммутатору, с которым соединяется коннектор.

Коннектор может использовать различные методы для ограничения сетевого доступа устройств. Предусмотрены методы создания правил блокировки в списках контроля доступа коммутатора по MAC-адресам (MAC ACL), по IP-адресам (IP ACL), а также с отключением Ethernet-портов, к которым подключены устройства.

Для использования метода отключения Ethernet-портов вам нужно настроить конфигурацию подключений к сетевому коммутатору таким образом, чтобы исключить соединение нескольких устройств через один порт. Иначе при отключении Ethernet-порта для блокировки одного устройства сетевой доступ будет также заблокирован для всех устройств, которые соединены с сетью через этот порт.

Для минимизации рисков влияния коннектора на сетевую доступность устройств, правомерно участвующих в технологическом процессе, вы можете включить следующие параметры при настройке коннектора:

- Параметр исключения сетевых устройств для применения метода ограничения сетевого доступа (если параметр включен, метод не применяется к устройствам категорий **Сетевое устройство**, **Брандмауэр**, **Коммутатор**, **Виртуальный коммутатор**, **Маршрутизатор**, **Виртуальный маршрутизатор**, **Wi-Fi**).

- Параметр применения правил блокировки только к новым устройствам (если параметр включен, метод применяется только к тем неразрешенным устройствам, для которых зарегистрировано событие обнаружения нового устройства с кодом типа события 4000005003).

Коннектор соединяется с сетевым коммутатором путем установки SSH-соединения. Учетные данные для установки SSH-соединения указываются при настройке параметров коннектора и сохраняются в нем. Эти учетные данные, представляющие идентификационную и аутентификационную информацию, требуется защищать от компрометации. Для защиты от компрометации, которая возможна в случае подмены сетевого коммутатора, в коннекторе предусмотрена функция проверки сохраненного открытого ключа коммутатора и полученного открытого ключа. Передача идентификационной и аутентификационной информации на сетевой коммутатор происходит после проверки идентичности полученного открытого ключа и открытого ключа, сохраненного в коннекторе.

В процессе работы коннектор регистрирует в программе события по результатам выполненных действий. События регистрируются по технологии Внешние системы. Предусмотрены события со следующими заголовками:

- `Для коммутатора <имя коммутатора> сброшены правила блокировки устройств`

  Это событие регистрируется, если при изменении метода ограничения сетевого доступа в коннекторе сброшены правила, которые ранее были заданы для блокировки устройств.

- `Обновлены сведения об устройстве <имя устройства> с адресом <MAC-адрес устройства> по данным от коммутатора <имя коммутатора>`

  Это событие регистрируется, если от сетевого коммутатора получена информация о подключении устройства к определенному порту.

- `Добавлено правило блокировки устройства <имя устройства> на коммутаторе <имя коммутатора>`

  Это событие регистрируется, если ограничен сетевой доступ неразрешенного устройства.

- `Удалено правило блокировки устройства <имя устройства> на коммутаторе <имя коммутатора>`

  Это событие регистрируется, если снято ограничение сетевого доступа устройства.

- `На коммутаторе <имя коммутатора> есть правила блокировки устройств, добавленные ранее`

  Это событие регистрируется, если после включения или перезапуска коннектора найдены устройства, для которых ранее были применены ограничения сетевого доступа.

- `Установлено SSH-соединение с коммутатором <имя коммутатора> без проверки открытого ключа`

  Это событие регистрируется, если коннектор установил SSH-соединение с сетевым коммутатором, однако проверка полученного открытого ключа коммутатора не выполнена. В этом случае вам нужно убедиться в отсутствии подменного устройства в сети и после этого сохранить в параметрах коннектора полученный открытый ключ.

- `Обнаружено несовпадение открытого ключа коммутатора <имя коммутатора>`

  Это событие регистрируется, если при проверке полученного открытого ключа сетевого коммутатора обнаружено несовпадение со значением, сохраненным в параметрах коннектора. Из-за этого SSH-соединение с коммутатором не установлено. В этом случае вам нужно убедиться как в отсутствии подменного устройства в сети, так и в действительном изменении открытого ключа коммутатора и после этого сохранить в параметрах коннектора полученный открытый ключ.

- `Отказ в установке SSH-соединения с коммутатором <имя коммутатора>: неверные учетные данные`

  Это событие регистрируется, если коннектору не удалось установить SSH-соединение с коммутатором из-за неверно указанных учетных данных в параметрах коннектора (имя пользователя и/или пароль).

- `На коммутаторе <имя коммутатора> не выполнено действие для привилегированного режима: неверный пароль`

  Это событие регистрируется, если коннектору недоступны функции привилегированного режима для выполнения действий по добавлению и удалению правил блокировки устройств на коммутаторе. В этом случае вам нужно ввести правильный пароль привилегированного режима в параметрах коннектора.

Добавление коннектора

Вы можете добавить в программу коннектор на основе одного из типов коннекторов из числа доступных в программе.

Если вы хотите использовать все возможности интеграции с программным решением KUMA, вам нужно добавить коннекторы двух типов. Для отправки в KUMA сведений об устройствах и рисках и применения команд на изменение статусов устройств вам нужно добавить коннектор типа **KUMA**. Для отправки событий Kaspersky Industrial CyberSecurity for Networks вам нужно добавить коннектор типа **Syslog** или **SIEM** и указать для этого коннектора данные для подключения к серверу KUMA.

Перед добавлением коннектора рекомендуется создать отдельную учетную запись пользователя, под которым сторонняя система будет подключаться к программе.

Чтобы добавить коннектор:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. На вкладке **Коннекторы** откройте область деталей по кнопке **Добавить коннектор**.
4. Настройте общие параметры коннектора:
   a. Выберите нужный тип коннектора и введите имя коннектора.
   b. Если вы хотите добавить неуправляемый коннектор (или коннектор с включенным режимом игнорирования функций управляемого коннектора), введите пароль для доступа к сертификату коннектора.

      С использованием заданного пароля будет зашифрован сертификат в файле свертки коннектора.
   c. Укажите адрес Сервера программы.

      По указанному адресу коннектор будет подключаться к Серверу.
   d. Укажите узел размещения коннектора:
      - Если вы хотите добавить управляемый коннектор, в качестве узла размещения коннектора вы можете указать один из узлов с установленными компонентами программы.
      - Если вы хотите добавить неуправляемый коннектор, вам нужно ввести IP-адрес компьютера, на котором будут работать программные модули коннектора.
   e. Выберите пользователя, под которым сторонняя система будет подключаться к программе через коннектор. Требуется указать имя одного из пользователей программы.
5. В блоке **Детали** укажите дополнительные параметры в зависимости от типа коннектора. Блок **Детали** отсутствует в области деталей, если тип коннектора не предусматривает настройку дополнительных параметров.

6. Если тип коннектора предусматривает возможность передачи записей аудита и сообщений программы, включите или выключите отправку этих данных с помощью соответствующих флажков.

7. При необходимости введите описание коннектора.

8. Нажмите на кнопку **Сохранить**.

   Новый коннектор появится в таблице коннекторов.

   Если добавлен неуправляемый коннектор, Сервер сформирует файл свертки для нового коннектора, после чего браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла. Содержимое полученного файла свертки вам нужно загрузить в приложение, которое будет использовать коннектор.

9. Для неуправляемого коннектора создайте службу на узле размещения этого коннектора. Для этого вы можете использовать соответствующий скрипт:

   - Если добавлен коннектор типа **Syslog**, **SIEM**, **Generic** или **Email** – для создания службы вы можете использовать скрипт default_connectors_registrar.py, который находится на компьютере узла с установленными компонентами программы в директории /opt/kaspersky/kics4net-connectors/libexec/. Для запуска скрипта в консоли операционной системы введите команду:

     ```
     sudo python3 default_connectors_registrar.py create
     ```

     После запуска последовательно укажите данные о коннекторе по запросам скрипта: имя коннектора, путь к файлу свертки, пароль для доступа к сертификату коннектора.

   - Если добавлен коннектор типа **Active poll** – для создания службы вы можете использовать скрипт register.py, который находится на компьютере узла с установленными компонентами программы в директории /opt/kaspersky/kics4net-apm/src/. Для запуска скрипта в консоли операционной системы введите команду:

     ```
     sudo python3 register.py -p "<полный путь к файлу свертки>"
     ```

Просмотр таблицы коннекторов

Таблица коннекторов отображается в разделе **Параметры** → **Коннекторы** на вкладке **Коннекторы**.

Параметры коннекторов отображаются в следующих столбцах таблицы:

- **Имя**.

  Заданное имя коннектора.

- **ID коннектора**.

  Идентификатор, присвоенный коннектору при его создании.

- **Включен**.

  Признак готовности Сервера к взаимодействию с программными модулями коннектора. Если параметр имеет значение **Нет**, Сервер не принимает запросы от программных модулей коннектора.

- **Статус**.

  Статус работы программных модулей коннектора. Предусмотрены следующие статусы:

  - **Ожидает регистрации** – после добавления неуправляемого коннектора или после создания нового файла свертки для неуправляемого коннектора подключение через этот коннектор еще не выполнялось.
  - **Переключение** – происходит переключение режима работы программных модулей коннектора из статуса **Не работает** в статус **Работает** или обратно.
  - **Не работает** – Сервер не принимает запросы от программных модулей коннектора. Если коннектор управляемый, для его программных модулей отправлена команда остановки работы.
  - **Работает** – выполнено успешное подключение через коннектор с использованием сертификата, созданного для этого коннектора.
  - **Ошибка** – возникла ошибка при попытке выполнения действий с программными модулями коннектора.

- **Тип**.

  Значок и название типа коннектора.

- **Последнее подключение**.

  Дата и время последнего подключения через коннектор.

- **Управляемый**.

  Признак управляемого коннектора. Если параметр имеет значение **Нет**, коннектор является неуправляемым или для коннектора включен режим игнорирования функций управляемого коннектора.

- **Изменен**.

  Дата и время последнего изменения параметров коннектора.

- **Описание**.

  Заданное описание коннектора.

При просмотре таблицы коннекторов вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Включение и выключение коннектора

Если вы хотите временно запретить подключение программных модулей коннектора к Серверу, вы можете выключить этот коннектор. Для возобновления подключения вам потребуется включить коннектор.

Чтобы включить или выключить коннектор:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. На вкладке **Коннекторы** выберите коннектор, который вы хотите включить или выключить.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на нужную кнопку: **Включить** или **Выключить**.

   Откроется окно с запросом подтверждения.

5. В окне запроса нажмите на кнопку **OK**.

Изменение параметров коннектора

Чтобы изменить параметры коннектора:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Коннекторы**.

3. На вкладке **Коннекторы** выберите нужный коннектор.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.

5. Измените параметры аналогично процедуре добавления коннектора.

   Для изменения доступны не все параметры. Например, невозможно изменить выбранный тип коннектора.

6. Нажмите на кнопку **Сохранить**.

Изменения отобразятся в соответствующих столбцах таблицы коннекторов. Если вы изменили имя коннектора, новое имя отобразится в заголовке столбца в таблице типов событий.

При изменении некоторых параметров неуправляемого коннектора Сервер сформирует новый файл свертки для коннектора (например, если вы изменили адрес сервера для коннектора **Syslog**, у которого включен режим игнорирования функций управляемого коннектора). В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла свертки. Содержимое нового файла свертки вам нужно загрузить в приложение, которое использует коннектор. Иначе новое подключение через коннектор для этого приложения будет невозможно.

Создание нового файла свертки для коннектора

При добавлении неуправляемого коннектора автоматически создается файл свертки для этого коннектора. При необходимости вы можете создать для коннектора новый файл свертки (например, если сертификат из предыдущего файла свертки был скомпрометирован).

После создания нового файла свертки сертификат из старого файла свертки становится недействительным. Поэтому для следующего подключения сторонней системы через этот коннектор вам потребуется использовать новый файл свертки.

Чтобы создать новый файл свертки для неуправляемого коннектора:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Коннекторы**.

3. На вкладке **Коннекторы** выберите неуправляемый коннектор, для которого вы хотите создать новый файл свертки.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Получить новый файл свертки**.

   Откроется окно **Генерация нового файла свертки**.

5. Укажите параметры для создания файла свертки:

   - Имя пользователя, под которым сторонняя система будет подключаться к программе через коннектор. Требуется указать имя одного из пользователей программы.

     Рекомендуется указать имя пользователя, которое было указано при добавлении коннектора. Если требуется указать имя другого пользователя, рекомендуется выбрать из учетных записей пользователей программы того пользователя, имя которого не указано для других коннекторов и не используется для подключения к Серверу через веб-интерфейс.

   - Адрес узла, на котором работают программные модули коннектора.

   - Пароль для доступа к сертификату коннектора. С использованием заданного пароля будет зашифрован сертификат в файле свертки коннектора.

6. Нажмите на кнопку **Создать файл свертки**.

Сервер сформирует новый файл свертки для выбранного коннектора, после чего браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла. Содержимое полученного файла свертки вам нужно загрузить в приложение, которое использует коннектор. Иначе новое подключение через коннектор для этого приложения будет невозможно.

Удаление коннектора

При удалении управляемого коннектора его программные модули автоматически останавливаются и удаляются на узле размещения коннектора.

Если вы удаляете неуправляемый коннектор (или коннектор, для которого включен режим игнорирования функций управляемого коннектора), перед удалением коннектора вам нужно вручную остановить и удалить его программные модули.

Чтобы подготовить неуправляемый коннектор к удалению,

на узле размещения коннектора выполните соответствующее действие:

- Для коннектора типа **Syslog**, **SIEM**, **Generic** или **Email** – используйте скрипт default_connectors_registrar.py, который находится на компьютере узла с установленными компонентами программы в директории /opt/kaspersky/kics4net-connectors/libexec/. Для запуска скрипта в консоли операционной системы введите команду:

```
sudo python3 default_connectors_registrar.py delete
```

После запуска укажите имя коннектора по запросу скрипта.

- Для коннектора типа **Active poll** – в консоли операционной системы введите команду:

```
sudo systemctl disable kics4net-apm
```

Чтобы удалить коннектор:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. На вкладке **Коннекторы** выберите коннектор, который вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление выбранного коннектора.

Добавление и удаление типов коннекторов

Типы коннекторов задают для коннекторов доступные функциональные возможности и реализуемую функциональность в рамках этих возможностей. Вы можете использовать как встроенные в программу типы коннекторов, поставщиком которых является "Лаборатория Касперского", так и дополнительные типы коннекторов от любых других поставщиков.

Для добавления типа коннектора в программу поставщик должен предоставить вам следующие файлы:

- файлы для установки программных модулей коннекторов;
- файл описания типа коннектора.

Если тип коннектора от стороннего поставщика позволяет сохранять в коннекторах учетные данные пользователей для доступа к сторонней системе, рекомендуется принять меры для защиты этих учетных данных от компрометации. Для минимизации рисков в случае компрометации учетных данных рекомендуется предоставлять минимально необходимые права для этих учетных записей (достаточные только для подключений через коннекторы).

Файлы для встроенных типов коннекторов входят в комплект поставки программы. Действия для добавления типов коннекторов с использованием этих файлов выполняются автоматически при установке компонентов программы. Если по каким-либо причинам встроенные типы коннекторов были удалены из программы, вы можете использовать файлы из комплекта поставки для повторного добавления этих типов коннекторов.

Таблица типов коннекторов отображается в разделе **Параметры** → **Коннекторы** на вкладке **Типы коннекторов**.

Просмотр таблицы типов коннекторов

Таблица типов коннекторов отображается в разделе **Параметры** → **Коннекторы** на вкладке **Типы коннекторов**.

Параметры коннекторов отображаются в следующих столбцах таблицы:

- **Название**.

  Название типа коннектора, заданное поставщиком.

- **Поставщик**.

  Название поставщика типа коннектора.

- **Версия**.

  Номер версии типа коннектора.

- **Код**.

  Уникальный номер типа коннектора.

- **Возможности**.

  Список функциональных возможностей, которые будут доступны для коннекторов данного типа.

При просмотре таблицы типов коннекторов вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Добавление типа коннектора

Вы можете добавить в программу тип коннектора с помощью файла описания, предоставленного поставщиком типа коннектора. Файл описания типа коннектора должен быть упакован в ZIP-архив.

Установку программных модулей коннекторов для добавляемого типа коннектора требуется выполнить вручную с помощью файлов, предоставленных поставщиком типа коннектора. Программные модули нужно установить на тех компьютерах, которые будут указаны в качестве узлов размещения коннекторов при добавлении коннекторов.

Чтобы добавить тип коннектора:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. На вкладке **Типы коннекторов** откройте область деталей по ссылке **Добавить тип коннектора**.
4. Укажите файл описания типа коннектора с помощью кнопки **Обзор**.
5. Нажмите на кнопку **Сохранить**.

Новый тип коннектора появится в таблице коннекторов.

Удаление типа коннектора

При удалении типа коннектора в программе удаляются сведения об этом типе коннектора, а также все коннекторы, которые были добавлены с использованием этого типа.

Чтобы удалить тип коннектора:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. На вкладке **Типы коннекторов** выберите тип коннектора, который вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление выбранного типа коннектора.
6. Если в программе есть коннекторы данного типа, подтвердите также и удаление этих коннекторов.

Управление заданиями для аудита безопасности

С помощью Kaspersky Industrial CyberSecurity for Networks вы можете проводить аудит безопасности контролируемых устройств. Аудит безопасности выполняется по заданиям, сформированным для выбранных устройств. Задания для аудита безопасности могут быть следующих типов:

- Аудит настроек и уязвимостей.

  Задания аудита настроек и уязвимостей позволяют оценивать соответствие устройств стандартам безопасности и выполнять другие проверки (например, поиск уязвимостей или определение установленного программного обеспечения на устройствах).

- Контроль конфигураций.

  Задания контроля конфигураций позволяют получать и сохранять в программе детальную информацию о конфигурациях устройств, а также с помощью программы сравнивать изменения в конфигурациях устройств.

- Активный опрос.

  Задания активного опроса позволяют получать наиболее точную и полную информацию об устройствах и их конфигурациях непосредственно от самих устройств.

Управлять заданиями для аудита безопасности могут только пользователи с ролью Администратор.

Для использования функциональности аудита безопасности вам нужно учитывать следующие особенности и ограничения:

- Функциональность доступна после добавления лицензионного ключа.

- Узлы с установленными компонентами программы, через которые выполняются сканирования устройств в рамках заданий для аудита безопасности, должны иметь сетевой доступ к устройствам для отправки и получения данных. Для обеспечения сетевого доступа к устройствам на компьютере узла должен быть сетевой интерфейс с подключением к сети этих устройств. Для этих целей не могут использоваться сетевые интерфейсы точек мониторинга, если на эти сетевые интерфейсы поступает зеркалированный трафик промышленной сети (например, от SPAN-портов сетевых коммутаторов).

Задания аудита настроек и уязвимостей

Вы можете использовать задания аудита настроек и уязвимостей для проведения аудита безопасности контролируемых устройств. Для каждого задания вы можете запускать выполнение вручную или настроить расписание автоматического запуска.

При запуске задания программа инициирует сканирования устройств, входящих в это задание. Результаты выполнения задания вы можете получать по электронной почте или просматривать и загружать нужные данные в веб-интерфейсе программы. По результатам заданий и сканирований программа может выполнять следующие действия:

- Формировать отчеты со сведениями о результатах.

  Программа формирует отчеты в виде файлов в формате PDF. Если в параметрах задания включена отправка отчетов по электронной почте, программа автоматически формирует отчеты о каждом выполнении задания и отправляет эти отчеты указанным адресатам. При необходимости вы можете вручную сформировать отчет для завершенного запуска задания или отдельного сканирования устройства и затем экспортировать отчет в файл.

- Регистрировать обнаруженные риски категории Уязвимость.

  Для рисков, регистрируемых по результатам заданий аудита настроек и уязвимостей, программа указывает источник уязвимости **OVAL**. Такие риски регистрируются программой, если в параметрах задания включена регистрация обнаруженных уязвимостей. При этом риски с указанным источником уязвимости **OVAL** регистрируются и обрабатываются независимо от рисков, для которых указаны другие источники уязвимостей. Таким образом, в таблице рисков могут отображаться риски с одним и тем же CVE-идентификатором (или идентификатором другой базы уязвимостей), но с различными источниками уязвимостей.

В заданиях аудита настроек и уязвимостей должны быть указаны правила, используемые для проведения проверок. Правила могут быть написаны на языке OVAL или на языке XCCDF с использованием OVAL-определений.

Сканирования устройств в рамках задания можно выполнять одним из следующих способов опроса устройств:

- **Локальный агент**.

  Вы можете использовать этот способ, если на устройствах, выбранных для задания, есть программный компонент Endpoint Agent и настроена интеграция EPP-приложения с Kaspersky Industrial CyberSecurity for Networks. Этот способ применяется для сканирования с помощью Endpoint Agent на каждом устройстве.

- **Удаленное подключение**.

  Этот способ нужно использовать, если на устройствах, выбранных для задания, нет программного компонента Endpoint Agent, но есть возможность подключиться к этим устройствам по протоколам, которые обеспечивают безопасное управление и передачу данных. Для этого способа требуется указать в задании один из узлов с установленными компонентами программы, с которого будут выполняться подключения к устройствам. Также требуется указать учетные данные для удаленных подключений (учетные данные хранятся в программе в виде секретов).

На устройствах под управлением операционных систем семейства Linux сканирования выполняются с использованием команд для запуска стандартных утилит диагностики Linux-устройств.

Вы можете управлять заданиями аудита настроек и уязвимостей в разделе **Аудит безопасности** на вкладке **Аудит настроек и уязвимостей**. Если сканирования устройств будут выполняться способом **Удаленное подключение**, вы можете создать секреты с нужными учетными данными в разделе **Параметры** → **Секреты**.

После запуска заданий и завершения сканирований на устройствах вы можете получать сведения о выполненных проверках.

Добавление задания аудита настроек и уязвимостей

Для имеющихся наборов правил аудита настроек и уязвимостей вы можете добавлять задания, по которым программа будет выполнять проверки на устройствах.

Добавлять задания аудита настроек и уязвимостей могут только пользователи с ролью Администратор.

Настройка задания аудита настроек и уязвимостей выполняется с помощью мастера. Мастер позволяет пошагово выполнить настройку всех нужных параметров задания. После завершения настройки вы можете дождаться запуска сканирований на устройствах по расписанию или запустить задание вручную.

При добавлении задания аудита настроек и уязвимостей вы можете вызвать мастер настройки следующими способами:

- Добавление задания для выбранного набора правил. Для этого:

  1. Выберите раздел **Аудит безопасности**.

  2. На вкладке **Наборы правил** выберите набор, для которого вы хотите добавить задание аудита настроек и уязвимостей.

  3. Нажмите на кнопку **Добавить задание**.

  В параметрах мастера настройки в качестве значения по умолчанию будет задан выбранный набор правил.

- Добавление задания с изначально пустыми значениями параметров. Для этого:

  1. Выберите раздел **Аудит безопасности**.

  2. На вкладке **Аудит настроек и уязвимостей** нажмите на кнопку **Добавить задание**.

  В параметрах мастера настройки не будут заданы значения по умолчанию.

- Добавление задания на основе имеющегося задания. Для этого:

  1. Выберите раздел **Аудит безопасности**.

  2. На вкладке **Аудит настроек и уязвимостей** выберите задание, на основе которого вы хотите добавить новое задание аудита настроек и уязвимостей.

  3. Нажмите на кнопку **Копировать**.

  В параметрах мастера настройки в качестве значений по умолчанию будут заданы значения параметров имеющегося задания.

- Добавление задания для выбранных устройств. Для этого:

  1. Выберите раздел **Активы**.

  2. На вкладке **Устройства** выберите устройства, для которых вы хотите добавить задание аудита настроек и уязвимостей.

  3. В панели инструментов, которая расположена над таблицей устройств, откройте раскрывающийся список **Создать задание** и выберите пункт **Аудит настроек и уязвимостей**.

  В параметрах мастера настройки по умолчанию будет сформирован список устройств, состоящий из выбранных устройств.

Чтобы настроить параметры задания в окне мастера настройки:

1. В разделе **Выбор правил** выполните следующие действия:

   a. Выберите нужный набор правил для задания (недоступно при изменении задания).

   b. Укажите профиль выбранного набора.

   c. Выберите правила, по которым будут выполняться проверки, и при необходимости укажите нужные значения переменных.

2. В разделе **Выбор устройств** сформируйте список устройств, на которых будут выполняться сканирования при выполнении задания. Выберите для задания не более 1000 устройств.

   Вы можете формировать список устройств с помощью кнопок **Добавить в задание** и **Удалить из задания**. Для добавления устройств программа открывает окно с таблицей устройств для выбора. Вы можете выполнять фильтрацию и сортировку таблицы для отображения нужных устройств.

3. В разделе **Настройка задания** настройте остальные параметры задания:

   a. Введите имя и описание задания.

      Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя задания должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

      Имя задания должно содержать не более 256 символов. Описание задания должно содержать не более 4096 символов.

   b. Выберите один из следующих способов опроса устройств:

      - **Локальный агент**.

        Вы можете использовать этот способ, если на устройствах, выбранных для задания, есть программный компонент Endpoint Agent и настроена интеграция EPP-приложения с Kaspersky Industrial CyberSecurity for Networks. Этот способ применяется для сканирования с помощью Endpoint Agent на каждом устройстве.

      - **Удаленное подключение**.

        Этот способ нужно использовать, если на устройствах, выбранных для задания, нет программного компонента Endpoint Agent, но есть возможность подключиться к этим устройствам по протоколам, которые обеспечивают безопасное управление и передачу данных. Для этого способа дополнительно требуется указать следующие данные:

        - Один из узлов с установленными компонентами программы, с которого будут выполняться подключения к устройствам.

        - Секрет с учетными данными для удаленных подключений.

          Вы можете выбрать для задания только один секрет с одним набором учетных данных. Учетные данные, хранящиеся в выбранном секрете, должны быть применимы на всех устройствах, выбранных для задания (подключения к этим устройствам возможны с одними и теми же учетными данными из секрета). Также нужно учитывать, что некоторые системные данные (например, данные о паролях пользователей операционной системы) могут быть получены только по запросу от имени пользователя, который обладает достаточно высоким уровнем привилегий. Для получения таких данных вам нужно указать в секрете учетные данные пользователя, у которого есть соответствующий уровень привилегий (пользователь с root-правами или пользователь, указанный в файле /etc/sudoers).

        > Если секрет с нужными учетными данными еще не добавлен в программу, вы можете, не закрывая окно мастера настройки, открыть в браузере новую вкладку, подключиться к Серверу и добавить секрет, после чего обновить список секретов с помощью кнопки в окне мастера настройки.

   c. При необходимости включите обнаружение рисков категории Уязвимость по результатам выполнения задания. Для этого установите флажок **Регистрировать обнаруженные уязвимости**.

   d. Если требуется запускать выполнение задания по расписанию, включите переключатель **Запускать задание по расписанию** и настройте параметры расписания:

      - В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять запуски: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.

      - В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска.

Программа выполняет запуск задания по расписанию при условии завершения предыдущего запуска этого задания. Если к моменту запуска задания по расписанию его предыдущий запуск имеет статус *Выполняется*, программа пропускает запуск задания по расписанию.

e. Если требуется отправлять отчеты о запусках задания по электронной почте, включите переключатель **Отправлять по электронной почте** и укажите адреса получателей.

   Максимальное количество получателей отчетов – 10.

4. Нажмите на кнопку **Создать задание** для завершения работы мастера.

Заданные параметры отобразятся в области деталей задания на вкладках **Параметры**, **Правила** и **Устройства**.

Изменение задания аудита настроек и уязвимостей

Изменять задания аудита настроек и уязвимостей могут только пользователи с ролью Администратор.

Чтобы изменить задание аудите настроек и уязвимостей:

1. Выберите раздел **Аудит безопасности**.

2. На вкладке **Аудит настроек и уязвимостей** выберите задание, для которого вы хотите изменить параметры.

3. Нажмите на кнопку **Изменить**.

   Запустится мастер настройки. В параметрах мастера настройки в качестве значений по умолчанию будут заданы значения параметров выбранного задания.

4. В разделе **Выбор устройств** сформируйте список устройств, на которых будут выполняться сканирования при выполнении задания. Выберите для задания не более 1000 устройств.

   Вы можете формировать список устройств с помощью кнопок **Добавить в задание** и **Удалить из задания**. Для добавления устройств программа открывает окно с таблицей устройств для выбора. Вы можете выполнять фильтрацию и сортировку таблицы для отображения нужных устройств.

5. В разделе **Настройка задания** настройте остальные параметры задания:

   a. Введите имя и описание задания.

      Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя задания должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

      Имя задания должно содержать не более 256 символов. Описание задания должно содержать не более 4096 символов.

   b. Выберите один из следующих способов опроса устройств:

      - **Локальный агент**.

        Вы можете использовать этот способ, если на устройствах, выбранных для задания, есть программный компонент Endpoint Agent и настроена интеграция EPP-приложения с Kaspersky Industrial CyberSecurity for Networks. Этот способ применяется для сканирования с помощью Endpoint Agent на каждом устройстве.

      - **Удаленное подключение**.

        Этот способ нужно использовать, если на устройствах, выбранных для задания, нет программного компонента Endpoint Agent, но есть возможность подключиться к этим устройствам по протоколам, которые обеспечивают безопасное управление и передачу данных. Для этого способа дополнительно требуется указать следующие данные:

        - Один из узлов с установленными компонентами программы, с которого будут выполняться подключения к устройствам.

        - Секрет с учетными данными для удаленных подключений.

          Вы можете выбрать для задания только один секрет с одним набором учетных данных. Учетные данные, хранящиеся в выбранном секрете, должны быть применимы на всех устройствах, выбранных для задания (подключения к этим устройствам возможны с одними и теми же учетными данными из секрета). Также нужно учитывать, что некоторые системные данные (например, данные о паролях пользователей операционной системы) могут быть получены только по запросу от имени пользователя, который обладает достаточно высоким уровнем привилегий. Для получения таких данных вам нужно указать в секрете учетные данные пользователя, у которого есть соответствующий уровень привилегий (пользователь с root-правами или пользователь, указанный в файле /etc/sudoers).

        Если секрет с нужными учетными данными еще не добавлен в программу, вы можете, не закрывая окно мастера настройки, открыть в браузере новую вкладку, подключиться к Серверу и добавить секрет, после чего обновить список секретов с помощью кнопки в окне мастера настройки.

   c. При необходимости включите обнаружение рисков категории Уязвимость по результатам выполнения задания. Для этого установите флажок **Регистрировать обнаруженные уязвимости**.

   d. Если требуется запускать выполнение задания по расписанию, включите переключатель **Запускать задание по расписанию** и настройте параметры расписания:

      - В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять запуски: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.

      - В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска.

Программа выполняет запуск задания по расписанию при условии завершения предыдущего запуска этого задания. Если к моменту запуска задания по расписанию его предыдущий запуск имеет статус *Выполняется*, программа пропускает запуск задания по расписанию.

e. Если требуется отправлять отчеты о запусках задания по электронной почте, включите переключатель **Отправлять по электронной почте** и укажите адреса получателей.

   Максимальное количество получателей отчетов – 10.

6. Нажмите на кнопку **Изменить задание** для завершения работы мастера.

Заданные параметры отобразятся в области деталей задания на вкладках **Параметры**, **Правила** и **Устройства**.

Просмотр таблицы заданий аудита настроек и уязвимостей

Таблица заданий аудита настроек и уязвимостей отображается в разделе **Аудит безопасности** на вкладке **Аудит настроек и уязвимостей**.

Параметры заданий отображаются в следующих столбцах таблицы:

- **ID задания**.

  Идентификатор задания, присвоенный в Kaspersky Industrial CyberSecurity for Networks.

- **Имя**.

  Имя, под которым задание представлено в программе.

- **Описание**.

  Описание задания.

- **Создано**.

  Дата и время добавления задания в программу.

- **Изменено**.

  Дата и время последнего изменения задания в программе.

- **Набор правил**.

  Имя набора правил, с которым связано задание.

- **Профиль**.

  Название профиля, который определяет состав правил и переменных для проверок при выполнении задания.

- **Правил XCCDF в наборе**.

  Количество выбранных правил для задания и общее количество правил в наборе правил.

- **Выбрано устройств**.

  Количество устройств, выбранных для задания.

- **Способ опроса**.

  Способ опроса, выбранный для сканирования устройств: **Локальный агент** или **Удаленное подключение**.

- **Регистрировать уязвимости**.

  Признак включенного обнаружения рисков категории Уязвимость по результатам выполнения задания.

- **Расписание**.

  Информация о расписании, по которому программа автоматически запускает выполнение задания.

- **Статус последнего запуска**.

  Результирующий статус сканирований всех устройств при последнем запуске задания.

- **Последний запуск**.

  Дата и время последнего запуска задания.

- **Следующий запуск**.

  Дата и время следующего запуска задания по расписанию.

При просмотре таблицы заданий аудита настроек и уязвимостей вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Запуск и остановка заданий аудита настроек и уязвимостей вручную

Вы можете запускать и останавливать задания аудита настроек и уязвимостей вручную. При запуске или остановке задания программа запускает или останавливает выполнение всех сканирований на устройствах, которые выбраны для этого задания.

Действия по остановке или запуску задания доступны при соответствующих статусах последнего запуска задания (например, запуск задания недоступен, если его последний запуск имеет статус *Выполняется*).

Запускать и останавливать задания аудита настроек и уязвимостей вручную могут только пользователи с ролью Администратор.

Чтобы запустить задание аудита настроек и уязвимостей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Аудит безопасности**.

3. На вкладке **Аудит настроек и уязвимостей** выберите задание, которое вы хотите запустить.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Запустить** (кнопка заблокирована, если запуск задания невозможен в текущий момент).

Kaspersky Industrial CyberSecurity for Networks запустит выполнение задания. Сведения о выполнении сканирований устройств вы можете просмотреть на вкладке **Запуски** в области деталей задания.

Чтобы остановить выполнение задания аудита настроек и уязвимостей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Аудит безопасности**.

3. На вкладке **Аудит настроек и уязвимостей** выберите задание, выполнение которого вы хотите остановить.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Остановить** (кнопка заблокирована, если остановка выполнения задания невозможна в текущий момент).

Просмотр общих сведений о выполнении запусков заданий аудита настроек и уязвимостей

Вы можете просматривать общие сведения о запусках заданий аудита настроек и уязвимостей при просмотре таблицы заданий. В таблице отображаются сведения о выполнении последних запусков заданий без вывода сведений о сканированиях устройств. Для просмотра общих сведений обо всех запусках задания, включая сведения о сканированиях устройств, вы можете выбрать это задание и перейти на вкладку **Запуски** в области деталей.

К общим сведениям о выполнении запусков заданий аудита настроек и уязвимостей относятся следующие:

- Статус выполнения запуска задания.

  Предусмотрены следующие статусы:

  - **Новое** или **Не запускалось** – создан новый запуск задания, в котором сканирования еще не выполнялись.
  - **Ожидание** – команда на начало сканирований готова к отправке.
  - **Выполняется** – запуск находится в процессе выполнения.
  - **Отменяется** – запуск находится в процессе остановки.
  - **Отменено** – запуск остановлен.
  - **Завершено** – все сканирования в запуске завершены успешно.
  - **Ошибка** – во всех сканированиях в запуске произошли ошибки.
  - **Не все успешно** – запуск задания завершен с частично успешным результатом: есть сканирования со статусом **Завершено** и есть сканирования со статусом **Отменено** или **Ошибка**.

- Статус выполнения сканирования устройства.

  Предусмотрены следующие статусы:

  - **Ожидание** – команда на начало сканирования готова к отправке.
  - **Выполняется** – сканирование находится в процессе выполнения.
  - **Отменяется** – сканирование находится в процессе остановки.
  - **Отменено** – сканирование остановлено.
  - **Завершено** – сканирование завершено успешно.
  - **Ошибка** – при сканировании произошла ошибка.

- Дата и время начала.
- Дата и время завершения.
- Длительность выполнения.

Остановка сканирования устройства в задании аудита настроек и уязвимостей

Вы можете вручную останавливать сканирование устройства в рамках задания аудита настроек и уязвимостей. При остановке сканирования устройства программа не останавливает другие сканирования устройств, которые требуется выполнить в этом задании.

Останавливать сканирования устройств вручную могут только пользователи с ролью Администратор.

Чтобы остановить сканирование устройства в задании аудита настроек и уязвимостей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Аудит настроек и уязвимостей** выберите задание, в котором вы хотите остановить сканирование устройства.

   В правой части окна веб-интерфейса появится область деталей.
4. В области деталей перейдите на вкладку **Запуски**.
5. Выберите нужное сканирование и нажмите на кнопку **Остановить** в появившейся области деталей сканирования (кнопка отсутствует, если остановка сканирования невозможна в текущий момент).

Удаление заданий аудита настроек и уязвимостей

Вы можете удалять задания аудита настроек и уязвимостей. При этом невозможно удалять задания со статусом последнего запуска **Выполняется** или **Ожидание**.

Удалять задания аудита настроек и уязвимостей могут только пользователи с ролью Администратор.

Чтобы удалить задания аудита настроек и уязвимостей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Аудит настроек и уязвимостей** выберите задания, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление заданий.

   Из выбранных заданий вы можете удалить только такие задания, у которых статус последнего запуска отличается от статусов **Выполняется** и **Ожидание**. Если среди выбранных заданий есть задания со статусом **Выполняется** или **Ожидание**, на экране появится сообщение об этом. Для удаления таких заданий вам нужно предварительно остановить выполнение заданий.

Управление параметрами хранения для запусков заданий аудита настроек и уязвимостей

Kaspersky Industrial CyberSecurity for Networks сохраняет сведения о запусках заданий аудита настроек и уязвимостей в базе данных на Сервере. Сведения о запусках хранятся до удаления заданий или до превышения заданного ограничения. Если объем сведений о запусках превышает заданное ограничение, программа автоматически удаляет 10% самых старых записей. При этом если включено ограничение на минимальное время хранения, при удалении записей, время хранения которых меньше заданного ограничения, в журнале сообщений программы появляется соответствующее сообщение. Вы можете настроить параметры хранения сведений о запусках.

Чтобы изменить параметры хранения для запусков заданий аудита настроек и уязвимостей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку Сервера.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров Сервера.
5. На вкладке **Общие** перейдите к блоку параметров **Аудит настроек и уязвимостей** и задайте ограничение занимаемого объема для хранения сведений о запусках с помощью параметра **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.
6. При необходимости с помощью параметра **Время хранения (дней)** включите ограничение на минимальное время хранения сведений о запусках и укажите нужное количество дней для хранения.
7. Нажмите на кнопку **Сохранить**.

Задания контроля конфигураций

С помощью заданий контроля конфигураций вы можете проводить аудит безопасности контролируемых устройств в части получения, сохранения и сравнения конфигураций устройств. Дополнительно задания контроля конфигураций позволяют загружать в Kaspersky Industrial CyberSecurity for Networks данные для контроля пользователей на устройствах, контроля приложений и патчей на устройствах и контроля оборудования на промышленных устройствах.

Программа может контролировать следующие типы конфигураций на устройствах:

- **Операционная система Windows** – к этому типу относятся конфигурации устройств под управлением операционных систем семейства Windows.
- **Операционная система Linux** – к этому типу относятся конфигурации устройств под управлением операционных систем семейства Linux.

- **Сетевые устройства** – к этому типу относятся конфигурации устройств, относящихся к сетевому оборудованию (например, маршрутизаторы, коммутаторы).

- **ПЛК** – к этому типу относятся конфигурации программируемых логических контроллеров или любых других устройств, получение конфигураций которых возможно с использованием коннекторов типа **Active poll**.

Особенности получения данных в зависимости от выбранного типа конфигурации см. в Приложении.

Для каждого задания вы можете запускать выполнение вручную или настроить расписание автоматического запуска.

При запуске задания программа инициирует сканирования устройств, входящих в это задание. Если при сканировании устройства обнаружены изменения конфигурации этого устройства, программа регистрирует событие. В зависимости от режима обработки конфигураций, выбранного для задания, событие содержит результаты сравнения полученной конфигурации с предыдущей конфигурацией устройства или с его эталонной конфигурацией.

Для заданий контроля конфигураций предусмотрены следующие режимы обработки конфигураций:

- **Только обновление** – в этом режиме для каждого устройства сохраняется только последняя полученная конфигурация.

- **Архивирование версий** – в этом режиме для каждого устройства сохраняются все его уникальные конфигурации.

- **Сравнение с эталоном** – в этом режиме для каждого устройства сохраняются все его уникальные конфигурации, при этом сравнение новой полученной конфигурации выполняется с эталонной конфигурацией (по умолчанию программа считает эталоном первую загруженную конфигурацию устройства).

Сканирования устройств для получения типа конфигурации **ПЛК** возможно только с использованием коннекторов типа **Active poll**. Для получения остальных типов конфигураций предусмотрены следующие способы опроса устройств:

- **Локальный агент**.

  Вы можете использовать этот способ, если на устройствах, выбранных для задания, есть программный компонент Endpoint Agent и настроена интеграция EPP-приложения с Kaspersky Industrial CyberSecurity for Networks. Этот способ применяется для сканирования с помощью Endpoint Agent на каждом устройстве.

- **Удаленное подключение**.

  Этот способ нужно использовать, если на устройствах, выбранных для задания, нет программного компонента Endpoint Agent, но есть возможность подключиться к этим устройствам по протоколам, которые обеспечивают безопасное управление и передачу данных. Способ поддерживается для получения типов конфигураций **Операционная система Linux** и **Сетевые устройства**. Для этого способа требуется указать в задании один из узлов с установленными компонентами программы, с которого будут выполняться подключения к устройствам. Также требуется указать учетные данные для удаленных подключений (учетные данные хранятся в программе в виде секретов).

Вы можете управлять заданиями контроля конфигураций в разделе **Аудит безопасности** на вкладке **Контроль конфигураций**. Если для сканирований устройств будет использоваться коннектор типа **Active poll** или сканирования будут выполняться способом **Удаленное подключение**, вы можете создать секреты с нужными учетными данными в разделе **Параметры → Секреты**.

После запуска заданий и завершения сканирований на устройствах вы можете просматривать сведения о полученных конфигурациях устройств в области деталей устройства на вкладке **Конфигурации**. На этой вкладке также доступны возможности сравнения конфигураций и назначения эталонной конфигурации.

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-интерфейс.

Добавление задания контроля конфигураций

Для известных программе устройств вы можете добавлять задания, по которым программа будет получать, сохранять и сравнивать конфигурации устройств.

Добавлять задания контроля конфигураций могут только пользователи с ролью Администратор.

Настройка задания контроля конфигураций выполняется с помощью мастера. Мастер позволяет пошагово выполнить настройку всех нужных параметров задания. После завершения настройки вы можете дождаться запуска сканирований на устройствах по расписанию или запустить задание вручную.

При добавлении задания контроля конфигураций вы можете вызвать мастер настройки следующими способами:

- Добавление задания с изначально пустыми значениями параметров. Для этого:

  1. Выберите раздел **Аудит безопасности**.
  2. На вкладке **Контроль конфигураций** нажмите на кнопку **Добавить задание**.

  В параметрах мастера настройки не будут заданы значения по умолчанию.

- Добавление задания для выбранных устройств. Для этого:

  1. Выберите раздел **Активы**.
  2. На вкладке **Устройства** выберите устройства, для которых вы хотите добавить задание контроля конфигураций.
  3. Вы можете выбрать не более 100 устройств.
  4. В панели инструментов, которая расположена над таблицей устройств, откройте раскрывающийся список **Создать задание** и выберите пункт **Контроль конфигураций**.

  В параметрах мастера настройки по умолчанию будет сформирован список устройств, состоящий из выбранных устройств.

Чтобы настроить параметры задания в окне мастера настройки:

1. В разделе **Выбор устройств** сформируйте список устройств, на которых будут выполняться сканирования при выполнении задания. Выберите для задания не более 100 устройств.

   Вы можете формировать список устройств с помощью кнопок **Добавить в задание** и **Удалить из задания**. Для добавления устройств программа открывает окно с таблицей устройств для выбора. Вы можете выполнять фильтрацию и сортировку таблицы для отображения нужных устройств.

2. В разделе **Выбор параметров** выполните следующие действия:

   a. Выберите тип конфигурации, который требуется получать при выполнении задания.

   b. Если выбран тип конфигурации **ПЛК**, то при появлении окна с предупреждением об особенностях активных опросов внимательно ознакомьтесь с описанием этих особенностей и подтвердите принятие рисков возможных последствий при использовании модуля активного опроса.

      В зависимости от версии программы окно с предупреждением об особенностях активных опросов появляется в следующих случаях:

      - В версии Kaspersky Industrial CyberSecurity for Networks 4.2 – один раз при добавлении первого задания, если ранее ни один из пользователей программы не проводил активных опросов устройств.
      - В версии Kaspersky Industrial CyberSecurity for Networks 4.2.1 – при добавлении каждого задания.

   c. Настройте параметры выбранного типа конфигурации. В зависимости от выбранного типа вы можете указать нужные компоненты конфигураций (например, компонент конфигурации **Локальные пользователи и группы**) или указать данные для подключений (например, коннектор и секрет с учетными данными для удаленных подключений, если выбран тип конфигурации **ПЛК**).

      Если секрет с нужными учетными данными не добавлен в программу, вы можете, не закрывая окно мастера настройки, открыть в браузере новую вкладку, подключиться к Серверу и добавить секрет, после чего обновить список секретов с помощью кнопки в окне мастера настройки.

3. В разделе **Настройка задания** настройте остальные параметры задания:

   a. Введите имя и описание задания.

      Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя задания должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

      Имя задания должно содержать не более 256 символов. Описание задания должно содержать не более 4096 символов.

   b. Выберите режим обработки конфигураций.

   c. Если в разделе **Выбор параметров** выбран тип конфигурации **Операционная система Windows**, **Операционная система Linux** или **Сетевые устройства**, выберите один из следующих способов опроса устройств:

      - **Локальный агент**.

        Вы можете использовать этот способ, если на устройствах, выбранных для задания, есть программный компонент Endpoint Agent и настроена интеграция EPP-приложения с Kaspersky Industrial CyberSecurity for Networks. Этот способ применяется для сканирования с помощью Endpoint Agent на каждом устройстве.

      - **Удаленное подключение**.

        Этот способ нужно использовать, если на устройствах, выбранных для задания, нет программного компонента Endpoint Agent, но есть возможность подключиться к этим устройствам по протоколам, которые обеспечивают безопасное управление и передачу данных. Способ поддерживается для получения типов конфигураций **Операционная система Linux** и **Сетевые устройства**. Для этого способа дополнительно требуется указать следующие данные:

        - Один из узлов с установленными компонентами программы, с которого будут выполняться подключения к устройствам.

        - Секрет с учетными данными для удаленных подключений.

          Вы можете выбрать для задания только один секрет с одним набором учетных данных. Учетные данные, хранящиеся в выбранном секрете, должны быть применимы на всех устройствах, выбранных для задания (подключения к этим устройствам возможны с одними и теми же учетными данными из секрета). Также нужно учитывать, что некоторые системные данные (например, данные о паролях пользователей операционной системы) могут быть получены только по запросу от имени пользователя, который обладает достаточно высоким уровнем привилегий. Для получения таких данных вам нужно указать в секрете учетные данные пользователя, у которого есть соответствующий уровень привилегий (пользователь с root-правами или пользователь, указанный в файле /etc/sudoers).

          Если секрет с нужными учетными данными еще не добавлен в программу, вы можете, не закрывая окно мастера настройки, открыть в браузере новую вкладку, подключиться к Серверу и добавить секрет, после чего обновить список секретов с помощью кнопки в окне мастера настройки.

   d. Если требуется запускать выполнение задания по расписанию, включите переключатель **Запускать задание по расписанию** и настройте параметры расписания:

      - В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять запуски: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.

- В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска.

Программа выполняет запуск задания по расписанию при условии завершения предыдущего запуска этого задания. Если к моменту запуска задания по расписанию его предыдущий запуск имеет статус *Выполняется*, программа пропускает запуск задания по расписанию.

4. Нажмите на кнопку **Создать задание** для завершения работы мастера.

Заданные параметры отобразятся в области деталей задания на вкладках **Параметры** и **Устройства**.

Изменение задания контроля конфигураций

Изменять задания контроля конфигураций могут только пользователи с ролью Администратор.

Чтобы изменить задание контроля конфигураций:

1. Выберите раздел **Аудит безопасности**.
2. На вкладке **Контроль конфигураций** выберите задание, для которого вы хотите изменить параметры.
3. Нажмите на кнопку **Изменить**.

   Запустится мастер настройки. В параметрах мастера настройки в качестве значений по умолчанию будут заданы значения параметров выбранного задания.
4. В разделе **Настройка задания** настройте параметры задания:

   a. Введите имя и описание задания.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя задания должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

   Имя задания должно содержать не более 256 символов. Описание задания должно содержать не более 4096 символов.

   b. Если требуется запускать выполнение задания по расписанию, включите переключатель **Запускать задание по расписанию** и настройте параметры расписания:

   - В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять запуски: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.
   - В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска.

Программа выполняет запуск задания по расписанию при условии завершения предыдущего запуска этого задания. Если к моменту запуска задания по расписанию его предыдущий запуск имеет статус *Выполняется*, программа пропускает запуск задания по расписанию.

5. Нажмите на кнопку **Изменить задание** для завершения работы мастера.

Заданные параметры отобразятся в области деталей задания на вкладках **Параметры** и **Устройства**.

Просмотр таблицы заданий контроля конфигураций

Таблица заданий контроля конфигураций отображается в разделе **Аудит безопасности** на вкладке **Контроль конфигураций**.

Параметры заданий отображаются в следующих столбцах таблицы:

- **ID задания**.

  Идентификатор задания, присвоенный в Kaspersky Industrial CyberSecurity for Networks.

- **Имя**.

  Имя, под которым задание представлено в программе.

- **Описание**.

  Описание задания.

- **Создано**.

  Дата и время добавления задания в программу.

- **Изменено**.

  Дата и время последнего изменения задания в программе.

- **Выбрано устройств**.

  Количество устройств, выбранных для задания.

- **Способ опроса**.

  Способ опроса, выбранный для сканирования устройств: **Локальный агент**, **Удаленное подключение** или **Коннектор Active poll**.

- **Расписание**.

  Информация о расписании, по которому программа автоматически запускает выполнение задания.

- **Статус последнего запуска**.

  Результирующий статус сканирований всех устройств при последнем запуске задания.

- **Последний запуск**.

  Дата и время последнего запуска задания.

- **Следующий запуск**.

  Дата и время следующего запуска задания по расписанию.

При просмотре таблицы заданий контроля конфигураций вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Запуск и остановка заданий контроля конфигураций вручную

Вы можете запускать и останавливать задания контроля конфигураций вручную. При запуске или остановке задания программа запускает или останавливает выполнение всех сканирований на устройствах, которые выбраны для этого задания.

Действия по остановке или запуску задания доступны при соответствующих статусах последнего запуска задания (например, запуск задания недоступен, если его последний запуск имеет статус *Выполняется*).

Запускать и останавливать задания контроля конфигураций вручную могут только пользователи с ролью Администратор.

Чтобы запустить задание контроля конфигураций:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Контроль конфигураций** выберите задание, которое вы хотите запустить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Запустить** (кнопка заблокирована, если запуск задания невозможен в текущий момент).

Kaspersky Industrial CyberSecurity for Networks запустит выполнение задания. Сведения о выполнении сканирований устройств вы можете просмотреть на вкладке **Запуски** в области деталей задания.

Чтобы остановить выполнение задания контроля конфигураций:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Контроль конфигураций** выберите задание, выполнение которого вы хотите остановить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Остановить** (кнопка заблокирована, если остановка выполнения задания невозможна в текущий момент).

Просмотр общих сведений о выполнении запусков заданий контроля конфигураций

Вы можете просматривать общие сведения о запусках заданий контроля конфигураций при просмотре таблицы заданий. В таблице отображаются сведения о выполнении последних запусков заданий без вывода сведений о сканированиях устройств. Для просмотра общих сведений обо всех запусках задания, включая сведения о сканированиях устройств, вы можете выбрать это задание и перейти на вкладку **Запуски** в области деталей.

К общим сведениям о выполнении запусков заданий контроля конфигураций относятся следующие:

- Статус выполнения запуска задания.

  Предусмотрены следующие статусы:

  - **Новое** или **Не запускалось** – создан новый запуск задания, в котором сканирования еще не выполнялись.
  - **Ожидание** – команда на начало сканирований готова к отправке.
  - **Выполняется** – запуск находится в процессе выполнения.
  - **Отменяется** – запуск находится в процессе остановки.
  - **Отменено** – запуск остановлен.
  - **Завершено** – все сканирования в запуске завершены успешно.
  - **Ошибка** – во всех сканированиях в запуске произошли ошибки.
  - **Не все успешно** – запуск задания завершен с частично успешным результатом: есть сканирования со статусом **Завершено** и есть сканирования со статусом **Отменено** или **Ошибка**.

- Статус выполнения сканирования устройства.

  Предусмотрены следующие статусы:

  - **Ожидание** – команда на начало сканирования готова к отправке.
  - **Выполняется** – сканирование находится в процессе выполнения.
  - **Отменяется** – сканирование находится в процессе остановки.
  - **Отменено** – сканирование остановлено.
  - **Завершено** – сканирование завершено успешно.
  - **Ошибка** – при сканировании произошла ошибка.

- Дата и время начала.
- Дата и время завершения.
- Длительность выполнения.

Назначение эталонной конфигурации устройства

По результатам выполнения заданий контроля конфигураций программа сохраняет полученные конфигурации для каждого устройства. Если для задания задан режим обработки конфигураций **Сравнение с эталоном**, программа по умолчанию считает эталонной конфигурацией первую загруженную конфигурацию устройства. Вы можете назначить в качестве эталонной любую другую сохраненную конфигурацию устройства.

При необходимости перед назначением эталонной конфигурации вы можете сравнить сохраненные конфигурации устройства.

Чтобы назначить эталонную конфигурацию устройства:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Активы** на вкладке **Устройства** выберите нужное устройство.

   В правой части окна веб-интерфейса появится область деталей.

3. На вкладке **Конфигурации** в области деталей выберите строку таблицы с нужным компонентом конфигурации (например, компонент **Локальные пользователи и группы**, в котором сохранены сведения о пользователях устройства). Для выбранного компонента в программе должно быть ненулевое количество уникальных записей, указанное в столбце **Архивных записей** (в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1 – количество 2 или больше в столбце **Архивных записей**).

   Появится окно с подробными сведениями о выбранном компоненте конфигурации.

4. В раскрывающемся списке выберите дату и время получения конфигурации, которую вы хотите назначить эталонной конфигурацией.

   В окне отобразятся подробные сведения о сохраненной конфигурации выбранного компонента.

5. Нажмите на кнопку **Назначить эталонной**.

6. В окне запроса подтвердите назначение эталонной конфигурации.

Остановка сканирования устройства в задании контроля конфигураций

Вы можете вручную останавливать сканирование устройства в рамках задания контроля конфигураций. При остановке сканирования устройства программа не останавливает другие сканирования устройств, которые требуется выполнить в этом задании.

Останавливать сканирования устройств вручную могут только пользователи с ролью Администратор.

Чтобы остановить сканирование устройства в задании контроля конфигураций:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Аудит безопасности**.

3. На вкладке **Контроль конфигураций** выберите задание, в котором вы хотите остановить сканирование устройства.

   В правой части окна веб-интерфейса появится область деталей.

4. В области деталей перейдите на вкладку **Запуски**.

5. Выберите нужное сканирование и нажмите на кнопку **Остановить** в появившейся области деталей сканирования (кнопка отсутствует, если остановка сканирования невозможна в текущий момент).

Удаление заданий контроля конфигураций

Вы можете удалять задания контроля конфигураций. При этом невозможно удалять задания со статусом последнего запуска **Выполняется** или **Ожидание**.

Удалять задания контроля конфигураций могут только пользователи с ролью Администратор.

Чтобы удалить задания контроля конфигураций:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Контроль конфигураций** выберите задания, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление заданий.

   Из выбранных заданий вы можете удалить только такие задания, у которых статус последнего запуска отличается от статусов **Выполняется** и **Ожидание**. Если среди выбранных заданий есть задания со статусом **Выполняется** или **Ожидание**, на экране появится сообщение об этом. Для удаления таких заданий вам нужно предварительно остановить выполнение заданий.

Задания активных опросов устройств

С помощью заданий активного опроса вы можете проводить аудит безопасности контролируемых устройств в части получения точной и полной информации об устройствах и их конфигурациях непосредственно от самих устройств. Активные опросы выполняются с помощью коннекторов. Для проведения активных опросов устройств вам нужно добавить в программу один или несколько коннекторов типа **Active poll**.

Коннекторы предоставляют различные методы проведения активных опросов. *Методы активных опросов* определяют используемые протоколы, а также команды и функции этих протоколов. Встроенный в программу тип коннектора **Active poll** содержит набор методов, поддерживающих активные опросы как по протоколам прикладного уровня, так и по протоколам общего применения. Kaspersky Industrial CyberSecurity for Networks поддерживает следующие методы для проведения активных опросов устройств:

- опрос по протоколу ARP (только для компьютеров с версией ядра 4.3 и выше);
- опрос по протоколу CIP™ (не поддерживается в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1);
- опрос по протоколу DNP3;
- определение параметров контроля процесса и тегов (только для компьютеров с версией ядра 4.3 и выше);
- опрос по протоколу IEC 61850: MMS;
- опрос по протоколу Modbus TCP;

- опрос по протоколу BECKHOFF ADS/AMS поверх UDP;
- опрос по протоколу PROFINET DCP (только для компьютеров с версией ядра 4.3 и выше);
- опрос по протоколу Siemens S7comm поверх Industrial Ethernet;
- опрос по протоколу Siemens S7comm поверх TCP;
- получение расширенной конфигурации Schneider Electric Modicon M580/M340;
- получение расширенной конфигурации Siemens SIMATIC S7-300/S7-400;
- получение расширенной конфигурации Emerson DeltaV (поддерживается только в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1);
- получение расширенной конфигурации Rockwell Automation Allen-Bradley (поддерживается только в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1);
- опрос по протоколу SMB;
- опрос по протоколу SNMP;
- опрос по протоколу SSH;
- опрос по протоколу WinRM HTTP;
- опрос по протоколу WinRM HTTPS;
- опрос по протоколу взаимодействия WMI;
- анализ рисков на устройствах Cisco по SSH;
- анализ рисков на устройствах Linux по SSH.

Методы различаются по составу получаемых сведений об устройствах. Вы можете выбирать нужные вам сведения и используемые методы при настройке параметров проведения активных опросов.

Некоторые методы используют секреты для подключения к устройствам. Подключение к устройствам осуществляется с помощью учетных данных из секретов, добавленных в программу.

При использовании соответствующих методов программа может автоматически обновлять следующие сведения об устройстве по результатам активного опроса:

- имя, под которым устройство представлено в программе;
- имя, под которым устройство представлено в сети (сетевое имя);
- название производителя аппаратного обеспечения устройства;
- название модели устройства;
- номер версии аппаратного обеспечения устройства;
- название производителя программного обеспечения устройства;
- название программного обеспечения устройства;

- номер версии программного обеспечения устройства;
- адресная информация для сетевых интерфейсов устройства;
- название операционной системы, установленной на устройстве (только для устройств под управлением операционных систем семейств Windows и Linux);
- конфигурация параметров контроля процесса и тегов;
- расширенная конфигурация промышленных устройств.

Список операционных систем, поддерживаемых программой для проведения активных опросов устройств, см. в Приложении.

Обновление не выполняется для тех сведений, для которых выключено автоматическое изменение с помощью переключателей **Автообновление** при добавлении устройства или при изменении сведений об устройстве. Также программа оценивает достоверность полученных сведений об устройстве и в некоторых случаях может не обновлять ранее полученные сведения.

Некоторые методы активных опросов поддерживают возможность обнаружения рисков и внесения изменений в топологическую карту по полученным данным об устройствах.

Для каждого задания вы можете запускать выполнение вручную или настроить расписание автоматического запуска. Запускать задания активного опроса устройств могут только пользователи с ролью Администратор.

Для использования функциональности активного опроса вам нужно учитывать следующие особенности и ограничения:

- Функциональность доступна после добавления лицензионного ключа.
- Программные модули коннекторов, с помощью которых выполняются активные опросы устройств, должны иметь сетевой доступ к устройствам для отправки запросов и получения данных от устройств. Если программные модули функционируют на узле с установленными компонентами программы, для обеспечения сетевого доступа к устройствам на этом компьютере должен быть сетевой интерфейс с подключением к сети этих устройств. Для этих целей не могут использоваться сетевые интерфейсы точек мониторинга, если на эти сетевые интерфейсы поступает зеркалированный трафик промышленной сети (например, от SPAN-портов сетевых коммутаторов).
- При активном опросе возможно возникновение непредвиденных проблем с устройствами из-за неверной интерпретации этими устройствами поступивших команд активного опроса. Проблемы могут быть вызваны неправильной или узкоспецифичной настройкой устройств. Также проблемы могут возникать из-за скрытых ошибок в сетевой конфигурации, которые не проявляются при обычном взаимодействии устройств. В связи с этим при активном опросе устройства имеются следующие риски возможных последствий:
  - выключение устройства;
  - потеря связи с устройством;
  - полная или частичная неработоспособность устройства;
  - замедление работы устройства;
  - другие потенциальные сбои в работе сети и оборудования.

Добавление задания активного опроса

Для известных программе устройств вы можете добавлять задания, по которым программа будет выполнять активный опрос.

Добавлять задания активного опроса могут только пользователи с ролью Администратор. Добавление задания активных опросов возможно после добавления лицензионного ключа.

Настройка задания активного опроса выполняется с помощью мастера. Мастер позволяет пошагово выполнить настройку всех нужных параметров задания. После завершения настройки вы можете дождаться запуска сканирований на устройствах по расписанию или запустить задание вручную.

При добавлении задания активного опроса вы можете вызвать мастер настройки следующими способами:

- Добавление задания с изначально пустыми значениями параметров. Для этого:

  1. Выберите раздел **Аудит безопасности**.
  2. На вкладке **Активный опрос** нажмите на кнопку **Добавить задание**.

  В параметрах мастера настройки не будут заданы значения по умолчанию.

- Добавление задания для выбранных устройств. Для этого:

  1. Выберите раздел **Активы**.
  2. На вкладке **Устройства** выберите устройства, для которых вы хотите добавить задание активного опроса. Вы можете выбрать не более 100 устройств.
  3. В панели инструментов, которая расположена над таблицей устройств, откройте раскрывающийся список **Создать задание** и выберите пункт **Активный опрос**.

  В параметрах мастера настройки по умолчанию будет сформирован список устройств, состоящий из выбранных устройств.

Чтобы настроить параметры задания в окне мастера настройки:

1. В окне с предупреждением об особенностях активных опросов внимательно ознакомьтесь с описанием этих особенностей и подтвердите принятие рисков возможных последствий при использовании модуля активного опроса.

   В зависимости от версии программы окно с предупреждением об особенностях активных опросов появляется в следующих случаях:

   - В версии Kaspersky Industrial CyberSecurity for Networks 4.2 – один раз при добавлении первого задания, если ранее ни один из пользователей программы не проводил активных опросов устройств.
   - В версии Kaspersky Industrial CyberSecurity for Networks 4.2.1 – при добавлении каждого задания.

2. В разделе мастера **Выбор устройств** сформируйте список устройств, для которых требуется выполнить активный опрос. Выберите не более 100 устройств.

   Вы можете сформировать список устройств с помощью кнопок **Добавить в задание** и **Удалить из задания**. Для добавления устройств программа открывает окно с таблицей устройств для выбора. Вы можете выполнять фильтрацию и сортировку таблицы для отображения нужных устройств.

3. В разделе мастера **Выбор параметров** установите флажки для тех сведений об устройствах, которые вы хотите обновить с помощью активного опроса. Вы также можете включить обнаружение рисков (флажок **Риски**) и обнаружение параметров топологии для устройств (флажок **Параметры топологии**).

4. В разделе мастера **Выбор методов** выполните следующие действия:

   a. Выберите модуль активного опроса.

   b. Установите флажки для тех методов, которые вы хотите использовать для получения сведений об устройствах, обнаружения рисков и/или параметров топологии.

      Доступные для использования методы сгруппированы по коннекторам, которые предоставляют возможности активного опроса устройств. Список содержит только методы, поддерживающие получение выбранных сведений. Если коннектор невозможно использовать для активного опроса выбранных устройств, доступные методы не отображаются для этого коннектора (например, если коннектор выключен или для коннектора выбрано адресное пространство, не содержащее адресов выбранных устройств).

   c. При необходимости настройте параметры для работы методов каждого коннектора (например, для метода **Опрос по протоколу SSH** требуется указать порт и секрет с учетными данными для подключения).

      > Если секрет с нужными учетными данными не добавлен в программу, вы можете, не закрывая окно мастера настройки, открыть в браузере новую вкладку, подключиться к Серверу и добавить секрет, после чего обновить список секретов с помощью кнопки в окне мастера настройки.

      Методы, для которых требуется настройка параметров, выделены красным. Для уточнения параметров нажмите на кнопку справа от нужного метода.

5. В разделе мастера **Настройка задания** настройте остальные параметры задания:

   a. Введите имя и описание задания.

      Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя задания должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

      Имя задания должно содержать не более 256 символов. Описание задания должно содержать не более 4096 символов.

   b. Если требуется запускать выполнение задания по расписанию, включите переключатель **Запускать задание по расписанию** и настройте параметры расписания:

      - В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять запуски: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.
      - В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска.

      > Программа выполняет запуск задания по расписанию при условии завершения предыдущего запуска этого задания. Если к моменту запуска задания по расписанию его предыдущий запуск имеет статус *Выполняется*, программа пропускает запуск задания по расписанию.

6. Нажмите на кнопку для завершения работы мастера: **Создать задание** или **Создать и запустить**.

Заданные параметры отобразятся в области деталей задания.

Изменение задания активного опроса

Изменять задания активного опроса могут только пользователи с ролью Администратор.

Чтобы изменить задание активного опроса:

1. Выберите раздел **Аудит безопасности**.
2. На вкладке **Активный опрос** выберите задание, для которого вы хотите изменить параметры.
3. Нажмите на кнопку **Изменить**.

   Запустится мастер настроек. В параметрах мастера настройки в качестве значений по умолчанию будут заданы значения параметров выбранного задания.
4. В разделе мастера **Настройка задания** настройте остальные параметры задания:

   a. Введите имя и описание задания.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя задания должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

   Имя задания должно содержать не более 256 символов. Описание задания должно содержать не более 4096 символов.

   b. Если требуется запускать выполнение задания по расписанию, включите переключатель **Запускать задание по расписанию** и настройте параметры расписания:

   - В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять запуски: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.
   - В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска.

   > Программа выполняет запуск задания по расписанию при условии завершения предыдущего запуска этого задания. Если к моменту запуска задания по расписанию его предыдущий запуск имеет статус *Выполняется*, программа пропускает запуск задания по расписанию.

5. Нажмите на кнопку **Изменить задание** для завершения работы мастера.

Заданные параметры отобразятся в области деталей задания.

Просмотр таблицы заданий активных опросов

Таблица заданий активного опроса отображается в разделе **Аудит безопасности** на вкладке **Активный опрос**.

Параметры заданий отображаются в следующих столбцах таблицы:

- **ID задания**.

  Идентификатор задания, присвоенный в Kaspersky Industrial CyberSecurity for Networks.

- **Имя**.

  Имя, под которым задание представлено в программе.

- **Описание**.

  Описание задания.

- **Создано**.

  Дата и время добавления задания в программу.

- **Изменено**.

  Дата и время последнего изменения в программе.

- **Выбрано устройств**.

  Количество устройств, выбранных для задания.

- **Расписание**.

  Информация о расписании, по которому программа автоматически запускает выполнение задания.

- **Статус последнего запуска**.

  Результирующий статус сканирований всех устройств при последнем запуске задания.

- **Последний запуск**.

  Дата и время последнего запуска задания.

- **Следующий запуск**.

  Дата и время следующего запуска задания по расписанию.

При просмотре таблицы заданий активного опроса вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Запуск и остановка заданий активных опросов

Вы можете запускать и останавливать задания активного опроса вручную. При запуске или остановке задания программа запускает или останавливает выполнение всех сканирований на устройствах, которые выбраны для этого задания.

Действия по остановке или запуску задания доступны при соответствующих статусах последнего запуска задания (например, запуск задания не доступен, если его последний запуск имеет статус *Выполняется*).

Запускать и останавливать задания активного опроса вручную могут только пользователи с ролью Администратор.

Чтобы запустить задание активного опроса:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Активный опрос** выберите задание, которое вы хотите запустить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Запустить** (кнопка заблокирована, если запуск задания невозможен в текущий момент).

   Kaspersky Industrial CyberSecurity for Networks запустит выполнение задания. Сведения о выполнении сканирований устройств вы можете просмотреть на вкладке **Запуски** в области деталей задания.

Чтобы остановить выполнение задания активного опроса:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Активный опрос** выберите задание, выполнение которого вы хотите остановить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Остановить** (кнопка заблокирована, если остановка выполнения задания невозможна в текущий момент).

Просмотр общих сведений о выполнении запусков заданий активных опросов

Вы можете просматривать общие сведения о запусках заданий активного опроса при просмотре таблицы заданий. В таблице отображаются сведения о выполнении последних запусков без вывода сведений о сканированиях устройств. Для просмотра общих сведений обо всех запусках задания, включая сведения о сканированиях устройств, вы можете выбрать это задание и перейти на вкладку **Запуски** в области деталей.

К общим сведениям о выполнении запусков заданий активного опроса относятся следующие:

- Статус выполнения запуска задания или сканирования устройства.

  Предусмотрены следующие статусы:

  - **Ожидание** – команда на начало сканирования еще не отправлена.
  - **Выполняется** – сканирование или запуск находится в процессе выполнения.
  - **Отменяется** – сканирование или запуск находится в процессе остановки.
  - **Отменено** – остановлено сканирование или запуск.
  - **Завершено** – сканирование завершено успешно или все сканирования в запуске завершены успешно.
  - **Ошибка** – при сканировании произошла ошибка или во всех сканированиях в запуске произошли ошибки.
  - **Не все успешно** – запуск задания завершен с частично успешным результатом: есть сканирования со статусом **Завершено** и есть сканирования со статусом **Отменено** или **Ошибка**.

- Дата и время начала.
- Дата и время завершения.
- Длительность выполнения.

Просмотр отчета о выполнении задания активного опроса

Вы можете просматривать отчеты с результатами выполнения сканирований на устройствах при просмотре подробных данных о запуске задания активного опроса. Отчеты формируются программой для заданий, выполнение которых завершилось со статусами **Завершено**, **Не все успешно**, **Отменено** и **Ошибка**.

В отчете отображается следующая информация:

- Имя устройства, для которого было выполнено сканирование.
- Статус обновления параметров устройства.
- Список параметров устройства, сгруппированных по статусу их обновления.
- Список методов, сгруппированных по статусу их выполнения. В случае возникновения ошибки при работе метода, программа отображает ее причину.

Чтобы просмотреть отчет о выполнении задания активного опроса:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.

3. На вкладке **Активный опрос** выберите задание, отчет о запуске которого вы хотите просмотреть.

   В правой части окна веб-интерфейса появится область деталей.

4. В области деталей перейдите на вкладку **Запуски** и выберите нужный запуск задания.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отображаются подробные сведения о выбранном запуске задания.

Удаление заданий активных опросов

Вы можете удалять задания активного опроса. При этом невозможно удалять задания со статусом последнего запуска **Выполняется** или **Ожидание**.

Удалять задания активного опроса могут только пользователи с ролью Администратор.

Чтобы удалить задания активного опроса:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Аудит безопасности**.

3. На вкладке **Активный опрос** выберите задания, которое вы хотите удалить.

4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

5. В окне запроса подтвердите удаление заданий.

   Из выбранных заданий вы можете удалить только такие задания, у которых статус последнего запуска отличается от статусов **Выполняется** и **Ожидание**. Если среди выбранных заданий есть задания со статусом **Выполняется** или **Ожидание**, на экране появится сообщение об этом. Для удаления таких заданий вам нужно предварительно остановить выполнение заданий.

Формирование топологической карты

Топологическая карта – это визуальное отображение схемы физических подключений устройств в промышленной сети. В отличие от карты сетевых взаимодействий, топологическая карта предназначена для отображения подключений устройств посредством сетевых кабелей, подсоединенных к портам сетевых интерфейсов. В результате формирования топологической карты вы получите один или несколько графов для наглядного отображения структуры соединений устройств через устройства сетевого оборудования (сетевые коммутаторы, концентраторы, маршрутизаторы и др.).

На топологической карте сети могут отображаться следующие объекты:

- Узлы. Эти объекты обозначают устройства и сетевое оборудование.
- Соединения. Эти объекты обозначают физические подключения узлов.

Узлы отображаются на топологической карте постоянно, независимо от наличия соединений этих узлов с другими узлами. Для узлов предусмотрены возможности фильтрации. Также узлы по-разному выделяются на топологической карте в зависимости от их типов, статусов и событий, связанных с узлами.

После того, как для узлов добавлены соединения, появляется возможность распределения этих узлов на топологической карте по алгоритму построения топологии.

Топологическая карта отображается в разделе **Карта сети** на вкладке **Топологическая карта**.

Данные для добавления соединений на топологическую карту могут быть получены автоматически по результатам активных опросов устройств, если используются соответствующие методы опроса (например, опрос по протоколу SNMP). Вы также можете добавлять соединения вручную.

Узлы на топологической карте

Узлы на топологической карте могут быть следующих типов:

- Известное программе устройство. Узел этого типа представляет устройство, входящее в таблицу устройств.

- Неуправляемый коммутатор. Узел этого типа представляет устройство, у которого неизвестны или отсутствуют MAC- и IP-адреса. Из-за отсутствия адресной информации такое устройство невозможно добавить в таблицу устройств. При этом есть соединенные с этим устройством другие устройства. Такой узел может появиться на топологической карте, например, если по результатам активного опроса обнаружено несколько подключений различных устройств к одному порту одного и того же устройства. В этом случае программа считает, что в сети присутствует неопределенное коммутирующее устройство (например, концентратор) и автоматически создает узел для этого устройства. В программу можно добавить не более 1000 неуправляемых коммутаторов.

  Если вам удалось определить MAC- и/или IP-адрес узла неуправляемого коммутатора, вы можете вручную добавить в таблицу известных программе устройств новое устройство на основе узла неуправляемого коммутатора.

Отображаемая информация на узлах, представляющих известные программе устройства

Для узлов, представляющих известные программе устройства, при максимальном масштабе топологической карты отображается следующее:

- Заданное имя устройства.

- Значок категории устройства.

- Сетевое имя или адрес устройства (если IP-адрес не задан, отображается MAC-адрес).

- Различные значки в зависимости от выполнения следующих условий:
  - если для устройства задан признак маршрутизирующего устройства;
  - если на устройстве установлено EPP-приложение (цвет значка зависит от состояния подключения);
  - если устройство имеет статус *Неиспользуемое*.
- Утолщенная линия на левой границе узла одного из следующих цветов в зависимости от состояния безопасности устройства:
  - зеленый цвет – состояние безопасности *OK*;
  - желтый цвет – состояние безопасности *Важное*;
  - красный цвет – состояние безопасности *Критическое*.

Если устройство имеет статус *Неразрешенное*, фон узла закрашен красным цветом.

Отображаемая информация на узлах, представляющих неуправляемые коммутаторы

Для узлов, представляющих неуправляемые коммутаторы, при максимальном масштабе топологической карты отображается следующее:

- Заданное имя узла.
- Значок неуправляемого коммутатора.

Узлы, представляющие неуправляемые коммутаторы, имеют серый цвет фона.

Соединения на топологической карте

Соединения на топологической карте показывают физические подключения узлов друг к другу. Каждое соединение отображает связь между портами сетевых интерфейсов устройств, соединенных сетевым кабелем.

Соединения отображаются на топологической карте в виде горизонтальных и вертикальных линий. Несколько линий соединений, идущих от одного узла, на общих участках отображаются в виде утолщенной линии – шины.

Просмотр подробных сведений об объектах топологической карты

Подробные сведения об объектах, представленных на топологической карте, отображаются в области деталей. Для отображения подробных сведений вы можете выбрать объект с помощью мыши.

Для выбранного узла отображаются следующие сведения:

- Если узел представляет известное программе устройство, в области деталей отображаются те же сведения, которые выводятся при выборе устройства в таблице устройств.
- Если узел представляет неуправляемый коммутатор, в области деталей отображаются следующие сведения:
  - имя узла неуправляемого коммутатора;
  - тип узла (Неуправляемый коммутатор);
  - раздел параметров **Параметры топологии**, содержащий список портов, для которых добавлены (или могут быть добавлены) соединения с другими узлами.

Для выбранного соединения отображается имя одного из узлов соединения и список портов этого узла с соединениями с другими узлами. Если выбрана шина, отображается список портов того узла, который имеет наибольшее количество соединений в выбранной шине.

Добавление узлов на топологическую карту

При формировании топологической карты программа может автоматически добавлять обнаруженные узлы на топологическую карту. Если нужные узлы не были добавлены программой автоматически, вы можете добавить их вручную при работе с топологической картой.

Добавлять узлы вручную могут только пользователи с ролью Администратор.

Если вам известен MAC- и/или IP-адрес устройства, которое вы хотите добавить на топологическую карту в качестве узла, вы можете добавить это устройство вручную. Если адресная информация узла неизвестна или отсутствует (например, устройство является концентратором), вы можете добавить узел неуправляемого коммутатора.

Чтобы добавить неуправляемый коммутатор на топологическую карту:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Топологическая карта** откройте раскрывающийся список **Добавить узел** и выберите пункт **Новый неуправляемый коммутатор**.

   В правой части окна появится область деталей с параметрами для неуправляемого коммутатора.
3. Введите имя узла.

   Имя узла должно быть уникальным (не совпадать с именами других неуправляемых коммутаторов) и может содержать не более 100 символов. Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ ' , . - _ = +`. Имя узла должно начинаться и заканчиваться любым допустимым символом, кроме пробела.
4. Нажмите на кнопку **Сохранить**.

Узел неуправляемого коммутатора появится на топологической карте. После этого вы сможете добавлять соединения с этим узлом для других узлов.

Добавление соединений для топологической карты вручную

Этот раздел содержит инструкции по добавлению соединений на топологическую карту. Вы можете вручную добавлять соединения и настраивать их параметры при работе с таблицей устройств или с топологической картой.

Добавлять соединения и настраивать их параметры могут только пользователи с ролью Администратор.

Добавление соединений для выбранного узла с настройкой дополнительных параметров топологии

Эту функцию удобно использовать, если вы хотите добавить для одного узла несколько соединений с другими узлами (например, добавить все соединения для коммутатора). При таком способе добавления соединений вы также можете настроить все параметры топологии устройства.

Чтобы добавить соединения для узла и настроить дополнительные параметры топологии:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите нужный узел в разделе **Карта сети** на вкладке **Топологическая карта**.

   Вы также можете выбрать устройство, которое представляет нужный узел, на вкладке **Карта сетевых взаимодействий** или в разделе **Активы** на вкладке **Устройства**. Однако на этих вкладках вы не сможете выбрать узел неуправляемого коммутатора.

   В правой части окна веб-интерфейса появится область деталей.

3. В правом верхнем углу области деталей нажмите на значок ⋮ и выберите пункт **Параметры топологии** → **Настроить параметры**.

   Появится окно для настройки параметров портов и соединений выбранного узла.

4. В блоке параметров **Физические порты** добавьте сведения о соединениях с другими узлами. Сведения о каждом соединении должны быть представлены в виде отдельной строки, в которой вы можете указать следующие параметры:

   - имя физического порта, к которому подключен сетевой кабель (необязательный параметр);
   - идентификаторы VLAN (необязательный параметр);
   - адреса сетевого интерфейса, связанного с портом (необязательный параметр);
   - узел, который будет являться второй стороной соединения (для выбора узла откроется окно с таблицей доступных узлов и портов на узлах).

5. При необходимости укажите сведения о виртуальных портах устройства в блоке параметров **Виртуальные порты**.

   Сведения о виртуальных портах не используются для формирования топологической карты.

6. Нажмите на кнопку **Сохранить**.

Добавление соединений для выбранных узлов без настройки дополнительных параметров топологии

Эту функцию удобно использовать, если вы хотите добавить соединения нескольких узлов с одним узлом (например, добавить соединение с одним коммутатором для каждого из выбранных узлов). При таком способе добавления соединений дополнительные параметры этих соединений остаются не заданными. В частности, вы не сможете выбрать порт на узле для добавляемых соединений. Вы можете настроить дополнительные параметры соединений после их добавления при изменении параметров топологии для узла.

Возможность добавления соединений доступна, если выбрано не более 50 узлов.

Чтобы добавить соединения для узлов без настройки дополнительных параметров соединений:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите один или несколько узлов в разделе **Карта сети** на вкладке **Топологическая карта**.

   Для выбора нескольких узлов выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

   Вы также можете выбрать устройства, которые представляют нужные узлы, на вкладке **Карта сетевых взаимодействий** или в разделе **Активы** на вкладке **Устройства**. Однако на этих вкладках вы не сможете выбрать узлы неуправляемых коммутаторов.
3. По правой кнопке мыши откройте контекстное меню.
4. В контекстном меню выберите пункт **Добавить соединение с узлом**.

   Появится окно с таблицей доступных узлов для выбора.
5. Выберите в таблице нужный узел и нажмите на кнопку **OK**.

Изменение параметров топологии для узла

При изменении параметров топологии вы можете добавлять, настраивать и удалять соединения для узла, а также настраивать параметры виртуальных портов.

Изменять параметры топологии могут только пользователи с ролью Администратор.

Чтобы настроить параметры топологии для узла:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите нужный узел в разделе **Карта сети** на вкладке **Топологическая карта**.

   Вы также можете выбрать устройство, которое представляет нужный узел, на вкладке **Карта сетевых взаимодействий** или в разделе **Активы** на вкладке **Устройства**. Однако на этих вкладках вы не сможете выбрать узел неуправляемого коммутатора.

   В правой части окна веб-интерфейса появится область деталей.

3. В правом верхнем углу области деталей нажмите на значок ⋮ и выберите пункт **Параметры топологии** → **Настроить параметры**.

   Появится окно для настройки параметров портов и соединений выбранного узла.

4. В блоке параметров **Физические порты** укажите сведения о соединениях с другими узлами. Сведения о каждом соединении должны быть представлены в виде отдельной строки, в которой вы можете указать следующие параметры:

   - имя физического порта, к которому подключен сетевой кабель (необязательный параметр);
   - идентификаторы VLAN (необязательный параметр);
   - адреса сетевого интерфейса, связанного с портом (необязательный параметр);
   - узел, который будет являться второй стороной соединения (для выбора узла откроется окно с таблицей доступных узлов и портов на узлах).

5. При необходимости укажите сведения о виртуальных портах устройства в блоке параметров **Виртуальные порты**.

   Сведения о виртуальных портах не используются для формирования топологической карты.

6. Нажмите на кнопку **Сохранить**.

Переименование узла неуправляемого коммутатора

Вы можете переименовать узел неуправляемого коммутатора, добавленный на топологическую карту автоматически или вручную.

Переименовать узел неуправляемого коммутатора могут только пользователи с ролью Администратор.

Чтобы переименовать узел неуправляемого коммутатора на топологической карте:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Карта сети** на вкладке **Топологическая карта** выберите нужный узел неуправляемого коммутатора.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Изменить**.

4. В поле с текущим именем узла введите новое имя.

   Имя узла должно быть уникальным (не совпадать с именами других неуправляемых коммутаторов) и может содержать не более 100 символов. Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ ' , . - _ = +`. Имя узла должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

5. Нажмите на кнопку **Сохранить**.

Удаление объектов топологической карты

Вы можете удалять узлы и соединения при работе с топологической картой. При удалении узлов, представляющих известные программе устройства, удаляются устройства из таблицы устройств.

Удалять объекты топологической карты могут только пользователи с ролью Администратор.

Чтобы удалить узел:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Топологическая карта** выберите узел, который вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

4. В окне запроса подтвердите удаление выбранного узла.

Чтобы удалить соединение или шину (несколько соединений):

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Топологическая карта** выберите нужное соединение или шину.
3. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

4. В окне запроса подтвердите удаление выбранных соединений.

Изменение масштаба топологической карты

Топологическая карта может отображаться в масштабе 1–100%. Текущее значение масштаба отображается в панели инструментов, которая расположена в левой части области отображения топологической карты.

Чтобы изменить масштаб топологической карты,

используйте колесико мыши или кнопки **+** и **–**, расположенные в панели инструментов рядом с текущим значением масштаба.

При уменьшении масштаба карты сокращается объем выводимой информации в узлах.

В масштабе отображения менее 25% в узлах не отображаются значки и текстовая информация. В таком масштабе на каждом узле, представляющем известное программе устройство, в правом верхнем углу отображается статус устройства в виде треугольника одного из следующих цветов:

- зеленый цвет – устройство имеет статус *Разрешенное*;
- красный цвет – устройство имеет статус *Неразрешенное*;
- серый цвет – устройство имеет статус *Неиспользуемое*.

Позиционирование топологической карты

При необходимости вы можете изменить позиционирование топологической карты вручную или автоматически. Автоматическое позиционирование позволяет переместить карту и изменить ее масштаб таким образом, чтобы на экране отображались все узлы, удовлетворяющие заданным параметрам фильтрации.

Чтобы позиционировать топологическую карту вручную:

1. Наведите курсор мыши на любое место топологической карты, не занятое объектами.
2. Удерживая нажатой левую кнопку мыши, перетащите изображение топологической карты.

Чтобы автоматически позиционировать топологическую карту,

нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения топологической карты.

Позиционирование и масштаб карты изменятся для отображения всех узлов.

Закрепление и открепление узлов на топологической карте

По умолчанию узлы не закреплены на топологической карте. Незакрепленные узлы могут автоматически перемещаться для оптимального отображения остальных объектов.

Закрепление узлов происходит при изменении их местоположения вручную. Также вы можете закрепить текущее местоположение отображаемых объектов, не перемещая их.

Для закрепления и открепления объектов без их перемещения вы можете использовать кнопки в панели инструментов, которая расположена в левой части области отображения топологической карты. С помощью кнопок и вы можете закрепить и открепить все узлы, отображаемые на топологической карте. Кнопки доступны, если на топологической карте есть объекты, к которым можно применить соответствующие действия.

После того, как местоположение узла закреплено, в правом верхнем углу этого элемента отображается значок (если для топологической карты задан масштаб не менее 25%). Вы также можете использовать этот значок для открепления объекта.

Местоположение закрепленного узла сохраняется. Если закрепленный узел перестал отображаться на топологической карте (например, после применения фильтрации), при следующем появлении этот узел отобразится на том же месте (или рядом, если это место уже занято другим закрепленным узлом).

Изменение местоположения узлов на топологической карте вручную

Вы можете вручную изменять местоположение узлов на топологической карте, распределяя их наиболее удобным для вас способом.

После перемещения узлы закрепляются на новом местоположении. При необходимости вы можете открепять эти объекты.

Чтобы изменить местоположение узлов на топологической карте:

1. На топологической карте выберите один или несколько узлов.

   Для выбора нескольких узлов выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

2. С помощью мыши перетащите выбранные объекты в нужное место.

   После перемещения узлы останутся закрепленными. В этих объектах появится значок .

Автоматическое распределение узлов на топологической карте

Для оптимального размещения объектов на топологической карте вы можете использовать алгоритм автоматического изменения местоположения (распределения) узлов. Алгоритм позволяет распределить незакрепленные узлы, имеющие соединения с другими узлами, по принципу топологической иерархии.

Чтобы распределить узлы на топологической карте,

нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения топологической карты.

После автоматического распределения незакрепленные узлы не будут закреплены на новых местах. При необходимости вы можете вручную закрепить эти объекты.

Фильтрация объектов на топологической карте

Для ограничения количества узлов, отображаемых на топологической карте, вы можете использовать функции, описанные ниже.

Фильтрация по статусам устройств

Чтобы отфильтровать объекты на топологической карте по статусам устройств:

1. В панели инструментов, которая расположена над топологической картой, откройте раскрывающийся список **Статусы устройств**.

   Появится список, содержащий названия статусов для известных программе устройств (*Неразрешенное*, *Разрешенное*, *Неиспользуемое*), а также статус *Неуправляемый коммутатор* для неуправляемых коммутаторов.

2. В раскрывающемся списке установите флажки для тех статусов, устройства с которыми нужно отобразить на топологической карте.

3. Нажмите на кнопку **OK**.

На топологической карте отобразятся только те узлы, которые имеют выбранные статусы.

Фильтрация по состояниям безопасности устройств

Чтобы отфильтровать объекты на топологической карте по состояниям безопасности устройств:

1. В панели инструментов, которая расположена над топологической картой, откройте раскрывающийся список **Состояния устройств**.

   Появится список, содержащий названия состояний безопасности для устройств (*OK*, *Важное*, *Критическое*).

2. В раскрывающемся списке установите флажки для тех состояний безопасности, устройства с которыми нужно отобразить на топологической карте.

3. Нажмите на кнопку **OK**.

На топологической карте отобразятся только те узлы, которые представляют устройства с выбранными состояниями безопасности.

Фильтрация по категориям устройств

Чтобы отфильтровать объекты на топологической карте по категориям устройств:

1. В панели инструментов, которая расположена над топологической картой, откройте раскрывающийся список **Категории устройств**.

   Появится список, содержащий названия категорий для известных программе устройств, а также отдельная категория для неуправляемых коммутаторов.

2. В раскрывающемся списке установите флажки для тех категорий, устройства с которыми нужно отобразить на топологической карте.

3. Нажмите на кнопку **OK**.

На топологической карте отобразятся только те узлы, которые представляют устройства выбранных категорий.

Фильтрация по указанным VLAN ID в параметрах топологии

Чтобы отфильтровать объекты на топологической карте по указанным VLAN ID в параметрах топологии:

1. В панели инструментов, которая расположена над топологической картой, откройте раскрывающийся список **VLAN ID**.

   Появится окно, содержащее поле для ввода идентификаторов VLAN.

2. Введите один или несколько идентификаторов VLAN, устройства с которыми нужно отобразить на топологической карте.

   Несколько идентификаторов вы можете указать через запятую и/или в виде диапазонов (например: `1, 2, 4-6, 8`).

3. Нажмите на кнопку **OK**.

   На топологической карте отобразятся только те узлы, у которых в параметрах топологии заданы порты с указанными идентификаторами VLAN.

Включение и выключение отображения узлов, не имеющих соединений с другими узлами

По умолчанию на топологической карте отображаются все узлы независимо от наличия у них соединений с другими узлами. При необходимости вы можете выключить отображение на топологической карте всех узлов, не имеющих соединений с другими узлами.

Чтобы включить или выключить отображение узлов, не имеющих соединений с другими узлами,

используйте переключатель **Отображать узлы без соединений** в панели инструментов, которая расположена над топологической картой.

Сброс параметров фильтрации

Вы можете сбросить заданные параметры фильтрации узлов в состояние по умолчанию.

Чтобы сбросить заданные параметры фильтрации на топологической карте,

в панели инструментов, которая расположена над топологической картой, нажмите на кнопку **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации).

Сохранение и загрузка параметров отображения топологической карты

Этот раздел содержит информацию о функциях для работы с параметрами отображения топологической карты.

Программа позволяет сохранить текущие параметры отображения топологической карты. Набор сохраняемых параметров отображения называется *видом*. Вы можете использовать виды для применения сохраненных в них параметров на топологической карте (например, чтобы быстро восстановить параметры отображения после каких-либо изменений или для работы с топологической картой на другом компьютере).

При сохранении вида топологической карты сохраняются следующие параметры отображения:

- масштаб;
- позиционирование топологической карты;
- местоположение закрепленных узлов;
- фильтрация узлов.

В программе можно сохранить и использовать не более 10 наборов параметров, представляющих различные виды топологической карты.

Управлять списком видов топологической карты (в том числе сохранять текущие параметры отображения) могут только пользователи с ролью Администратор. При этом просматривать список видов и применять сохраненные наборы параметров могут как пользователи с ролью Администратор, так и пользователи с ролью Оператор.

Добавление нового вида с сохранением текущих параметров отображения топологической карты

Чтобы добавить новый вид с сохранением текущих параметров отображения топологической карты:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Топологическая карта** настройте параметры отображения топологической карты.
3. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
4. Нажмите на кнопку **Добавить**.
5. В поле ввода введите имя вида.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя вида должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 100 символов;
   - не совпадает с именем другого вида (регистр символов не учитывается).
6. Нажмите на значок ✓ справа от поля ввода.

Обновление вида с сохранением текущих параметров отображения топологической карты

Чтобы обновить вид с сохранением текущих параметров отображения топологической карты:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Топологическая карта** настройте параметры отображения топологической карты.
3. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
4. Выберите вид, в котором вы хотите сохранить текущие параметры отображения топологической карты.
5. Нажмите на кнопку **Перезаписать**.

   Откроется окно с запросом подтверждения.
6. В окне запроса подтвердите сохранение текущих параметров в выбранном виде.

Переименование вида топологической карты

Чтобы переименовать вид топологической карты:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Топологическая карта** откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
3. Выберите вид, который вы хотите переименовать.
4. Нажмите на значок справа от текущего имени вида.
5. В поле ввода введите новое имя вида.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя вида должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 100 символов;
   - не совпадает с именем другого вида (регистр символов не учитывается).
6. Нажмите на значок справа от поля ввода.

Удаление вида топологической карты

Чтобы удалить вид топологической карты:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Топологическая карта** откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
3. Выберите вид, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление выбранного вида.

Применение на топологической карте параметров, сохраненных в виде

Чтобы применить параметры, сохраненные в виде, на топологической карте:

1. В разделе **Карта сети** на вкладке **Топологическая карта** откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
2. Выберите нужный вид в списке.
3. Нажмите на кнопку **Применить**.

   Откроется окно с запросом подтверждения.
4. В окне запроса подтвердите применение вида.

Поиск узлов на топологической карте

Вы можете выполнять поиск узлов на топологической карте по сведениям об этих узлах. В поиске участвуют все узлы, удовлетворяющие текущим параметрам фильтрации, в том числе находящиеся за пределами отображаемой части топологической карты.

Для узлов, представляющих известные программе устройства, поиск выполняется по всем столбцам таблицы устройств, кроме столбцов **Статус**, **Состояние безопасности**, **Последнее появление**, **Последнее изменение** и **Создано**. Поиск также выполняется по значениям пользовательских полей для устройств.

Чтобы найти нужные узлы на топологической карте,

в разделе **Карта сети** на вкладке **Топологическая карта** введите поисковый запрос в поле **Поиск узлов**. Поиск инициируется по мере ввода символов в строку поиска.

Если найдены узлы, удовлетворяющие поисковому запросу, контуры этих узлов подсвечиваются желтым цветом. При этом в правой части поля **Поиск узлов** появляются следующие элементы:

- Порядковый номер текущего выбранного узла среди результатов поиска.
- Общее количество найденных узлов.
- Стрелки для переходов между найденными узлами. Переходы выполняются в алфавитном порядке имен найденных объектов. При переходе к очередному узлу топологическая карта автоматически позиционируется для отображения этого узла.

Настройка типов событий

Типы событий задают параметры, используемые при регистрации событий: заголовки, описания, базовые оценки и параметры регистрации. В Kaspersky Industrial CyberSecurity for Networks вы можете просматривать параметры типов событий, изменять некоторые параметры типов событий и настраивать автоматическое сохранение трафика и передачу зарегистрированных событий через коннекторы.

Просмотр таблицы типов событий

Предусмотренные в программе типы событий отображаются в разделе **Параметры** → **Типы событий** веб-интерфейса программы.

Таблица типов событий содержит *системные типы событий*. Эти типы событий создаются программой при установке и не могут быть удалены из списка. Для реализованных в программе технологий регистрации событий используются различные наборы системных типов событий.

На основе некоторых системных типов событий могут быть настроены *пользовательские параметры событий*, которые будут использоваться при регистрации событий в определенных случаях. Пользовательские параметры могут быть заданы для следующих типов событий:

- тип события по технологии Контроль технологического процесса с кодом 4000002900 – для регистрации событий по правилам контроля процесса;
- тип события по технологии Внешние системы с кодом 4000005400 – для регистрации событий с использованием Kaspersky Industrial CyberSecurity for Networks API.

Пользовательские параметры имеют приоритет при регистрации событий. Параметры, заданные в системных типах событий, используются в том случае, если не заданы пользовательские параметры.

Для типов событий предусмотрены следующие параметры:

- **Код** – уникальный номер типа события. В таблице типов событий номер отображается вместе с заголовком события в столбце **Код и заголовок**. В таблице зарегистрированных событий номер типа события отображается в столбце **Тип события**.

- **Заголовок** – содержимое заголовка события, представленное текстом и/или переменными. В системных типах событий могут использоваться специфические переменные только для этих типов событий (например, переменная `$systemCommandShort` в типе события по технологии Контроль системных команд) или общие переменные, которые также можно использовать и в пользовательских параметрах (например, переменная `$top_level_protocol` в типе события по технологии Контроль целостности сети). В таблице типов событий содержимое заголовка отображается вместе с номером типа события в столбце **Код и заголовок**. В таблице зарегистрированных событий текст заголовка и/или полученные значения переменных отображаются в столбце **Заголовок**.

- **Базовая оценка** – исходное значение для расчета оценки зарегистрированного события. Если у типа события могут быть различные базовые оценки, то отображается максимальное значение. Этот параметр отображается в таблице типов событий.

- **Технология** – технология регистрации события. Этот параметр отображается в таблице типов событий.

- **Описание** – дополнительный текст, описывающий тип события. Аналогично заголовку, может содержать переменные. Этот параметр не отображается в таблице типов событий (вы можете просмотреть описание в области деталей выбранного типа события). В таблице зарегистрированных событий текст описания и/или полученные значения переменных отображаются в столбце **Описание**.

- **<Имя коннектора-получателя>** – имя коннектора, через который программа передает события в стороннюю систему. Программа передает в сторонние системы события только тех типов, для которых настроена передача событий через коннектор. Каждый коннектор, через который настроена передача событий в сторонние системы, отображается в отдельном столбце таблицы типов рисков. Этот параметр не отображается в области деталей выбранного типа событий.

- **Время разрешения повтора события** – максимальный период времени, по истечении которого разрешается повторная регистрация события. Если до истечения заданного периода времени повторяются условия для регистрации события, то новое событие не регистрируется, а увеличивается счетчик количества повторов ранее зарегистрированного события и обновляются дата и время последнего появления события. После окончания этого периода при повторении условий для регистрации события программа зарегистрирует новое событие такого типа. Период разрешения повтора отсчитывается от момента последней регистрации события такого типа. Например, если задано время 8 часов, то при обнаружении условий для регистрации этого события через два часа после предыдущего события, новое событие не будет зарегистрировано. Новое событие будет зарегистрировано при обнаружении условий для регистрации через 8 часов и более. Этот параметр не отображается в таблице типов событий (вы можете просмотреть и настроить этот параметр в области деталей выбранного типа события).

  > Для зарегистрированных событий время разрешения повтора может наступить раньше заданного периода. Повторная регистрация события разрешается раньше заданного периода, если событию присвоен статус *Обработано*, а также если был перезагружен компьютер, который выполняет функции Сервера.

- **Сохранять трафик** – параметр для включения/выключения автоматического сохранения трафика при регистрации события. Этот параметр не отображается в таблице типов событий (вы можете просмотреть и настроить этот параметр в области деталей выбранного типа события).

  > Если автоматическое сохранение трафика выключено, вы можете загружать трафик вручную в течение некоторого времени после регистрации события этого типа. При поступлении запроса на загрузку трафика программа выполняет поиск сетевых пакетов в файлах дампа трафика, временно создаваемых программой. Если в файлах дампа трафика найдены нужные сетевые пакеты, они загружаются (с предварительным сохранением в базе данных).

При просмотре таблицы типов событий вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Изменение параметров системного типа события

Чтобы изменить параметры системного типа события:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Типы событий**.
3. В таблице типов событий выберите тип события, который вы хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Настройте изменяемые параметры: время разрешения повтора события и параметры сохранения трафика.
6. Нажмите на кнопку **Сохранить**.

Настройка автоматического сохранения трафика для системных типов событий

При изменении типов событий вы можете включать и выключать автоматическое сохранение трафика для событий при их регистрации. Если сохранение трафика включено, в базе данных сохраняется сетевой пакет, вызвавший регистрацию события, а также пакеты до и после регистрации события, обнаруженные в рамках сетевого сеанса, в котором было зарегистрировано событие. Параметры сохранения трафика определяют количество сохраняемых сетевых пакетов и ограничения по времени.

Если автоматическое сохранение трафика выключено для типа события (и для этого типа события не заданы пользовательские параметры, включающие автоматическое сохранение трафика), возможность загрузки трафика будет доступна только в течение некоторого времени после регистрации события этого типа. В этом случае для загрузки трафика программа использует файлы дампа трафика (эти файлы хранятся временно и автоматически удаляются по мере поступления трафика). При загрузке трафика из этих файлов в базе данных сохраняются сетевые пакеты в том объеме, который задан по умолчанию при включении сохранения трафика для типов событий.

> Программа сохраняет трафик в базе данных только при регистрации события. Если в течение времени разрешения повтора события повторяются условия для регистрации этого события, трафик на этот момент времени не сохраняется в базе данных.

Вы можете включить и настроить сохранение трафика для любых типов событий, кроме системного типа события, которому присвоен код 4000002700. Событие с кодом 4000002700 регистрируется при отсутствии трафика на точке мониторинга, поэтому для этого типа события наличие трафика не предполагается.

Если включено сохранение трафика для инцидентов (то есть для системного типа события, которому присвоен код 8000000001), то при регистрации инцидента программа сохраняет трафик для всех вложенных событий инцидента. Для сохранения трафика вложенных событий применяются параметры, заданные для инцидента. При этом параметры сохранения трафика, заданные непосредственно для типов событий, вложенных в инцидент, имеют приоритет перед параметрами, заданными для инцидента. То есть трафик для вложенных событий инцидента будет сохранен в соответствии с параметрами, заданными для типов этих событий, а при отсутствии таких параметров – в соответствии с параметрами, заданными для инцидента.

Чтобы включить и настроить параметры сохранения трафика для типа события:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Типы событий**.
3. В таблице типов событий выберите тип события, который вы хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Установите переключатель **Сохранять трафик** в положение *Включено*.

6. Настройте сохранение трафика до момента регистрации события. Для этого укажите нужные значения в полях **Пакетов до события, шт** и/или **Время до события, мс**. При нулевом значении параметр не применяется. Если значения заданы в обоих этих полях, программа будет сохранять минимальное количество пакетов, которое соответствует одному из заданных значений.

7. Настройте сохранение трафика после момента регистрации события. Для этого укажите нужные значения в полях **Пакетов после события, шт** и/или **Время после события, мс**. При нулевом значении параметр не применяется. Если значения заданы в обоих этих полях, программа будет сохранять минимальное количество пакетов, которое соответствует одному из заданных значений.

   Для некоторых технологий (в частности, Контроль технологического процесса) в событиях может сохраняться меньше пакетов после момента регистрации, чем задано параметрами сохранения трафика. Это связано с технологическими особенностями отслеживания трафика.

8. Нажмите на кнопку **Сохранить**.

Настройка передачи событий через коннекторы

При настройке системных типов событий вы можете указать коннекторы, через которые Kaspersky Industrial CyberSecurity for Networks будет передавать зарегистрированные события в сторонние системы (например, в Kaspersky Security Center). Kaspersky Industrial CyberSecurity for Networks может передавать информацию о событиях одновременно через несколько коннекторов.

Чтобы настроить передачу событий через коннекторы в сторонние системы:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Типы событий**.

3. Убедитесь, что в таблице типов событий отображаются столбцы с нужными коннекторами.

   Если столбец с нужным коннектором отсутствует, проверьте параметры отображения столбцов. Если коннектор не был добавлен в список коннекторов, добавьте его.

4. В таблице типов событий выберите типы событий, для которых вы хотите включить или выключить передачу через коннекторы.

   Если вы выбрали один тип события, в правой части окна веб-интерфейса появится область деталей.

5. Выполните одно из следующих действий:

   - Если вы выбрали один тип события, в области деталей нажмите на кнопку **Выбрать коннекторы**.
   - Если вы выбрали несколько типов событий, в верхней части окна нажмите на кнопку **Выбрать коннекторы**.

   Откроется окно **Коннекторы-получатели событий**.

6. Установите флажки напротив тех коннекторов, через которые вы хотите передавать события в сторонние системы.

7. Нажмите на кнопку **OK**.

Общие переменные для подстановки значений в Kaspersky Industrial CyberSecurity for Networks

Для подстановки текущих значений в Kaspersky Industrial CyberSecurity for Networks могут использоваться общие переменные. Вы можете использовать общие переменные в следующих параметрах:

- заголовки и описания событий в пользовательских параметрах для регистрации событий (например, в правилах контроля процесса);
- параметры передачи событий, сообщений программы или записей аудита через коннектор для электронной почты.

Чтобы вставить общую переменную в поле ввода,

начните вводить имя переменной с символа $ и выберите подходящую общую переменную в появившемся списке.

В зависимости от своего назначения, общие переменные могут использоваться для подстановки значений в различных параметрах (см. таблицу ниже).

Общие переменные для подстановки значений

Переменная	Назначение	Где используется
`$communications`	Строки описания сетевых взаимодействий (по одной строке на каждое сетевое взаимодействие) с указанием протокола и адресов отправителя и получателя сетевого пакета	• Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.
`$dst_address`	Адрес получателя сетевого пакета (в зависимости от доступных в протоколе данных это могут быть IP-адрес, номер порта, MAC-адрес и/или другие адресные данные)	• Пользовательские параметры для регистрации событий.
`$extra.<paramName>`	Дополнительная переменная, добавленная с помощью функции `AddEventParam` для внешней системы или Lua-скрипта	• Пользовательские параметры для регистрации событий.
`$rule_max_value`	Заданное максимальное значение в правиле контроля процесса	• Пользовательские параметры для регистрации событий.
`$rule_min_value`	Заданное минимальное значение в правиле контроля процесса	• Пользовательские параметры для регистрации событий.
`$monitoring_point`	Имя точки мониторинга, трафик с которой вызвал регистрацию события	• Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.
`$occurred`	Дата и время регистрации	• Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.

`$protocol`	Название протокола прикладного уровня, при отслеживании которого зарегистрировано событие	• Пользовательские параметры для регистрации событий.
`$src_address`	Адрес отправителя сетевого пакета (в зависимости от доступных в протоколе данных это могут быть IP-адрес, номер порта, MAC-адрес и/или другие адресные данные)	• Пользовательские параметры для регистрации событий.
`$tags`	Список всех имен и значений тегов, указанных в правиле контроля процесса	• Пользовательские параметры для регистрации событий.
`$technology_rule`	Имя правила в событии	• Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.
`$top_level_protocol`	Название протокола верхнего уровня	• Пользовательские параметры для регистрации событий.
`$type_id`	Код типа события, сообщения программы или записи аудита	• Пользовательские параметры для регистрации событий (также может использоваться переменная `$event_type_id`). • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
`$rule_values`	Список значений правила контроля процесса (разрешенных или запрещенных)	• Пользовательские параметры для регистрации событий.
`$closed`	Дата и время присвоения статуса *Обработано* или дата и время разрешения повтора события (для событий, не являющихся инцидентами), либо дата и время регистрации последнего события, включенного в инцидент (для инцидентов)	• Параметры передачи событий через коннектор.
`$count`	Количество срабатываний события или инцидента	• Параметры передачи событий через коннектор.
`$description`	Описание	• Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
`$id`	Уникальный идентификатор зарегистрированного события, сообщения программы или записи аудита	• Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
`$message_category`	Категория переданных данных (событие, сообщение программы или запись аудита)	• Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.

`$message_count`	Количество передаваемых событий, сообщений программы или записей аудита	• Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
`$messages`	Шаблон, представляющий собой блок со списком данных	• Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
`$msg_line_templ`	Шаблон строк для уведомлений в письмах	• Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
`$node`	Узел с установленным компонентом программы, от которого поступили данные	• Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
`$result`	Результат действия в записи аудита	• Параметры передачи записей аудита через коннектор.
`$score`	Значение оценки события	• Параметры передачи событий через коннектор.
`$severity`	Уровень критичности события	• Параметры передачи событий через коннектор.
`$status`	Статус сообщения программы	• Параметры передачи сообщений программы через коннектор.
`$system_process`	Процесс программы, который вызвал регистрацию сообщения	• Параметры передачи сообщений программы через коннектор.
`$technology`	Технология, к которой относится событие	• Параметры передачи событий через коннектор.
`$title`	Заголовок события, текст сообщения или зарегистрированное действие	• Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
`$user`	Имя пользователя, который совершил зарегистрированное действие	• Параметры передачи записей аудита через коннектор.

Настройка типов рисков

Типы рисков задают параметры, используемые при регистрации рисков в Kaspersky Industrial CyberSecurity for Networks: названия, категории и базовые оценки для рисков. Вы можете просматривать параметры типов рисков и при необходимости изменять значения базовых оценок для некоторых типов рисков.

После установки программы используется исходный список типов рисков. Вы можете обновлять и дополнять поддерживаемые типы рисков, устанавливая обновления.

Просмотр таблицы типов рисков

Таблица типов рисков отображается в разделе **Параметры** → **Типы рисков** веб-интерфейса программы.

Параметры типов рисков отображаются в следующих столбцах таблицы:

- **Код**.

  Уникальный номер типа риска. В таблице зарегистрированных рисков номер типа риска отображается в области деталей выбранного риска.

- **Название**.

  Название типа риска, отображаемое в таблице типов рисков. При регистрации риска его название может не полностью совпадать с названием использованного типа риска. Названия некоторых типов рисков могут быть полностью заменены на другие названия для зарегистрированных рисков. В частности, к типам рисков с такими названиями относятся типы рисков **Риск от внешней системы**. Если такой тип риска используется при регистрации риска, в программе будет сохранено название риска, указанное в источнике сведений о риске (например, в стороннем приложении, которое использует Kaspersky Industrial CyberSecurity for Networks API).

- **Категория**.

  Название категории риска.

- **Базовая оценка**.

  Исходное значение для расчета оценки зарегистрированного риска. Заданные значения базовых оценок применяются при регистрации всех рисков, кроме рисков от внешних систем. Типы рисков с названиями **Риск от внешней системы** имеют нулевые значения базовых оценок. Базовые оценки для таких рисков должны быть указаны в сторонних приложениях, которые регистрируют риски с помощью Kaspersky Industrial CyberSecurity for Networks API.

При просмотре таблицы типов рисков вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Изменение базовой оценки для типа риска

Изменение базовых оценок недоступно для типов рисков с названием **Риск от внешней системы**. Если такой тип риска используется для регистрации риска, базовая оценка этого риска должна быть определена из источника сведений о риске (например, сторонним приложением, которое использует Kaspersky Industrial CyberSecurity for Networks API).

Чтобы изменить базовую оценку для типа риска:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Типы рисков**.
3. В таблице типов рисков выберите тип риска, для которого вы хотите изменить базовую оценку.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Укажите нужное значение базовой оценки.
6. Нажмите на кнопку **Сохранить**.

Управление параметрами хранения рисков

Вы можете изменить ограничения максимального объема для хранения рисков.

Чтобы изменить параметры хранения рисков:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку Сервера.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров Сервера.
5. На вкладке **Общие** перейдите к блоку параметров **Риски** и задайте ограничение занимаемого объема для хранения рисков с помощью параметра **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.

6. При необходимости с помощью параметра **Время хранения (дней)** включите ограничение на минимальное время хранения рисков и укажите нужное количество дней для хранения.

7. Нажмите на кнопку **Сохранить**.

Управление наборами правил для заданий аудита настроек и уязвимостей

Вы можете управлять наборами правил для заданий аудита настроек и уязвимостей в разделе **Аудит безопасности** на вкладке **Наборы правил**. После установки обновлений баз и программных модулей по умолчанию используются системные наборы правил для заданий аудита настроек и уязвимостей.

Управлять наборами правил для заданий аудита настроек и уязвимостей могут только пользователи с ролью Администратор.

Правила аудита настроек и уязвимостей

В Kaspersky Industrial CyberSecurity for Networks поддерживаются правила аудита настроек и уязвимостей, написанные на следующих языках:

- OVAL (Open Vulnerability and Assessment Language) – открытый язык описания уязвимостей и оценки конфигураций информационных систем. Язык стандартизирует способы подачи информации, процесс анализа системы и формат выдаваемого результата.

  Правила, использующие только этот язык, представляют собой OVAL-определения, которые формализуют предъявляемые требования к информационным системам, предоставляя возможности автоматизированной обработки этих требований.

- XCCDF (The Extensible Configuration Checklist Description Format) – язык на основе XML для описания контрольных списков параметров безопасности. XCCDF-документы обычно содержат наборы требований к информационным системам.

  Правила, использующие этот язык, представляют собой списки высокоуровневых требований в виде документов с профилями и группами данных. Для автоматизированной обработки такие правила должны содержать связанные с ними OVAL-определения.

Правила аудита настроек и уязвимостей группируются в наборы правил. Вы можете использовать следующие типы наборов правил:

- Системные наборы правил. Эти наборы правил поставляются и обновляются вместе с обновлениями баз и программных модулей. Чтобы использовать системные наборы правил, вам нужно установить обновления.

- Пользовательские наборы правил. Эти наборы правил пользователь самостоятельно загружает в программу путем импорта файлов.

При загрузке набора правил программа выполняет проверку содержащихся в нем правил. Если в проверяемых правилах обнаружены ошибки, программа блокирует применение таких правил. Если обнаружены ошибки во всех правилах набора или набор не содержит правил, программа блокирует применение всего набора.

При создании или изменении заданий аудита настроек и уязвимостей вы можете выбирать правила, по которым будут выполняться проверки.

Просмотр таблицы наборов правил аудита настроек и уязвимостей

Таблица наборов правил аудита настроек и уязвимостей отображается в разделе **Аудит безопасности** на вкладке **Наборы правил**.

Параметры наборов правил отображаются в следующих столбцах таблицы:

- **ID**.

  Идентификатор набора правил, присвоенный в Kaspersky Industrial CyberSecurity for Networks.

- **Имя**.

  Имя, под которым набор правил представлен в программе.

- **Описание**.

  Описание набора правил.

- **Издатель**.

  Название издателя XCCDF-документа (если указано).

- **Версия XCCDF-документа**.

  Информация о версии XCCDF-документа (если указана).

- **Статус XCCDF**.

  Финальный статус, указанный для XCCDF-документа.

- **Профилей XCCDF**.

  Количество профилей в XCCDF-документе.

- **Правил XCCDF в наборе**.

  Количество правил в XCCDF-документе.

- **OVAL-определений**.

  Количество OVAL-определений.

- **Создано**.

  Дата и время добавления набора правил в программу.

- **Изменено**.

  Дата и время последнего изменения набора правил в программе.

- **Источник**.

  Тип набора правил, определяющий способ загрузки набора в программу: системный или пользовательский набор.

При просмотре таблицы наборов правил вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Импорт наборов правил аудита настроек и уязвимостей

Вы можете импортировать в Kaspersky Industrial CyberSecurity for Networks правила аудита настроек и уязвимостей из файлов. Файлы могут содержать правила, написанные на языке OVAL или на языке XCCDF с использованием OVAL-определений.

Импортированные наборы правил называются *пользовательскими*. У этих наборов правил параметр **Источник** содержит значение **Пользователь**.

Для импорта файлы должны быть упакованы в ZIP-архив. Поддерживаемые варианты для содержимого ZIP-архива:

- Файлы XCCDF-пакета, представляющие XCCDF-документ и OVAL-определения в формате XML. Если пакет включает файлы справочника в формате CPE (Common Platform Enumeration), эти файлы также нужно добавить в архив.

  Файлы должны быть размещены в корне архива. Имена файлов в архиве должны соответствовать следующим маскам имен:

  - `*-xccdf.xml` – маска для имени файла XCCDF-документа (например: SCAP1-xccdf.xml);
  - `*-oval.xml` – маска для имени файла с OVAL-определениями (например: SCAP1-oval.xml);
  - `*-cpe-dictionary.xml` – маска для имени файла CPE-справочника (например: SCAP1-cpe-dictionary.xml);
  - `*-cpe-oval.xml` – маска для имени файла с OVAL-определениями к CPE-справочнику (например: SCAP1-cpe-oval.xml).

- Файл, содержащий OVAL-определения и не являющийся частью XCCDF-пакета (для использования файла не требуется XCCDF-документ).

  Файл должен быть размещен в корне архива. Имя файла в архиве должно соответствовать маске: `*-oval.xml` (например: SCAP2-oval.xml).

Чтобы импортировать набор правил аудита настроек и уязвимостей:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Наборы правил** нажмите на кнопку **Импорт** в панели инструментов.
4. Укажите локальный путь к ZIP-архиву с помощью кнопки **Обзор**.

5. Нажмите на кнопку **Импортировать**.

   Запустится процесс импорта данных. Сведения о выполнении операции импорта отображаются в списке фоновых операций.

6. Для перехода к новому набору правил выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции импорта.

   c. Нажмите на кнопку **Показать**.

Изменение наборов правил аудита настроек и уязвимостей

Для пользовательских наборов правил аудита настроек и уязвимостей вы можете изменять имена и текстовые описания. Для системных наборов правил такие изменения недоступны.

Чтобы изменить имя и/или текстовое описание набора правил:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Аудит безопасности**.

3. На вкладке **Наборы правил** выберите нужный набор правил.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.

5. Введите имя и/или описание набора правил.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . ' - " _`. Имя набора должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

   Имя набора должно содержать не более 1024 символов. Описание набора должно содержать не более 4096 символов.

6. Нажмите на кнопку **Сохранить**.

Удаление наборов правил аудита настроек и уязвимостей

Вы можете удалять пользовательские и системные наборы правил аудита настроек и уязвимостей. При этом невозможно удалять наборы, с которыми связаны задания.

Чтобы удалить наборы правил:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Аудит безопасности**.
3. На вкладке **Наборы правил** выберите наборы, которые вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление наборов правил.

   Из выбранных наборов правил вы можете удалить только такие наборы, с которыми не связаны задания аудита настроек и уязвимостей. Если среди выбранных наборов правил есть наборы, с которыми связаны задания, на экране появится сообщение об этом. Для удаления таких наборов правил вам нужно предварительно удалить связанные задания.

Управление секретами с учетными данными для удаленных подключений

В Kaspersky Industrial CyberSecurity for Networks реализовано хранилище секретов. *Секреты* позволяют безопасно хранить и использовать идентификационную и аутентификационную информацию, которая необходима программе для автоматических удаленных подключений к устройствам. Секреты применяются в заданиях для аудита безопасности, в которых выбран способ опроса устройств **Удаленное подключение** или настроено использование коннектора типа **Active poll**.

В программе предусмотрены различные типы секретов. В зависимости от назначения секрета вы можете выбирать нужный тип и вводить соответствующие данные при добавлении или изменении параметров секрета.

Вам нужно сохранять в секретах такие учетные данные, которые необходимы для удаленных подключений к устройствам по протоколам удаленных подключений. В заданиях для аудита безопасности, в которых выбран способ опроса устройств **Удаленное подключение**, для удаленных подключений используется протокол SSH. Коннекторы типа **Active poll** могут использовать для удаленных подключений различные протоколы, в зависимости от выбранных методов опроса.

Для безопасного использования идентификационной и аутентификационной информации, хранящейся в секретах, в программе реализована защита от компрометации секретов при удаленных подключениях к устройствам. После сохранения в программе открытых ключей, полученных от устройств, программа контролирует все последующие удаленные подключения к этим устройствам и не отправляет информацию из секретов в случае подмены устройств в сети.

Критически важная информация секрета (пароль или закрытый ключ сертификата) доступна вам в открытом виде только один раз – при вводе этой информации во время создания секрета. После сохранения секрета его критически важную информацию невозможно просмотреть. Вы можете только заменить критически важную информацию секрета на новую при изменении секрета (например, ввести другой пароль).

Вы можете управлять секретами в разделе **Параметры** → **Секреты**. В программу можно добавить не более 500 секретов.

Управлять секретами могут только пользователи с ролью Администратор.

Добавление секрета

Вы можете добавлять секреты в хранилище секретов программы.

Чтобы добавить секрет:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Секреты**.
3. Откройте область деталей по ссылке **Добавить секрет**.
4. Введите имя секрета.

   Имя секрета должно быть уникальным (не совпадать с именами других секретов) и может содержать до 256 символов. Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. Имя секрета должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

5. Выберите тип секрета и настройте его параметры.

   Для выбора доступны следующие типы секретов:

   - **Только пароль** – этот тип секрета применяется, если для доступа к конфигурационным данным устройства требуется только пароль пользователя, обладающего необходимыми правами.

   - **Имя и пароль пользователя** – этот тип секрета применяется, если для получения данных от устройства требуется указать имя пользователя и его пароль.

   - **Имя и пароль пользователя, пароль для root** – этот тип секрета применяется, если для получения данных от устройства требуется указать имя пользователя и его пароль, а для подключения с привилегиями администратора (с root-правами) дополнительно требуется пароль учетной записи root или учетной записи для обработки запросов с привилегиями администратора.

   - **Имя и пароль пользователя, пароль шифрования** – этот тип секрета применяется, если для получения данных от устройства требуется указать имя пользователя и его пароль, а для установки зашифрованных соединений дополнительно требуется пароль шифрования.

   - **Смешанный** – этот тип секрета применяется для способа опроса устройств **Удаленное подключение** в заданиях аудита настроек и уязвимостей или в заданиях контроля конфигураций. Для секрета этого типа вы можете задать следующие параметры:

     - Имя пользователя, которое будет использоваться для удаленных подключений к устройствам.

       Имя пользователя может содержать буквы латинского алфавита, цифры, точки, а также специальные символы `_` и `-`. Имя должно начинаться с буквы и заканчиваться любым поддерживаемым символом, кроме точки.

     - **Пароль пользователя** – если для аутентификации будет использоваться пароль пользователя.

       Пароль должен содержать до 256 символов ASCII.

     - **Закрытый ключ** – если для аутентификации будет использоваться закрытый ключ сертификата.

       Вы можете ввести последовательность символов ключа вручную или загрузить ключ из файла сертификата по ссылке **Копировать из файла**. Для загрузки закрытых ключей поддерживаются файлы форматов CRT, PEM, CER. Если файл с закрытым ключом защищен парольной фразой, перед загрузкой ключа введите парольную фразу в поле **Парольная фраза**.

       > Для использования закрытого ключа сертификата вам нужно скопировать открытый ключ этого сертификата на все устройства, к которым будут выполняться удаленные подключения с помощью секрета. Действия для копирования открытого ключа на устройства выполняются без участия Kaspersky Industrial CyberSecurity for Networks.

     Пароль для пользователя root – если требуется дополнительный пароль для подключений к сетевому оборудованию с привилегиями администратора (с root-правами). Запрос доступа в таких случаях выполняется от имени учетной записи root или от имени той учетной записи, которая задана на сетевом оборудовании для обработки запросов с привилегиями администратора.

6. Нажмите на кнопку **Создан**.

Просмотр таблицы секретов

Таблица секретов для удаленных подключений отображается в разделе **Параметры → Секреты** веб-интерфейса программы.

Сведения о секретах отображаются в следующих столбцах таблицы:

- **Имя секрета**.

  Имя, под которым секрет представлен в программе.

- **Создан**.

  Дата и время добавления секрета в программу.

- **Изменен**.

  Дата и время последнего изменения секрета в программе.

При просмотре таблицы секретов вы можете использовать функции настройки, фильтрации, поиска и сортировки.

Защита от компрометации секретов при удаленных подключениях к устройствам

Идентификационная и аутентификационная информация из секретов должна использоваться при удаленных подключениях только к тем устройствам, которые выбраны для заданий аудита безопасности. Для защиты этой информации от компрометации, которая возможна в случае подмены устройства, перед ее отправкой программа проверяет открытый ключ, полученный от этого устройства. Открытый ключ используется на устройстве для установки SSH-соединений. Открытый ключ позволяет программе удостовериться в том, что SSH-соединение устанавливается с правильным устройством. Передача идентификационной и аутентификационной информации на устройство происходит после проверки идентичности полученного открытого ключа и открытого ключа, сохраненного в программе.

Сохраненный открытый ключ устройства отображается в области деталей выбранного устройства на вкладке **Общие**.

Получение и сохранение открытых ключей устройств в программе

В Kaspersky Industrial CyberSecurity for Networks по умолчанию не заданы открытые ключи устройств. Получение и сохранение открытого ключа устройства происходит при первой установке SSH-соединения с этим устройством для сканирования в рамках задания аудита безопасности способом опроса **Удаленное подключение** или с использованием коннектора типа **Active poll**. При этом идентификационная и аутентификационная информация из выбранного секрета передается на устройство без проверки полученного открытого ключа. Поэтому перед первым запуском задания аудита безопасности, для которого выбрано это устройство и будет устанавливаться SSH-соединение, вам нужно убедиться в отсутствии подменного устройства в сети. Для этого, например, вы можете проверить совпадение IP-адресов устройства, заданных в программе, и IP-адресов на сетевых интерфейсах самого устройства с помощью команды `ifconfig`.

Сброс сохраненных открытых ключей устройств

С течением времени на устройствах могут изменяться ключи, используемые для установки SSH-соединений. Например, пользователи устройств могут выполнять процедуры генерации новых ключей при угрозе компрометации текущих закрытых ключей.

При смене закрытого ключа на устройстве происходит смена открытого ключа. После изменения открытого ключа программа не передает на это устройство информацию из секретов из-за несовпадения нового открытого ключа и открытого ключа, сохраненного в программе. Как следствие, следующие сканирования устройства в рамках заданий аудита безопасности завершаются с ошибкой.

После изменения открытого ключа на устройстве вам нужно сбросить текущий сохраненный открытый ключ этого устройства в программе. Это позволит снова использовать секреты при удаленных подключениях к устройству.

После сброса сохраненного открытого ключа программа сохранит новый полученный открытый ключ при следующей установке SSH-соединения с этим устройством. При этом вам нужно убедиться в отсутствии подменного устройства в сети аналогично, как при первичном получении и сохранении открытого ключа.

Сбросить сохраненные открытые ключи устройств могут только пользователи с ролью Администратор.

Чтобы сбросить сохраненные открытые ключи устройств:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На вкладке **Устройства** выберите устройства, для которых вы хотите сбросить сохраненные открытые ключи.
4. По правой кнопке мыши откройте контекстное меню одного из выбранных устройств.
5. В контекстном меню выберите пункт **Сбросить открытый ключ**.

   Откроется окно с запросом подтверждения.
6. В окне запроса нажмите на кнопку **ОК**.

Изменение параметров секрета

При изменении параметров секрета вы можете изменить его тип и/или задать другие значения для учетных данных.

После изменения параметров секрета (в том числе после изменения имени секрета) новые параметры применяются в заданиях для аудита безопасности, в которых этот секрет был указан ранее. Если вы изменяете тип секрета, при следующих запусках этих заданий могут возникать ошибки в тех случаях, когда новый тип секрета не соответствует параметрам заданий.

Чтобы изменить параметры секрета:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Секреты**.
3. Выберите секрет, который вы хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.

5. Измените нужные параметры. Для изменения параметров вам доступны те же действия, что и при добавлении секрета.

   Критически важная информация секрета (пароли и закрытый ключ сертификата) не отображается в открытом виде. Вы можете только заменить критически важную информацию секрета на новую с помощью ссылок, расположенных над полями с учетными данными.

Удаление секретов

Вы можете удалять секреты из хранилища секретов Kaspersky Industrial CyberSecurity for Networks.

Перед удалением секрета рекомендуется указать другой секрет или другой способ опроса в заданиях для аудита безопасности, в которых указан этот секрет. Если удаленный секрет остался указанным в задании для аудита безопасности, при следующих запусках этого задания будут возникать ошибки.

Чтобы удалить секреты:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Секреты**.

3. Выберите секреты, которые вы хотите удалить.

4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

5. В окне запроса подтвердите удаление секретов.

Управление отчетами и шаблонами отчетов

Kaspersky Industrial CyberSecurity for Networks может формировать отчеты с информацией о состоянии устройств и безопасности системы, отслеживаемых параметрах технологического процесса и системных командах, а также об обнаруженных рисках и взаимодействиях со сторонними устройствами. Программа формирует такие отчеты в соответствии с *шаблонами отчетов*. Шаблон отчета – это набор параметров, определяющих условия формирования отчета. Шаблоны могут быть системными (созданными при установке программы) и пользовательскими (созданными путем дублирования шаблонов).

В разделе **Отчеты** пользователь с ролью Администратор может дублировать шаблоны для создания пользовательских шаблонов отчетов, изменять и удалять шаблоны отчетов, а также удалять сформированные отчеты и отменять формирование отчетов.

Отчеты сохраняются в виде файлов в формате PDF.

Kaspersky Industrial CyberSecurity for Networks также может формировать отчеты с результатами сканирования устройств в рамках задания аудита настроек и уязвимостей, а также отчеты о запуске всего задания аудита настроек и уязвимостей. Запуск формирования отчетов выполняется в разделе **Аудит безопасности**. Просмотреть сформированные отчеты вы можете на вкладке **Сформированные отчеты**.

Дублирование шаблона отчета

В текущей версии Kaspersky Industrial CyberSecurity for Networks вы можете создавать пользовательские шаблоны путем дублирования существующих шаблонов отчетов. Вы можете дублировать как системные, так и пользовательские шаблоны. При дублировании шаблона вы не можете изменять состав и расположение информационных блоков в отчете.

Максимальное количество шаблонов в программе – 5000.

Дублировать шаблоны отчетов могут только пользователи с ролью Администратор.

Чтобы дублировать шаблон отчета:

1. Выберите раздел **Отчеты**.
2. На вкладке **Шаблоны отчетов** выберите нужный шаблон.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Создать новый шаблон**.
4. В поле **Имя** измените название шаблона отчета.

   Вы можете использовать буквы русского и латинского алфавитов, цифры, пробел, а также символы -, – и _.

   Название шаблона отчета должно удовлетворять следующим требованиям:

   - не совпадает с названием другого шаблона отчета (регистр символов не учитывается);
   - содержит до 100 символов.

   Названия отчетов, сформированные по обновленному шаблону, будут соответствовать новому названию шаблона.
5. В раскрывающемся списке **Период для данных** выберите период времени, за который вы хотите получить информацию о системе в отчете.

   Вы можете формировать отчеты с информацией, поступившей в программу, за последние 24 часа, 7 дней, 30 дней, за последний год или задать период вручную.
6. Если требуется запускать формирование отчетов по расписанию, включите переключатель **Формирование отчета по расписанию** и настройте параметры расписания:

   a. В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять формирование отчета: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.

   b. В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска формирования отчета.
7. Если требуется, в поле **Адреса получателей** введите адрес электронной почты, на которую вы хотите отправлять сформированные отчеты. Если требуется указать дополнительных получателей отчета, нажмите на кнопку **Добавить адрес получателя** и введите адрес электронной почты.

   Максимальное количество получателей отчета – 20.
8. Нажмите на кнопку **Сохранить**.

В таблице шаблонов отчетов отобразится новый шаблон отчета.

Изменение шаблона отчета

Изменять параметры шаблона отчета могут только пользователи с ролью Администратор.

Чтобы изменить параметры шаблона отчета:

1. Выберите раздел **Отчеты**.
2. На вкладке **Шаблоны отчетов** выберите нужный шаблон.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. В поле **Имя** измените название шаблона отчета.

   Вы можете использовать буквы русского и латинского алфавитов, цифры, пробел, а также символы -, – и _.

   Название шаблона отчета должно удовлетворять следующим требованиям:

   - не совпадает с названием другого шаблона отчета (регистр символов не учитывается);
   - содержит до 100 символов.

   Названия отчетов, сформированные по обновленному шаблону, будут соответствовать новому названию шаблона.
5. В раскрывающемся списке **Период для данных** выберите период времени, за который вы хотите получить информацию о системе в отчете.

   Вы можете формировать отчеты с информацией, поступившей в программу, за последние 24 часа, 7 дней, 30 дней, за последний год или задать период вручную.
6. Если требуется запускать формирование отчетов по расписанию, включите переключатель **Формирование отчета по расписанию** и настройте параметры расписания:

   a. В раскрывающемся списке **Периодичность** выберите, как часто требуется выполнять формирование отчета: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.

   b. В зависимости от выбранного варианта задайте значения параметров, чтобы уточнить время запуска формирования отчета.
7. Если требуется, в поле **Адреса получателей** введите адрес электронной почты, на которую вы хотите отправлять сформированные отчеты. Если требуется указать дополнительных получателей отчета, нажмите на кнопку **Добавить адрес получателя** и введите адрес электронной почты.

   Максимальное количество получателей отчета – 20.
8. Нажмите на кнопку **Сохранить**.

Изменения отобразятся в соответствующих столбцах таблицы шаблонов отчетов.

Удаление шаблона отчета

Вы можете удалять только пользовательские шаблоны отчетов.

Удалять шаблоны отчетов могут только пользователи с ролью Администратор.

Чтобы удалить шаблон отчета:

1. Выберите раздел **Отчеты**.
2. На вкладке **Шаблоны отчетов** выберите один или несколько шаблонов отчетов, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Вы не можете удалить системные шаблоны отчетов. В таблице шаблонов отчетов системные шаблоны отображаются со значком .
4. В открывшемся окне запроса подтвердите удаление шаблонов отчетов.

Удаление отчета

Удалять отчеты в программе могут только пользователи с ролью Администратор.

Чтобы удалить отчет:

1. Выберите раздел **Отчеты**.
2. На вкладке **Сформированные отчеты** выберите один или несколько отчетов, которые вы хотите удалить.

   Отчеты в таблице отчетов отфильтрованы по идентификаторам отчетов, запущенных последними в текущем сеансе подключения к Серверу. Для отображения всех сформированных отчетов сбросьте параметры фильтрации с помощью кнопки **Фильтр по умолчанию**. Если требуется, вы можете настроить фильтрацию по нужному периоду времени.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне запроса подтвердите удаление отчета.

Отмена формирования отчета

Вы можете отменить формирование отчета только со статусом **Формируется**.

Если требуется, пользователь с ролью Администратор может отменять формирование отчетов, запущенных любым пользователем программы.

Чтобы отменить формирование отчета:

1. Выберите раздел **Отчеты**.
2. На вкладке **Сформированные отчеты** выберите отчет со статусом **Формируется**, формирование которого вы хотите отменить.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Отменить**.
4. В открывшемся окне запроса подтвердите отмену формирования отчета.

После выполнения запроса статус отчета изменится на **Отменено**.

Управление параметрами хранения файлов отчетов

Вы можете изменить ограничения максимального объема для хранения файлов отчетов.

Чтобы изменить параметры хранения файлов отчетов:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку Сервера.

   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

   В области деталей появятся вкладки для изменения параметров Сервера.
5. На вкладке **Общие** перейдите к блоку параметров **Отчеты** и задайте ограничение занимаемого объема для хранения файлов отчетов с помощью параметра **Макс. объем**.

   Вы можете выбрать единицу измерения для ограничения объема: **МБ** или **ГБ**.

   При изменении значения параметра вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.
6. При необходимости с помощью параметра **Время хранения (дней)** включите ограничение на минимальное время хранения файлов отчетов и укажите нужное количество дней для хранения.
7. Нажмите на кнопку **Сохранить**.

Управление политикой безопасности

Политика безопасности – это набор данных, которые определяют следующие параметры работы программы:

- пользовательские наборы правил обнаружения вторжений;
- разрешающие правила для контроля взаимодействий и для событий;
- параметры устройств и тегов, используемые при контроле активов и контроле процесса;
- параметры отображения карты сети;
- параметры пользователей;
- параметры приложений и патчей;
- параметры адресных пространств;
- параметры типов событий;
- параметры типов рисков.

Остальные параметры работы программы не входят в политику безопасности и применяются отдельно от нее. К таким параметрам относятся параметры узлов с установленными компонентами, список пользователей программы, объекты, связывающие события и устройства в таблице устройств, и другие параметры.

Политика безопасности хранится на Сервере и автоматически обновляется при каждом изменении параметров работы программы (например, при добавлении правил контроля взаимодействий).

Вы можете экспортировать политику безопасности в файлы и импортировать из файлов. Также вы можете очистить текущую политику безопасности на Сервере, чтобы удалить все ранее сохраненные параметры.

При экспорте, импорте или очистке политики безопасности вы можете выбирать нужные разделы политики, с которыми требуется выполнить операцию. Например, вы можете экспортировать только устройства и разрешающие правила.

В результате экспорта политики безопасности программа создает файл, содержащий информацию о выбранных параметрах работы программы. Для импорта параметров вы можете выбрать ранее экспортированный файл.

Изменение содержимого файла политики безопасности может привести к нарушению работы Kaspersky Industrial CyberSecurity for Networks при импорте политики безопасности из этого файла. Программа может перестать выполнять функции по защите промышленной сети.

Экспорт политики безопасности в файл

Вы можете экспортировать в файл параметры, входящие в политику безопасности. Экспорт можно выполнить для всей политики безопасности или для ее отдельных разделов.

В дальнейшем при необходимости вы можете импортировать нужные параметры работы программы из файла с сохраненной политикой безопасности.

Чтобы экспортировать текущую политику безопасности:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс.
2. Выберите раздел **Параметры** → **Политика безопасности**.
3. Нажмите на кнопку **Экспорт**.

   Появится дерево разделов политики безопасности, в котором вы можете выбрать нужные разделы для экспорта.
4. Установите флажки для нужных разделов политики безопасности.
5. Нажмите на кнопку **Экспортировать**.
6. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции формирования файла.

   c. Нажмите на кнопку **Скачать файл**.

Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Импорт политики безопасности из файла

Вы можете импортировать параметры работы программы из файла с сохраненной политикой безопасности. Для импорта можно использовать файл, полученный при экспорте политики безопасности.

При импорте разделов политики безопасности программа предварительно очищает текущее содержимое этих разделов и затем импортирует данные в эти разделы.

Если файл содержит несколько разделов политики безопасности, вы можете выбрать нужные разделы для импорта.

> Импорт политики безопасности невозможен, если в текущий момент выполняется установка обновлений или запущен другой процесс импорта.

Импортировать политику безопасности из файла могут только пользователи с ролью Администратор.

Чтобы импортировать политику безопасности из файла:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выключите использование всех технологий и методов на узлах Сервера, сенсоров и точек мониторинга.
3. Выберите раздел **Параметры** → **Политика безопасности**.
4. Нажмите на кнопку **Импорт**.

   Откроется стандартное окно используемого браузера для выбора файла.
5. Укажите путь к файлу политики безопасности.
6. Нажмите на кнопку открытия файла.

   После проверки содержимого файла появится дерево разделов политики безопасности, доступных для импорта.
7. Установите флажки для тех разделов политики безопасности, которые вы хотите импортировать в программу.
8. Нажмите на кнопку **Импортировать**.

Начнется процесс импорта политики безопасности. До окончания импорта Сервер программы недоступен для подключений. Во время импорта на странице веб-интерфейса программы отображается специальный раздел **Обслуживание программы**. После возвращения веб-интерфейса программы в основной режим работы снова включите использование нужных технологий и методов.

Очистка текущей политики безопасности

Вы можете очистить текущие параметры, входящие в политику безопасности. Очистку можно выполнить для всей политики безопасности или для ее отдельных разделов.

После очистки политики безопасности некоторые данные будет невозможно восстановить, даже если предварительно был выполнен экспорт политики безопасности. Например, после очистки раздела, содержащего сведения об устройствах, безвозвратно удаляются все объекты, связывающие события и устройства в таблице устройств.

Очистка политики безопасности невозможна, если в текущий момент выполняется установка обновлений или запущен процесс импорта данных.

Очистить политику безопасности могут только пользователи с ролью Администратор.

Чтобы очистить политику безопасности:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выключите использование всех технологий и методов на узлах Сервера, сенсоров и точек мониторинга.

3. Выберите раздел **Параметры** → **Политика безопасности**.

4. Нажмите на кнопку **Очистка**.

   Появится дерево разделов политики безопасности, в котором вы можете выбрать нужные разделы для очистки.

5. Установите флажки напротив разделов политики безопасности, которые вы хотите очистить.

6. Нажмите на кнопку **Очистить**.

   Начнется процесс очистки политики безопасности. До окончания очистки Сервер программы недоступен для подключений. Во время очистки на странице веб-интерфейса программы отображается специальный раздел **Обслуживание программы**. После возвращения веб-интерфейса программы в основной режим работы снова включите использование нужных технологий и методов.

Преобразование политики безопасности предыдущей версии программы

Если вы хотите импортировать в текущую версию программы файл, в котором сохранена политика безопасности от предыдущей версии программы, вам нужно преобразовать этот файл с помощью скрипта для преобразования политик policy_updater.py. Этот скрипт находится на компьютере Сервера в директории /opt/kaspersky/kics4net/sbin/.

Скрипт policy_updater.py предназначен для преобразования политик безопасности, экспортированных в Kaspersky Industrial CyberSecurity for Networks, начиная с версии 3.1.

Чтобы преобразовать файл с политикой безопасности, созданный в предыдущей версии программы, выполните следующие действия:

1. Откройте консоль операционной системы на компьютере Сервера и перейдите в директорию /opt/kaspersky/kics4net/sbin/.

2. В командной строке введите команду:

   ```
   python3 ./policy_updater.py -i <путь к файлу исходной политики> -o <путь к файлу преобразованной политики>
   ```

   Пример:
   ```
   python3 ./policy_updater.py -i /home/user1/policy_2023-09-01_12-00 -o /home/user1/policy_for_4_2
   ```

Полученный файл вы можете импортировать в программу текущей версии.

Использование Kaspersky Industrial CyberSecurity for Networks API

В Kaspersky Industrial CyberSecurity for Networks реализован интерфейс прикладного программирования (Application Programming Interface, далее API), который обеспечивает доступ к функциям программы для сторонних приложений.

В комплект поставки Kaspersky Industrial CyberSecurity for Networks входит пакет с описаниями спецификаций для представления данных в запросах к серверу REST API. *Сервер REST API* функционирует на компьютере Сервера Kaspersky Industrial CyberSecurity for Networks и обрабатывает запросы с использованием архитектурного стиля взаимодействия REST (Representational State Transfer). Обращения к серверу REST API выполняются по протоколу HTTPS. Вы можете настроить параметры сервера REST API в разделе **Параметры** → **Серверы подключений** (в том числе заменить используемый по умолчанию самоподписанный сертификат на доверенный).

Для представления данных в запросах и ответах используется формат JSON.

Документация с описанием запросов на основе архитектурного стиля REST публикуется в виде онлайн-справки на странице Kaspersky Online Help. Документация представляет собой руководство разработчика на английском языке. В руководстве разработчика также представлены примеры кода и подробные описания вызываемых элементов, которые доступны в запросах к серверу REST API.

ОТКРЫТЬ ДОКУМЕНТАЦИЮ С ОПИСАНИЕМ ЗАПРОСОВ К СЕРВЕРУ REST API, версия 3

ОТКРЫТЬ ДОКУМЕНТАЦИЮ С ОПИСАНИЕМ ЗАПРОСОВ К СЕРВЕРУ REST API, версия 4

С помощью Kaspersky Industrial CyberSecurity for Networks API сторонние приложения могут выполнять следующие действия:

- получать данные об известных программе устройствах;
- добавлять, изменять и удалять устройства;
- получать данные о зарегистрированных событиях;
- отправлять события в Kaspersky Industrial CyberSecurity for Networks (для регистрации используется системный тип события с кодом 4000005400);
- получать данные о списке тегов и о параметрах тегов;
- подписываться на уведомления о полученных значениях тегов;
- получать данные об обнаруженных уязвимостях;
- получать сообщения программы и записи аудита;
- получать данные о разрешающих правилах;
- включать, выключать и удалять разрешающие правила;
- получать данные о рисках, связанных с устройствами;

- получать данные об адресных пространствах;
- отправлять отчет о топологической карте сети в Kaspersky Industrial CyberSecurity for Networks;
- отправлять, получать и удалять сведения о пользователях на устройствах;
- отправлять и получать сведения о приложениях и патчах на устройствах;
- отправлять и удалять сведения об исполняемых файлах на устройствах;
- отправлять содержимое журналов устройств;
- получать следующие данные о программе:
  - список узлов с установленными компонентами программы;
  - список точек мониторинга и их параметры;
  - список поддерживаемых стеков протоколов и их параметры;
  - список типов событий и их параметры;
  - текущее состояние и режимы работы технологий;
  - версия программы и даты выпуска установленных обновлений;
  - информация о добавленном лицензионном ключе;
  - язык локализации программы.

Все перечисленные действия доступны при выполнении запросов к серверу REST API версии 4. При выполнении запросов к серверу REST API версии 3 некоторые действия не поддерживаются.

Сторонние приложения, использующие Kaspersky Industrial CyberSecurity for Networks API, подключаются к Серверу программы через коннекторы. Коннекторы обеспечивают безопасное соединение с использованием сертификатов. Для каждого стороннего приложения, из которого вы хотите отправлять запросы на сервер REST API, вам нужно создать отдельный коннектор в Kaspersky Industrial CyberSecurity for Networks.

Для соединения с Kaspersky Industrial CyberSecurity for Networks стороннее приложение должно использовать токен аутентификации. Программа выдает токен аутентификации по запросу стороннего приложения и использует для токена сертификаты коннектора, который был создан для этого стороннего приложения. Время действия токена аутентификации составляет 10 часов. Стороннее приложение может обновить токен аутентификации по специальному запросу.

Документация с описанием запросов для выполнения действий с токеном аутентификации публикуется в виде онлайн-справки на странице Kaspersky Online Help. Документация представляет собой руководство разработчика на английском языке.

ОТКРЫТЬ ДОКУМЕНТАЦИЮ С ОПИСАНИЕМ ЗАПРОСОВ ДЛЯ ДЕЙСТВИЙ С ТОКЕНОМ АУТЕНТИФИКАЦИИ, версия 3

[ОТКРЫТЬ ДОКУМЕНТАЦИЮ С ОПИСАНИЕМ ЗАПРОСОВ ДЛЯ ДЕЙСТВИЙ С ТОКЕНОМ АУТЕНТИФИКАЦИИ, версия 4]

В Kaspersky Industrial CyberSecurity for Networks API предусмотрены следующие способы работы со сторонними приложениями:

- взаимодействие на основе архитектурного стиля REST;
- взаимодействие по протоколу WebSocket.

Сторонние приложения могут использовать способ взаимодействия по протоколу WebSocket в Kaspersky Industrial CyberSecurity for Networks API для создания подписок на изменяемые значения, которые получает программа. Например, этот способ взаимодействия позволяет подписываться на уведомления о полученных значениях определенного тега.

Обеспечение безопасного взаимодействия при использовании Kaspersky Industrial CyberSecurity for Networks API

Сторонние приложения получают доступ к функциям программы с использованием Kaspersky Industrial CyberSecurity for Networks API, устанавливая зашифрованные соединения по протоколу HTTPS. Для обеспечения безопасности соединений используются сертификаты, выданные Сервером Kaspersky Industrial CyberSecurity for Networks. Сервер выдает сертификаты для коннекторов, через которые подключаются сторонние приложения.

Для каждого стороннего приложения в программе должен быть создан отдельный коннектор. Подключение через коннектор возможно с использованием только того сертификата, который был выдан Сервером и сохранен в файле свертки для этого коннектора. Подключение невозможно установить, если стороннее приложение предъявляет сертификат от другого коннектора, другого Сервера Kaspersky Industrial CyberSecurity for Networks, или сертификат, используемый для других подключений (например, сертификат сенсора).

После установки зашифрованного соединения стороннее приложение должно запросить *токен аутентификации* для коннектора, который будет указываться сторонним приложением в запросах к серверу REST API. Для выдачи токена аутентификации Сервер проверяет текущее состояние учетной записи пользователя программы, которая была указана при создании коннектора. Сервер не выдает токен аутентификации, если учетная запись пользователя программы удалена или заблокирована.

Токен аутентификации действителен в течение 10 часов после выдачи Сервером. При необходимости дальнейшего использования токена стороннее приложение должно запросить продление времени его действия до наступления момента прекращения действия.

Сведения о предусмотренных запросах и методах в Kaspersky Industrial CyberSecurity for Networks API см. в документации для Kaspersky Industrial CyberSecurity for Networks API.

В течение времени действия токена аутентификации при поступлении запросов от стороннего приложения Сервер проверяет наличие и текущие права доступа учетной записи пользователя программы, которая была указана при создании коннектора. Метод, указанный в запросе от стороннего приложения, не выполняется, если учетная запись не найдена (удалена из программы) или недостаточно прав для выполнения операции (роль учетной записи не соответствует выполняемой операции).

При обработке запросов от сторонних приложений программа сохраняет в журнале аудита сведения о попытках выполнения следующих операций:

- получение токена аутентификации;
- продление времени действия для токена аутентификации;
- добавление устройства в таблицу устройств;
- изменение сведений об устройстве;
- удаление устройства;
- запрос журнала аудита (при первом чтении записей аудита через коннектор после загрузки веб-сервера).

Создание и использование коннекторов для Kaspersky Industrial CyberSecurity for Networks API

Для взаимодействия стороннего приложения с программой с использованием Kaspersky Industrial CyberSecurity for Networks API вам нужно добавить коннектор для этого приложения. При создании коннектора для него требуется указать системный тип **Generic**.

При добавлении коннектора, а также при создании нового файла свертки для этого коннектора Сервер формирует файл свертки, который вам нужно использовать для работы коннектора.

Файл свертки представляет собой архив, содержащий следующие файлы:

- certificates.pfx – содержит в зашифрованном виде открытый ключ сертификата Сервера, а также сертификат, выданный Сервером для коннектора (с закрытым ключом). Содержимое файла зашифровано с использованием пароля, который был указан при добавлении коннектора или при создании нового файла свертки для этого коннектора.
- metadata.json – содержит конфигурационные данные для коннектора. Данные представлены в формате JSON.

Перечисленные файлы вам нужно использовать для подключения стороннего приложения через коннектор. Для расшифрования файла certificates.pfx и применения содержащегося в нем сертификата с ключами вы можете использовать стандартные методы обработки файлов этого формата (например, команды `openssl`). Адреса, указанные в файле metadata.json, требуются для работы коннектора и отправки запросов к серверу REST API.

Сертификат и конфигурационные данные в файле свертки действительны до тех пор, пока не создан новый файл свертки или пока не удален коннектор в программе.

Подписка на уведомления о значениях тега по протоколу WebSocket

При использовании Kaspersky Industrial CyberSecurity for Networks API стороннее приложение может создавать подписку на уведомления об изменении значений определенного тега. Для создания подписки и получения уведомлений используется протокол WebSocket.

Сценарий подписки для стороннего приложения состоит из следующих этапов:

1. **Стороннее приложение устанавливает соединение с Сервером Kaspersky Industrial CyberSecurity for Networks через коннектор для этого приложения с использованием сервера REST API.**

   После успешного соединения с Сервером коннектору отправляется токен аутентификации. Коннектор использует токен аутентификации для всех последующих взаимодействий с Сервером в этом сеансе (в частности для запроса своей конфигурации с Сервера).

2. **Стороннее приложение подключается с использованием WebSocket и отправляет запрос для создания подписки на уведомления о получении значений нужного тега.**

   Сервер Kaspersky Industrial CyberSecurity for Networks принимает запрос и создает подписку. Для отправки запроса используются соответствующие функции, предусмотренные протоколом WebSocket.

3. **Kaspersky Industrial CyberSecurity for Networks обнаруживает в трафике новое значение при чтении или записи тега.**

4. **Kaspersky Industrial CyberSecurity for Networks отправляет полученное значение тега стороннему приложению, для которого действует подписка на уведомления о получении значений этого тега.**

Основные особенности реализации подписки:

- После того, как стороннее приложение указывает нужные теги Kaspersky Industrial CyberSecurity for Networks, Сервер отправляет подтверждение о возможности получать значения этих тегов. Далее стороннее приложение ожидает поступление значений этих тегов по установленному соединению.
- Для создания и сопровождения подписки используется протокол WebSocket и соединение по тому же адресу, который используется сервером REST API.
- Сервер Kaspersky Industrial CyberSecurity for Networks поддерживает не более одной активной подписки на значения тегов. Если активная подписка уже создана и используется, при попытке создания еще одной подписки возвращается ошибка о слишком большом количестве подключений.
- Стороннее приложение имеет возможность в любой момент закрыть установленное соединение по подписке для прекращения получения значений тега.
- Подписка прекращается либо после ее закрытия сторонним приложением, либо при разрыве соединения. Если Сервер Kaspersky Industrial CyberSecurity for Networks был временно недоступен (разорвано соединение) и отправка значений по подписке не выполнялась, то после восстановления соединения стороннему приложению потребуется заново подписаться на получение значений тегов.

Подключение с использованием WebSocket

Для получения тегов по подписке могут использоваться как стандартные функции WebSocket, так и библиотека SignalR Core. Пакеты для работы с библиотекой SignalR Core доступны для наиболее распространенных языков программирования: C++, C#, Java, Python, Go, JavaScript/TypeScript.

Для подключения с использованием WebSocket вам нужно указывать следующий адрес:
`<адрес publicApi из файла свертки>/kics4net/api/v4/tag-values`

При этом указываемый протокол в строке адреса зависит от используемой функциональности для подключения.

Если используется библиотека SignalR Core, строка адреса начинается с `https://`. Например:
`https://kics-server:8080/kics4net/api/v4/tag-values`

Если используются стандартные функции WebSocket, в строке адреса нужно заменить `https` на `wss`. Например:
`wss://kics-server:8080/kics4net/api/v4/tag-values`

Если при подключении не предоставлен токен аутентификации (или предоставленный токен не прошел проверку), в ответ на открытие подключения сервер возвращает код 401.

Создание подписки на значения тегов

Для создания подписки требуется выполнить запрос с именем метода `GetTagValuesStream`.

Пример аргумента запроса:

```
{
    "tagIdentifiers": [
        { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
        { "tagName": "Asdu_1_object_1003", "assetName": "Asset 079" }
    ],
    "streamConfig": {
        "samplingRateHz": 1
    }
}
```

Аргумент запроса состоит из следующих полей:

- `tagIdentifiers` – массив идентификаторов тегов, значения которых нужно получать по подписке.
- `assetName`, `tagName` – значения, представляющие имя устройства и имя тега (используются для идентификации тега, на значения которого нужно создать подписку).
- `samplingRateHz` – частота сэмплирования значений тегов (используется для уменьшения объема передаваемых данных). Если для поля задано нулевое значение, сэмплирование не выполняется.

Если аргумент создания подписки не удовлетворяет требованиям к полям, возвращается ошибка с описанием проблемы.

Пример ошибки для аргумента создания подписки:

```
HubException: GetTagValuesStreamRequest has validation errors:
   TagIdentifiers:
      The TagName field is required.
   The StreamConfig field is required.
```

Подтверждение подписки

При подтверждении подписки сервер возвращает по одному результату подтверждения для каждого тега, подходящего под значения `tagIdentifiers` в запросе.

Пример подтверждения подписки:

```
{
    "confirmation": {
        "result": "ok",
        "tagIdentifier": { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
        "tagId": 102
    }
}
```

Ответ с подтверждением подписки состоит из следующих полей:

- `result` – статус подписки на значение тега. Может принимать значения:
  - `ok` – подписка успешно создана;
  - `notFound` – тег с указанными `assetName`, `tagName` не найден.
- `tagIdentifier` – идентификатор тега, аналогичный одному значению из массива `tagIdentifiers` аргументов запроса на создание подписки.
- `tagId` – уникальный идентификатор тега в программе. Может быть использован для получения информации о теге через Kaspersky Industrial CyberSecurity for Networks API, а также для идентификации тега в ответе с его значениями.

Значения тегов по подписке

Программа отправляет значения тегов по подписке в структуре полей. На верхнем уровне в структуре представлены следующие поля:

```
{
    "value": {
        "tagId": <уникальный идентификатор тега в программе>,
        "tagValue": "<JSON-объект с данными тега>"
    }
}
```

Информация о новом значении тега отправляется в стороннее приложение в формате JSON. Отправляемый объект с данными содержит следующие поля:

- `n` – тип данных тега, представленный именем из `TagStructure`.
- `ts` – время регистрации последнего обновления значений тега. Указывается в микросекундах от 01.01.1970.
- `dn` – направление передачи. Может принимать значения: `r`, `w`, `rw`.
- `mp` – идентификатор точки мониторинга.
- `d` – содержимое полей тега.

Атрибут `d` представляет словарь, в котором каждый ключ является именем поля тега нулевой иерархии. Значение каждого поля имеет следующие атрибуты:

- `t` – обязательный атрибут, указывающий один из следующих типов данных:
  - `u` – UINT64.
  - `i` – INT64.
  - `b` – BOOL.
  - `d` – DOUBLE.
  - `s` – строка UTF8.
  - `t` – время в микросекундах от 01.01.1970.
  - `e` – ENUM. Дополнительно поле содержит следующие атрибуты:
    - `n` – имя типа ENUM;
    - v – исходное значение ENUM;
    - s – строковое значение ENUM.
  - `st` – структура.
  - `un` – UNION.
- `v` – обязательный атрибут, указывающий значение поля тега.
- `n` – имя типа ENUM из `TagStructure` (только для типа `e` – ENUM).
- `s` – строковое значение ENUM (только для типа `e` – ENUM).

  Пример:

```
- enum:
    name: OpType # Имя типа ENUM (атрибут 'n')
    data:
        0: NUL # 0 запишется в атрибут 'v', NUL запишется в 's'
        1: PULSE_ON
        2: PULSE_OFF
```

- `x` – идентифицирует основное значение тега.

  Формат: `"x": 1`

  Для всех остальных полей тега атрибут `x` отсутствует.

- m – специальный маркер параметра тега. Соответствует атрибуту marker со следующими полями:

  - `q` – значение атрибута качества.
  - `ts` – статус метки времени, отображающий её правильность, временное состояние или причину ошибки при проверке.
  - `ds` – статус данных.
  - `o` – источник, от которого пришло значение или команда.
  - `t` – время последнего обновления значений тега, взятое из трафика.
  - `ct` – причина передачи.

  Формат: `"m": "q"`

Пример отправляемого значения тега в формате JSON:


```
{
    "n": "TagStructure1",
    "ts": 18446744073709551616,
    "dn": "r",
    "mp": 1,
    "d":
    {
        "value":
        {
            "t": "d",
            "v": 3.1415,
            "x": 1
        },
        "quality":
        {
            "t": "s",
            "v": "good",
            "m": "q"
        },
        "mask":
        {
            "t": "u",
            "v": 18446744073709551616
        },
        "enumfield":
        {
            "t": "e",
            "n": "SwitchState",
            "v": 0,
            "s": "Off"
        },
        "strucfield":
        {
            "t": "st",
            "v":
            {
                "v1":
                {
                    "t": "d",
                    "v": 3.1415
                },
                "q2":
                {
                    "t": "s",
                    "v": "good",
                    "m": "q"
                }
            }
        },
        "unionfield":
        {
            "t": "un",
            "v":
            {
                "_":
                {
                    "t": "u",
                    "v": 42
                },
                "low4bits":
                {
                    "t": "u",
                    "v": 10
                },
                "high4bits":
                {
                    "t": "u",
                    "v": 2
                }
            }
        }
    }
}
```


Примеры получения значений тегов по подписке

Ниже представлен пример получения значений тегов по подписке с использованием стандартных функций WebSocket на языке Python.

Предварительно требуется выполнить команду:
`pip install websocket_client`

Пример подписки с использованием стандартных функций WebSocket:

```
import json, ssl, websocket


def on_message(ws, message):
    print(message)


def on_error(ws, error):
    print(f' error: {error}')


def on_close(ws):
    print("### closed ###")


def on_open(ws):
    print("connection opened and handshake received ready to send messages")

    # all sent messages must end with this character
    message_separator = chr(30)

    # setting up json as messages format
    protocol_selection_args = {
        'protocol': 'json',
        'version': 1
    }
    ws.send(json.dumps(protocol_selection_args) + message_separator)

    # creating subscription
    args = {
        'arguments': [
            {
                'tagIdentifiers': [
                    {
                        'tagName': 'tag_01',
                        'assetName': 'asset_02'
                    }
                ],
                'streamConfig': {
                    'samplingRateHz': 5
                }
            }
        ],
        'invocationId': '0',             # will be included in response message
        'target': 'getTagValuesStream',
        'type': 4                        # must be equal to 4 for outgoing messages
    }

    ws.send(json.dumps(args) + message_separator)


 def login():
    token = "you should get access token for API here"
    return token


if __name__ == "__main__":
    server_url = "wss://localhost:8091/kics4net/api/tag-values"
    auth = "Authorization: Bearer " + login()

    # for troubleshooting uncomment next line
    # websocket.enableTrace(True)
    ws = websocket.WebSocketApp(server_url,
                                on_message=on_message,
                                on_error=on_error,
                                on_close=on_close,
                                header=[auth])

    print(f'opening connection to {server_url}')
    ws.on_open = on_open
    ws.run_forever(
        # use it only if Server has self-signed certificate
        sslopt={"cert_reqs": ssl.CERT_NONE}
    )
```

Ниже представлен пример получения значений тегов по подписке с использованием библиотеки SignalR Core на языке Python.

Предварительно требуется выполнить команду:
`pip install signalrcore`

Пример подписки с использованием библиотеки SignalR Core:

```
import logging
from signalrcore.hub_connection_builder import HubConnectionBuilder

TOKEN = 'you should get access token for API here’
IP = '192.168.0.7'
PORT = '8080'
HUB = 'kics4net/api/v4/tag-values'

class WebsocketConnection(HubConnectionBuilder):
    def __init__(self, url: str = None, options: dict = None, verify_ssl: bool = False):
        super().__init__()
        self.with_url(url, options=options)
        self.configure_logging(logging.WARNING)
        self.with_automatic_reconnect({
            "type": "raw",
            "keep_alive_interval": 10,
            "reconnect_interval": 5,
            "max_attempts": 5
        })
        self.verify_ssl = verify_ssl

    def on_tag_stream_value(self, m):
        result.append(m)
        print(f'on_new_tag_value, {m}')

    def on_tag_strean_error(self, e):
        print(f'onError, {e}')

    def on_tag_stream_complete(self, q):
        print(f'onComplete, {q}')

    def subscribe_tags(self):
        print("connection opened and handshake received ready to send messages")

        args = {
            'tagIdentifiers': [
                {
                    'tagName': 'tag_01',
                    'assetName': 'asset_02'}
            ],
            'streamConfig': {
                'samplingRateHz': 5
            }
        }

        self.stream("GetTagValuesStream", [args]) \
            .subscribe({
            "next": self.on_tag_stream_value,
            "complete": self.on_tag_stream_complete,
            "error": self.on_tag_strean_error
        })

def main():
    server_url = "https://{}:{}/{}".format(IP, PORT, HUB)
    login = 'bearer {}'.format(TOKEN)

    conn = WebsocketConnection(url=server_url, options={"headers": {"authorization": login}})
    conn.build()

    logging.info(f'opening connection to {server_url}')
    conn.on_open(conn.subscribe_tags)
    conn.start()

    logging.info('closing connection')
    conn.stop()


if __name__ == '__main__':
    main()
```

Решение типовых задач

Этот раздел содержит описание типовых пользовательских задач и инструкции по их выполнению.

Мониторинг системы в онлайн-режиме

Kaspersky Industrial CyberSecurity for Networks отображает данные для мониторинга текущего состояния системы в разделе **Мониторинг** веб-интерфейса программы. Обновление данных происходит автоматически в онлайн-режиме.

Данные в разделе **Мониторинг** представлены в виде отдельных блоков, называемых *виджетами*. В зависимости от назначения, виджет может содержать обновляемое значение, сообщение о текущем состоянии программы или предоставлять развернутую информацию об актуальных данных.

В разделе **Мониторинг** могут отображаться следующие виджеты:

- Виджеты с информацией для контроля текущего состояния системы и наиболее значимых изменений:

  - **Устройства с состояниями безопасности** – распределение устройств по их состояниям безопасности.

  - **Оценки событий** – гистограмма распределения событий по значениям их оценок за выбранный период. Столбцы гистограммы соответствуют целочисленным значениям оценок. Вы можете изменить режим отображения данных на круговую диаграмму с распределением событий по уровням критичности. В зависимости от числового значения оценки события могут относиться к уровням критичности *Низкий* (оценки 0.0–3.9), *Средний* (оценки 4.0–7.9) или *Высокий* (оценки 8.0–10.0).

  - **События по технологиям** – количественное распределение событий по технологиям регистрации событий за выбранный период.

  - **Частые пользователи приложений в событиях** – наиболее часто регистрируемые имена пользователей в событиях по данным от EPP-приложений за выбранный период.

  - **Частые приложения в событиях** – наиболее часто регистрируемые сторонние приложения в событиях по данным от EPP-приложений за выбранный период.

  - **Частые устройства в событиях** – наиболее часто регистрируемые устройства в событиях за выбранный период.

  - **Частые устройства по количеству рисков** – наиболее часто регистрируемые устройства в обнаруженных рисках за выбранный период.

  - **Оценки рисков** – гистограмма распределения рисков по значениям их оценок за выбранный период. Столбцы гистограммы соответствуют целочисленным значениям оценок. Вы можете изменить режим отображения данных на круговую диаграмму с распределением рисков по уровням критичности. В зависимости от числового значения оценки риска могут относиться к уровням критичности *Низкий* (оценки 0.0–3.9), *Средний* (оценки 4.0–7.9) или *Высокий* (оценки 8.0–10.0).

  - **Ситуационная осведомленность** – уведомления о текущих выявленных угрозах для безопасности системы (например, **Обнаружено 10 неразрешенных сетевых взаимодействий**). Виджет отображает уведомления в порядке их уровня важности.

  - **Защищенность EPP-приложениями** – количественное соотношение компьютеров, защищенных и не защищенных EPP-приложениями. В центре круговой диаграммы отображается суммарное количество защищенных и не защищенных компьютеров.

    Компьютер считается защищенным EPP-приложением, если в Kaspersky Industrial CyberSecurity for Networks имеются сведения о выполнении следующих условий:

    - на компьютере установлено EPP-приложение;
    - для EPP-приложения выполняется задача Постоянная защита (Real-Time Protection);
    - EPP-приложение имеет статус подключения к серверу интеграции *Активное*.

    Компьютер считается не защищенным EPP-приложением если не выполнено хотя бы одно из перечисленных условий. Проверка на незащищенность EPP-приложением выполняется для всех устройств в Kaspersky Industrial CyberSecurity for Networks, содержащих название операционной системы Windows (любой версии) в качестве установленной операционной системы, или если устройства относятся к одной из следующих категорий:

- **Сервер**;
- **Рабочая станция**.

- **Устройства** – содержит информацию об устройствах в промышленной сети (используется распределение по категориям устройств).
- **События** – содержит информацию о событиях и инцидентах, имеющих наиболее поздние значения даты и времени последнего появления.

- Виджеты с информацией о программе и аппаратных ресурсах Сервера и сенсоров:
  - **Трафик** – скорость поступления входящего трафика. Виджет может отображать данные по всем точкам мониторинга всех узлов с установленными компонентами программы, по точкам мониторинга выбранного узла или только по одной точке мониторинга.
  - **Процессор** – загруженность процессора на выбранном узле с установленным компонентом программы.
  - **Оперативная память** – объем потребления физической оперативной памяти на выбранном узле с установленным компонентом программы.
  - **Работоспособность** – информация о текущем состоянии работоспособности программы. Виджет может отображать следующие значения:
    - **OK** – нет сообщений о нарушении работоспособности или все проблемы работоспособности устранены.
    - **Некритический сбой** – есть сообщения о некритических сбоях (отображается до момента устранения проблемы работоспособности).
    - **Нарушена работа** – есть сообщения о нарушении работы программы (отображается до момента устранения проблемы работоспособности).
    - **Режим обслуживания** – программа находится в режиме обслуживания.
  - **Теги** – скорость обработки тегов, обнаруженных программой. Виджет может отображать данные по всем точкам мониторинга всех узлов с установленными компонентами программы, по точкам мониторинга выбранного узла или только по одной точке мониторинга.
  - **Хранилище** – данные о диске, который находится в локальной файловой системе на выбранном узле с установленным компонентом программы. В этом виджете вы можете выбрать следующие данные для отображения:
    - **Использование диска** – процентное значение времени на обработку операций чтения и записи данных.
    - **Занято на диске** – объем занятого дискового пространства.
    - **Чтение с диска** – скорость чтения данных с диска.
    - **Запись на диск** – скорость записи данных на диск.
  - **Задержка обработки трафика** – текущее время задержки при обработке трафика с момента его поступления на точку мониторинга узла (выводится максимальное время задержки, полученное со

всех включенных точек мониторинга). Виджет может отображать данные по всем точкам мониторинга всех узлов с установленными компонентами программы или по точкам мониторинга выбранного узла.

- **Статус функций** – общая информация о текущем состоянии функций защиты в составе программы. Виджет может отображать следующие значения:
  - **Включены все** – работают все технологии и методы, предназначенные для постоянного использования, а также включены все созданные точки мониторинга.
  - **Не все включены** – некоторые функции защиты выключены или включены в режиме обучения, либо включены не все точки мониторинга.
- **Время работы** – время работы Kaspersky Industrial CyberSecurity for Networks. В этом виджете вы можете выбрать следующие данные для отображения:
  - **Эффективное время работы** – время нормальной работы программы (без сбоев) с последнего запуска до текущего момента.
  - **Общее время работы** – время работы с первого запуска программы до текущего момента (включает периоды нормальной работы программы и периоды работы со сбоями).
  - **С первого запуска программы** – общее время, прошедшее с первого запуска программы до текущего момента (включает периоды нормальной работы программы, периоды работы со сбоями и периоды неработоспособного состояния).

- Виджеты без динамически изменяемой информации. Вы можете создавать виджеты с произвольно заданным содержанием. Такие виджеты называются *пользовательскими*. С помощью пользовательских виджетов вы можете, например, логически разделять группы виджетов в разделе **Мониторинг**.

Для виджетов предусмотрены различные средства привлечения внимания в зависимости от поступающих данных. Например, виджеты с информацией о программе и аппаратных ресурсах могут автоматически изменять цвет, если информация требует внимания (в частности, при нагрузке на аппаратный ресурс близкой к критической).

В виджетах отображается только основная информация, которая изменяется динамически. Если вам нужно просмотреть более подробную информацию (например, об устройствах, требующих внимания), вы можете перейти из раздела **Мониторинг** к другим разделам веб-интерфейса программы. Переходы можно выполнять путем выбора элементов интерфейса виджетов с помощью мыши.

Добавление виджета

Чтобы добавить виджет:

1. В разделе **Мониторинг** нажмите на кнопку **Виджеты**.

   Откроется окно **Добавление виджетов**.

2. Добавьте нужный виджет по ссылке **Добавить** справа от названия виджета.

   Новый виджет займет свободное место в области отображения виджетов.

3. Нажмите на кнопку **Закрыть** в окне **Добавление виджетов**.

После добавления вы можете настроить отображение виджета.

Настройка отображения виджетов

Этот раздел содержит инструкции по настройке отображения виджетов.

Перемещение виджета

Чтобы переместить виджет:

1. В разделе **Мониторинг** наведите курсор на верхнюю часть нужного виджета (например, на название виджета).

   Курсор примет вид .

2. Перетащите виджет в нужную часть области отображения виджетов.

Изменение размера виджета

Чтобы изменить размер виджета:

1. В разделе **Мониторинг** наведите курсор на нижний правый угол нужного виджета.

2. Удерживая нажатой левую кнопку мыши, задайте размер для рамки виджета.

Изменение параметров отображения данных в виджете

После добавления виджета для отображения данных используются параметры, заданные по умолчанию. При необходимости вы можете изменить параметры отображения (например, чтобы указать нужный источник или выбрать другие данные для отображения в виджете **Хранилище**).

Чтобы настроить параметры отображения виджета:

1. В разделе **Мониторинг** откройте меню управления виджетом с помощью кнопки в правом верхнем углу виджета.

2. В меню управления виджетом выберите пункт **Настроить**.

   Откроется окно для настройки параметров отображения.

3. Настройте параметры виджета.

   В зависимости от выбранного виджета окно может содержать следующие параметры:

   - **Изменить название** – если установлен флажок **Изменить название**, вы можете задать произвольное название виджета (отличающееся от заданного по умолчанию) в поле **Название виджета**. Параметр **Изменить название** отсутствует для пользовательских виджетов.
   - **Название виджета** – поле для ввода названия виджета, отличающегося от названия по умолчанию.
   - **Изменить описание** – если установлен флажок **Изменить описание**, вы можете задать произвольное описание виджета (отличающееся от заданного по умолчанию) в поле **Описание виджета**. Параметр **Изменить описание** отсутствует для пользовательских виджетов.
   - **Описание виджета** – поле для ввода названия виджета, отличающегося от названия по умолчанию.
   - **Период обновления** – задает период времени в секундах, после которого обновляются отображаемые данные.
   - **Отображать** – задает тип отображаемых данных (для виджетов с возможностью выбора данных для отображения).
   - **Источник данных** – задает узел с установленными компонентами программы, данные от которого отображаются в виджете. Если выбран вариант **Вся программа**, виджет отображает данные со всех узлов.
   - **Точка мониторинга** – задает точку мониторинга выбранного узла для отображения данных. Если выбран вариант **Все точки мониторинга**, виджет отображает данные по всем точкам мониторинга выбранного узла.
   - **Изменять цвет по статусу** – если флажок установлен, цвет фона виджета автоматически изменяется в зависимости от уровня важности поступивших данных. Критическому (максимальному) уровню важности данных соответствует красный цвет фона. Если флажок снят, закрашивание фона выключено.
   - **Заданный фон** – определяет цвет фона пользовательского виджета. Вы можете выбрать вариант закрашивания цветом, который соответствует одному из уровней важности (**Информационный**, **Важный**, **Критический**), или выключить закрашивание фона с помощью варианта **Бесцветный**.
   - **Режим отображения** – определяет режим отображения данных на виджете. Вы можете настроить отображение данных в виде гистограммы или круговой диаграммы.
   - **Учитывать события со статусом Обработано** – если установлен флажок **Учитывать события со статусом Обработано**, виджет отображает данные по всем событиям.
   - **Учитывать устраненные и принятые риски** – если установлен флажок **Учитывать устраненные и принятые риски**, виджет отображает данные по всем рискам.

4. Нажмите на кнопку **OK**.

Информация в виджете Устройства

Виджет **Устройства** в разделе **Мониторинг** отображает информацию об устройствах, входящих в список известных программе устройств.

В виджете представлена следующая информация:

- Данные о количественном распределении известных программе устройств по категориям. Эти данные отображаются в верхней части виджета в виде значков категорий. Под значком каждой категории указано количество устройств этой категории. Если в списке известных программе устройств есть устройства, требующие внимания, на значках категорий этих устройств отображается значок предупреждения.

- Список категорий с устройствами, требующими внимания. Эти данные отображаются в средней части виджета при наличии таких устройств. Пространство для отображения графических элементов ограничено размером виджета.

Устройства, требующие внимания

Программа считает, что устройство требует внимания, в любом из следующих случаев:

- устройство имеет статус *Разрешенное* и состояние безопасности устройства отличается от *OK*;

- устройство имеет статус *Неразрешенное*.

При наличии устройств, требующих внимания, для каждой категории в списке отображается следующая информация:

- Строка, содержащая значок категории, текстовый комментарий и ссылку с количеством устройств, требующих внимания.

- Строка с графическими элементами, представляющими устройства. Строка отображается, если достаточно свободного пространства в виджете. Количество графических элементов в строке зависит от текущего размера окна браузера. Если устройств, требующих внимания, больше чем отображаемых графических элементов в строке, то справа отображается количество скрытых устройств в формате `+ <количество устройств>`.

Графические элементы устройств

Графические элементы, представляющие устройства, содержат следующую информацию:

- Имя устройства.

- Статус устройства. Отображается в виде значка, если устройство имеет статус *Неразрешенное*.

- Состояние безопасности устройства. Отображается в виде цветной линии на левой границе графического элемента. Цвет линии соответствует состояниям *OK*, *Важное* или *Критическое*.

Графические элементы отображаются в следующем порядке:

1. Устройства с присвоенным статусом *Неразрешенное*.

2. Устройства, имеющие состояние безопасности *Критическое*.

3. Устройства, имеющие состояние безопасности *Важное*.

Переходы к другим разделам из виджета

С помощью элементов интерфейса виджета **Устройства** вы можете переходить к таблице устройств для отображения подробных сведений об устройствах. Для этого предусмотрены возможности, описанные ниже.

Переход к таблице устройств и фильтрация таблицы

Чтобы перейти к таблице устройств и просмотреть сведения о всех устройствах выбранной категории,

в верхней части виджета **Устройства** нажмите на значок нужной категории.

Откроется раздел **Активы** с таблицей устройств. В таблице будет применена фильтрация по выбранной категории устройств.

Чтобы перейти к таблице устройств и просмотреть сведения об устройствах, требующих внимания и относящихся к определенной категории,

в списке категорий с устройствами, требующими внимания, воспользуйтесь ссылкой с количеством устройств нужной категории (ссылка отображается в конце строки со значком категории и текстовым комментарием **требующие внимания**).

Откроется раздел **Активы** с таблицей устройств. В таблице будет применена фильтрация по идентификаторам устройств, требующих внимания и относящихся к определенной категории.

Фильтрация в таблице устройств выполняется по идентификаторам тех устройств, которые отображались в виджете **Устройства** на момент перехода к таблице устройств. После перехода к таблице устройств параметры фильтрации не обновляются. Если вы хотите просмотреть текущее количество устройств, требующих внимания, вы можете снова перейти в раздел **Мониторинг**.

Чтобы перейти к таблице устройств и просмотреть сведения об устройстве, требующем внимания,

в виджете **Устройства** нажмите на графический элемент, представляющий нужное устройство.

Откроется раздел **Активы** с таблицей устройств. В таблице будет применена фильтрация по идентификатору устройства.

Чтобы перейти к таблице устройств без изменений текущих параметров фильтрации таблицы,

выполните переход по ссылке **Показать все устройства** в виджете **Устройства**.

Откроется раздел **Активы** с таблицей устройств. В таблице отобразятся устройства, удовлетворяющие параметрам фильтрации, которые были заданы ранее в таблице устройств.

Переход к таблице устройств и поиск в таблице

Чтобы перейти к таблице устройств и найти устройства в таблице:

1. В виджете **Устройства** введите поисковый запрос в поле **Поиск устройств**.
2. Нажмите на кнопку **Поиск**.

Откроется раздел **Активы** с таблицей устройств. В таблице отобразятся устройства, которые удовлетворяют условиям поиска.

Информация в виджете События

Виджет **События** в разделе **Мониторинг** отображает общую информацию о событиях и инцидентах, имеющих наиболее поздние значения даты и времени последнего появления.

В виджете отображаются следующие элементы:

- Гистограмма событий и инцидентов за выбранный период. Эти данные отображаются в верхней части виджета. Гистограмма отображает распределение событий и инцидентов по уровням критичности.
- Список с информацией о зарегистрированных событиях и инцидентах, отсортированный по дате и времени последнего появления. Эти данные отображаются в средней части виджета.

Статистика событий и инцидентов

На гистограмме распределения событий и инцидентов столбцы соответствуют суммарному количеству событий за каждый интервал времени. Внутри столбцов цветом обозначены уровни критичности событий и инцидентов. Уровням критичности соответствуют следующие цвета:

- Синий цвет. Этот цвет используется для событий и инцидентов с уровнем критичности *Низкий*.
- Желтый цвет. Этот цвет используется для событий и инцидентов с уровнем критичности *Средний*.
- Красный цвет. Этот цвет используется для событий и инцидентов с уровнем критичности *Высокий*.

Для вывода информации о столбце гистограммы наведите на него курсор мыши. Во всплывающем окне отобразятся сведения о дате и времени интервала, а также о количестве событий и инцидентов по уровням критичности.

Длительность интервалов времени зависит от выбранного периода для отображения. Вы можете выбрать нужный период для построения гистограммы с помощью следующих кнопок:

- **1ч** – период в один час, делится на интервалы по одной минуте.
- **12ч** – период в 12 часов, делится на интервалы по одному часу.
- **24ч** – период в 24 часа, делится на интервалы по одному часу.
- **7д** – период в семь дней, делится на интервалы по одному дню.

Список событий и инцидентов

Список событий и инцидентов в виджете **События** обновляется в онлайн-режиме. События и инциденты с наиболее поздними значениями даты и времени последнего появления помещаются в начало списка.

Количество отображаемых элементов списка событий и инцидентов ограничено размером виджета.

Для каждого события или инцидента в списке представлены следующие сведения:

- заголовок события или инцидента;
- дата и время последнего появления;
- значок, обозначающий уровень критичности события или инцидента:
  - – уровень критичности *Низкий*;
  - – уровень критичности *Средний*;
  - – уровень критичности *Высокий*.

Инциденты в списке обозначаются значком .

Переходы к другим разделам из виджета

С помощью элементов интерфейса виджета **События** вы можете переходить к таблице событий для отображения подробных сведений о событиях и инцидентах. Для этого предусмотрены возможности, описанные ниже.

Переход к таблице событий и фильтрация таблицы

Вы можете просмотреть подробные сведения о событии или инциденте, нажав на нужное событие или инцидент в списке виджета **События**. После этого откроется раздел **События**, в котором будет применена фильтрация таблицы по идентификатору выбранного события или инцидента. Также для фильтрации будет задан период от даты и времени регистрации события или инцидента до текущего момента (без указания конечной границы периода).

Если вы хотите перейти к таблице событий без изменения текущих параметров фильтрации таблицы в разделе **События**, выполните переход по ссылке **Показать все события** в виджете **События**.

Переход к таблице событий и поиск в таблице

Чтобы перейти к таблице устройств и найти устройства в таблице:

1. В виджете **События** введите поисковый запрос в поле **Поиск событий**.
2. Нажмите на кнопку **Поиск**.

   Откроется раздел **События**. В таблице событий отобразятся события и инциденты, которые удовлетворяют условиям поиска.

Удаление виджета

Чтобы удалить виджет:

1. В разделе **Мониторинг** вызовите меню управления виджетом с помощью кнопки ⚙ в правом верхнем углу виджета.
2. В меню управления виджетом выберите пункт **Удалить**.

   Откроется окно с запросом подтверждения.
3. В окне запроса подтвердите удаление выбранного виджета.

Контроль активов

Kaspersky Industrial CyberSecurity for Networks позволяет контролировать устройства промышленной сети, представляющие активы предприятия. Для контроля активов вы можете просматривать таблицу устройств в разделе **Активы** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks. Также вы можете просматривать информацию о взаимодействиях устройств и выполнять различные действия с устройствами при работе с картой сетевых взаимодействий и с топологической картой.

Таблица устройств

Для контроля устройств в программе формируется таблица устройств. Все устройства, присутствующие в таблице, считаются известными программе. Вы можете просмотреть таблицу устройств в разделе **Активы** на вкладке **Устройства**.

Для таблицы устройств действуют следующие ограничения по количеству элементов:

- Суммарное количество устройств со статусами *Разрешенное* и *Неразрешенное* – не более 100 тыс.

  Если достигнуто ограничение максимального количества устройств со статусами *Разрешенное* и *Неразрешенное*, новые устройства с этими статусами не добавляются в таблицу. В этом случае, чтобы добавить новое устройство в таблицу, вам нужно удалить одно из ранее добавленных устройств.
- Количество устройств со статусом *Неиспользуемое* – не более 100 тыс.

  Если достигнуто ограничение максимального количества устройств со статусом *Неиспользуемое*, новые устройства с этим статусом добавляются в таблицу вместо устройств, которые дольше всего не проявляли активность.

При переполнении таблицы устройств программа выводит соответствующее сообщение.

Таблица устройств содержит следующие сведения:

- **Имя** – имя, под которым устройство представлено в программе.
- **ID устройства** – идентификатор устройства, присвоенный в Kaspersky Industrial CyberSecurity for Networks.

- **Статус** – статус устройства, определяющий разрешение активности устройства в промышленной сети. Устройство может иметь один из следующих статусов:

  - *Разрешенное*. Этот статус присваивается устройству, которому разрешена активность в промышленной сети.

  - *Неразрешенное*. Этот статус присваивается устройству, которому не разрешена активность в промышленной сети.

  - *Неиспользуемое*. Этот статус присваивается устройству, если оно больше не используется или не должно использоваться в промышленной сети, либо если устройство длительное время не проявляло активность и не изменялись сведения об этом устройстве (30 дней и более).

- **Адресная информация** – MAC- и/или IP-адреса устройства. Если устройство имеет несколько сетевых интерфейсов, можно указать различные MAC- и/или IP-адреса устройства на различных сетевых интерфейсах (в сведениях об устройстве могут быть представлены до 512 сетевых интерфейсов). Если в программу добавлены дополнительные адресные пространства, при настройке таблицы устройств можно включать и выключать отображение имен адресных пространств с помощью параметра **Отображать адресные пространства**. При просмотре сведений об устройстве информация об MAC- и/или IP-адресах устройства, а также адресных пространств отображается на вкладке **Адреса**.

- **Категория** – название категории, определяющей функциональное назначение устройства. В Kaspersky Industrial CyberSecurity for Networks предусмотрены следующие категории устройств:
  - **ПЛК** – программируемые логические контроллеры.
  - **IED** – интеллектуальные электронные устройства.
  - **HMI / SCADA** – компьютеры с установленным ПО систем человеко-машинного интерфейса (Human-machine interface, HMI) или SCADA-систем.
  - **Инженерная станция** – компьютеры с установленным ПО для использования инженерами АСУ ТП.
  - **Сервер** – устройства с установленным серверным ПО.
  - **Сетевое устройство** – устройства, относящиеся к сетевому оборудованию (например, маршрутизаторы, коммутаторы).
  - **Рабочая станция** – стационарные персональные компьютеры или рабочие станции операторов.
  - **Мобильное устройство** – портативные электронные устройства с функциями компьютера.
  - **Ноутбук** – переносные персональные компьютеры.
  - **HMI-панель** – устройства, использующие человеко-машинный интерфейс для управления отдельными устройствами или операциями технологического процесса.
  - **Принтер** – печатающие устройства.
  - **ИБП** – блоки бесперебойного питания, подключаемые к вычислительной сети.
  - **Сетевая камера** – устройства, выполняющие функции видеонаблюдения и передачи изображения в цифровом виде.
  - **Шлюз** – устройства для сопряжения сетей, преобразующие различные интерфейсы (например, Serial/Ethernet) в сетях с разнородной средой передачи данных и разными протоколами.
  - **Система хранения** – устройства для хранения информации внутри систем памяти.
  - **Брандмауэр** – устройства, выполняющие функции сетевого экрана для проверки и блокировки нежелательного трафика.
  - **Коммутатор** – устройства для физического соединения узлов локальной сети.
  - **Виртуальный коммутатор** – устройства, логически объединяющие физические коммутаторы, или программно реализованные коммутаторы для систем виртуализации.
  - **Маршрутизатор** – устройства, выполняющие функции перенаправления сетевых пакетов между сегментами вычислительной сети.
  - **Виртуальный маршрутизатор** – устройства, логически объединяющие физические маршрутизаторы, или маршрутизаторы, использующие несколько независимых таблиц маршрутизации.
  - **Wi-Fi** – точки доступа, обеспечивающие беспроводное подключение устройств из сетей Wi-Fi.
  - **Сервер Historian** – серверы архивных данных.

- **Другое** – устройства, не относящиеся к вышеперечисленным категориям.

- **Группа** – имя группы, в которую помещено устройство в дереве групп устройств (содержит имя самой группы и имена всех ее родительских групп).

- **Состояние безопасности** – состояние безопасности устройства, определяемое по наличию связанных с устройством событий. Предусмотрены следующие состояния безопасности:

  - *Критическое*. С устройством связаны события со значением оценки критичности в диапазоне 8.0–10.0.

  - *Важное*. С устройством связаны события со значением оценки критичности в диапазоне 4.0–7.9.

  - *OK*. С устройством связаны события со значением оценки критичности в диапазоне 0.0–3.9, или у устройства нет связанных событий.

- **Значимость** – значимость устройства для предприятия. Значимость присваивается устройству в соответствии с его категорией. Предусмотрены следующие значимости устройств:

  - *Высокая*. Присваивается устройствам категории **ПЛК**, **IED**, **HMI / SCADA** или **Сервер**.

  - *Средняя*. Присваивается устройствам категории **Инженерная станция**, **Сетевое устройство**, **Рабочая станция**, **HMI-панель**, **Шлюз**, **Система хранения**, **Брандмауэр**, **Коммутатор**, **Виртуальный коммутатор**, **Маршрутизатор**, **Виртуальный маршрутизатор**, **Wi-Fi** или **Сервер Historian**.

  - *Низкая*. Присваивается устройствам категории **Мобильное устройство**, **Ноутбук**, **Принтер**, **ИБП**, **Сетевая камера** или **Другое**.

- **Последнее появление** – дата и время последней зафиксированной активности устройства.

- **Риски** – категории рисков, обнаруженных для устройства. По умолчанию в таблице устройств отображается информация только по актуальным рискам. Для отображения информации по всем рискам можно установить флажок **Отображать устраненные и принятые риски** при настройке таблицы устройств.

- **Последнее изменение** – дата и время последнего изменения сведений об устройстве.

- **Создано** – дата и время добавления устройства в таблицу устройств.

- **ОС** – название операционной системы, установленной на устройстве.

- **Производитель аппаратной части** – название производителя аппаратного обеспечения устройства. В области деталей этот параметр называется **Производитель** и отображается на вкладке **Общие** в блоке параметров **Аппаратное обеспечение**.

- **Модель аппаратной части** – название модели устройства. В области деталей этот параметр называется **Модель** и отображается на вкладке **Общие** в блоке параметров **Аппаратное обеспечение**.

- **Версия аппаратной части** – номер версии аппаратного обеспечения устройства. В области деталей этот параметр называется **Версия** и отображается на вкладке **Общие** в блоке параметров **Аппаратное обеспечение**.

- **Производитель ПО** – название производителя программного обеспечения устройства. В области деталей этот параметр называется **Производитель** и отображается на вкладке **Общие** в блоке параметров **Программное обеспечение**.

- **Название ПО** – название программного обеспечения устройства. В области деталей этот параметр называется **Название** и отображается на вкладке **Общие** в блоке параметров **Программное обеспечение**.

- **Версия ПО** – номер версии программного обеспечения устройства. В области деталей этот параметр называется **Версия** и отображается на вкладке **Общие** в блоке параметров **Программное обеспечение**.

- **Сетевое имя** – имя, под которым устройство представлено в сети.

- **Метки** – список меток, назначенных устройству.

- **Параметры контроля процесса** – признак наличия или отсутствия параметров контроля процесса, заданных для устройства. В области деталей параметры контроля процесса, заданные для устройства, отображаются на вкладке **Контроль процесса**.

- **Приложение EPP** – краткое название EPP-приложения, установленного на устройстве (если данные от этого приложения поступали в Kaspersky Industrial CyberSecurity for Networks).

- **Подключение EPP** – статус подключения EPP-приложения, установленного на устройстве, к серверу интеграции. Предусмотрены следующие статусы:

  - *Активное*. Со времени последнего соединения приложения с сервером интеграции прошло менее суток.

  - *Неактивное*. Со времени последнего соединения приложения с сервером интеграции прошло более суток.

  - *Отсутствует*. Статус подключения неизвестен.

- **Последнее соединение с EPP** – Дата последнего соединения EPP-приложения, установленного на устройстве, с сервером интеграции.

При просмотре таблицы устройств вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Просмотр сведений об устройстве

Подробные сведения об устройстве включают информацию из таблицы устройств, а также следующие поля (если есть значения для этих полей):

- **Маршрутизирующее устройство** – признак маршрутизирующего устройства.

  Если признак маршрутизирующего устройства не был определен программой автоматически, то его требуется выставить вручную (например, для устройства, которое выполняет функции сетевого коммутатора между сегментами промышленной сети). Этот признак позволяет программе использовать дополнительные алгоритмы обнаружения устройств, взаимодействующих между собой через маршрутизирующее устройство. В частности, если выставлен признак маршрутизирующего устройства (автоматически или вручную) для сетевого коммутатора, который соединяет сегмент с несколькими ПЛК и сегмент компьютера со SCADA-системой, программа сможет обнаруживать и добавлять в таблицу устройств все новые устройства в первом сегменте, взаимодействующие с компьютером со SCADA-системой во втором сегменте.

- **Доп. сведения** – дополнительные сведения об устройстве, заданные пользователем программы (например, описание размещения устройства).

- **Пользовательские поля** – набор нестандартных сведений об устройстве, заданных пользователем программы (например, категории и классы защиты устройства). Для устройства может быть указано до 16 пользовательских полей.

- **Динамические поля** – набор расширенных сведений об устройстве, обнаруженных в трафике при работе метода обнаружения сведений об устройствах. Поле отображается, если расширенные сведения были обнаружены программой.

- **Endpoint Agent** – сведения о программном компоненте Endpoint Agent на устройстве.

- **Открытый ключ** – открытый ключ для проверки устройства перед установкой SSH-соединения и сканирования устройства в рамках заданий аудита безопасности.

- **Параметры топологии** – вкладка, содержащая сведения о последнем активном опросе устройства, а также сведения о соединениях устройства с другими узлами.

- **Оборудование** – вкладка, содержащая сведения о BIOS-программах и процессорах устройства, сведения об объемах свободной оперативной памяти и памяти на локальных дисках устройства, а также сведения об используемых USB-устройствах и оптических приводах. Сведения отображаются, если они были получены при использовании функциональности контроля оборудования.

- **Конфигурации** – вкладка, содержащая сведения о полученных конфигурациях устройства. Сведения отображаются, если они были получены по результатам выполнения заданий контроля конфигураций.

Чтобы просмотреть сведения об устройстве,

в разделе **Активы** на вкладке **Устройства** выберите нужное устройство.

В правой части окна веб-интерфейса появится область деталей. В области деталей отображаются все сведения, для которых заданы значения.

Автоматическое добавление и обновление устройств

Программа может автоматически добавлять устройства в таблицу и обновлять сведения об устройствах. Для автоматического добавления и обновления устройств в Kaspersky Industrial CyberSecurity for Networks требуется включить следующие методы контроля активов:

- Обнаружение активности устройств. При использовании этого метода программа добавляет в таблицу новые обнаруженные устройства по полученным MAC- и/или IP-адресам устройств. Если обнаружена активность уже известного программе устройства, программа может изменить его статус в зависимости от текущего режима работы контроля активов.

- Обнаружение сведений об устройствах. При использовании этого метода программа обновляет сведения об известных устройствах на основе полученных данных из трафика или от EPP-приложений. По данным из трафика обновляются те сведения, для которых включено автоматическое изменение в параметрах устройства (включено по умолчанию до изменения значения вручную пользователем программы). Если обнаружение сведений об устройствах выключено, программа не обновляет и не дополняет имеющиеся сведения об устройствах по поступающим данным из трафика и от EPP-приложений.

При добавлении устройства программа по умолчанию задает имя устройства по шаблону: **Устройство <значение внутреннего счетчика устройств>**. При этом значение внутреннего счетчика в имени устройства может не совпадать с идентификатором устройства, который отображается в столбце **ID устройства**.

С помощью метода обнаружения сведений об устройствах программа может обновить имя устройства после получения данных, представляющих следующие сведения:

- название модели устройства;

- сетевое имя, под которым устройство представлено в сети (сетевое имя устройства имеет приоритет при актуализации).

Программа может автоматически обновлять сведения, относящиеся к производителям сетевого оборудования устройств, на основе MAC-адресов устройств. Для определения производителей по MAC-адресам программа сверяет MAC-адреса устройств с диапазонами адресов, которые были зарегистрированы в открытой базе данных международной организации Institute of Electrical and Electronics Engineers (IEEE). Если производитель сетевого оборудования определен по MAC-адресу, то в качестве названия производителя программа сохраняет такое же название, какое представлено в базе данных IEEE.

После установки программы используется копия базы данных IEEE, содержащая сведения о MAC-адресах и производителях на момент выпуска текущей версии программы. Вы можете поддерживать локальную копию базы данных IEEE в актуальном состоянии, устанавливая обновления.

Автоматическое присвоение статусов устройств

При отслеживании активности устройств в промышленной сети программа может автоматически присваивать статусы обнаруженным устройствам по полученным MAC- и/или IP-адресам устройств. Статусы присваиваются в зависимости от текущего режима контроля активов.

В режиме обучения программа присваивает статус *Разрешенное* всем обнаруженным устройствам (как новым устройствам, так и ранее добавленным в таблицу устройств). Статус обнаруженного устройства не изменяется, если устройству ранее был присвоен статус *Неразрешенное*.

В режиме наблюдения присваиваемый статус зависит от того, является ли устройство, проявившее активность, известным или неизвестным программе. В этом режиме присвоение статусов происходит по следующим правилам:

- Если устройство является новым (отсутствовало в таблице устройств на момент обнаружения), этому устройству присваивается статус *Неразрешенное*.
- Если устройство присутствует в таблице устройств со статусом *Разрешенное* или *Неразрешенное*, статус не меняется.
- Если устройство присутствует в таблице устройств со статусом *Неиспользуемое*, этому устройству присваивается статус *Неразрешенное*.

По умолчанию если устройство со статусом *Разрешенное* не проявляет активность более 30 дней и за это время не изменялись сведения об устройстве, этому устройству автоматически присваивается статус *Неиспользуемое*. Вы можете выключить автоматическое изменение статуса устройства на статус *Неиспользуемое* при изменении статуса устройства вручную (например, чтобы статус *Разрешенное* не изменялся на статус *Неиспользуемое* для редко подключаемого устройства).

При использовании коннекторов типа **Cisco Switch** может происходить автоматическое ограничение сетевого доступа устройств после присвоения этим устройствам статуса *Неразрешенное*. Вам нужно учитывать заданные параметры коннекторов этого типа, чтобы не допустить блокировку нужных устройств из-за изменения их статуса.

При появлении в таблице устройств со статусом *Неразрешенное*, вам нужно определить, требуется ли каждое из этих устройств для обеспечения технологического процесса. После этого каждому такому устройству рекомендуется вручную присвоить один из следующих статусов:

- *Разрешенное* – если устройство требуется для обеспечения технологического процесса.
- *Неиспользуемое* – если устройство не должно использоваться в промышленной сети.

  Вместо присвоения статуса *Неиспользуемое* вы можете удалить устройство. Однако в этом случае также будут удалены все сведения, указанные для этого устройства. Если удаленное устройство снова будет обнаружено, в программе будут доступны только сведения, полученные с момента повторного добавления в таблицу устройств (в том числе обновится дата и время первого обнаружения устройства).

Дерево групп устройств

Дерево групп устройств предназначено для распределения устройств в соответствии с их назначением, размещением или по каким-либо другим произвольным признакам. Устройства могут быть распределены по группам вручную (например, для соответствия местоположению устройств в производственной структуре предприятия) или автоматически (по принадлежности IP-адресов устройств подсетям, по категориям устройств или по производителям).

Если устройство не включено ни в одну из групп, это устройство считается относящимся к верхнему уровню иерархии в дереве групп. Устройства, автоматически добавленные в таблицу, по умолчанию не включаются в группы.

Распределять устройства по группам могут только пользователи с ролью Администратор.

Узнать, в какие группы входят устройства, вы можете при просмотре таблицы устройств. Пути к группам указаны в столбце **Группа**. Группы устройств также отображаются и на карте сетевых взаимодействий, однако входящие в эти группы устройства могут не отображаться, если они не удовлетворяют параметрам фильтрации объектов на карте сетевых взаимодействий.

Контроль чтения и записи проектов ПЛК

Kaspersky Industrial CyberSecurity for Networks может обнаруживать в трафике промышленной сети информацию о проектах ПЛК и сравнивать эту информацию с ранее полученной информацией о проектах ПЛК.

Проект ПЛК – микропрограмма, написанная для ПЛК. Проект ПЛК хранится в памяти ПЛК и выполняется в рамках технологического процесса, использующего ПЛК. Проект ПЛК может состоять из блоков, которые по отдельности передаются и принимаются по сети при чтении или записи проекта.

Информация о проекте или блоке проекта ПЛК может быть получена программой при обнаружении операций чтения проекта/блока из ПЛК или записи проекта/блока в ПЛК. Полученная информация сохраняется в Kaspersky Industrial CyberSecurity for Networks. При следующем обнаружении операции чтения или записи проекта/блока программа сравнивает полученную информацию о проекте/блоке и сохраненную информацию. Если полученная информация о проекте/блоке не совпадает с последней сохраненной информацией об этом проекте/блоке (в том числе при отсутствии сохраненной информации), программа регистрирует соответствующее событие.

Получение информации о проектах ПЛК поддерживается для устройств следующих типов:

- Emerson DeltaV;
- Schneider Electric серии Modicon: M580, M340;
- Siemens серии SIPROTEC 4 и SIMATIC серий S7-300, S7-400, S7-1200, S7-1500.

Для контроля чтения и записи проектов ПЛК не требуется добавлять параметры контроля процесса для устройств. Контроль чтения и записи проектов ПЛК осуществляется для всех обнаруженных устройств перечисленных типов.

Для каждого устройства программа сохраняет не более 100 различных вариантов проектов ПЛК. Если проект ПЛК передается или принимается отдельными блоками, сохраняется до 100 различных вариантов каждого блока.

Если для устройства достигнуто ограничение максимального количества сохраненных проектов ПЛК (или одноименных блоков проекта ПЛК), программа сохраняет новый обнаруженный проект/блок вместо самого старого обнаруженного проекта/блока.

При контроле чтения и записи проектов ПЛК программа регистрирует события по технологии Контроль активов. Для регистрации используются системные типы событий, которым присвоены следующие коды:

- коды типов событий при обнаружении чтения проекта/блока из ПЛК:
  - 4000005200 – для события обнаружения чтения неизвестного блока проекта из ПЛК (если отсутствует сохраненная информация об этом блоке);
  - 4000005201 – для события обнаружения чтения известного блока проекта из ПЛК (если есть сохраненная информация об этом блоке, но полученная информация не совпадает с последней сохраненной информацией об этом блоке);
  - 4000005204 – для события обнаружения чтения неизвестного проекта из ПЛК (если отсутствует сохраненная информация об этом проекте);
  - 4000005205 – для события обнаружения чтения известного проекта из ПЛК (если есть сохраненная информация об этом проекте, но полученная информация не совпадает с последней сохраненной информацией об этом проекте);
- коды типов событий при обнаружении записи проекта/блока в ПЛК:
  - 4000005202 – для события обнаружения записи нового блока проекта в ПЛК (если отсутствует сохраненная информация об этом блоке);
  - 4000005203 – для события обнаружения записи известного блока проекта в ПЛК (если есть сохраненная информация об этом блоке, но полученная информация не совпадает с последней сохраненной информацией об этом блоке);
  - 4000005206 – для события обнаружения записи нового проекта в ПЛК (если отсутствует сохраненная информация об этом проекте);
  - 4000005207 – для события обнаружения записи известного проекта в ПЛК (если есть сохраненная информация об этом проекте, но полученная информация не совпадает с последней сохраненной информацией об этом проекте).

Вы можете настроить доступные параметры для типов событий в разделе **Параметры → Типы событий**.

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-интерфейс.

Контроль оборудования на промышленных устройствах

Kaspersky Industrial CyberSecurity for Networks может контролировать оборудование на специализированных промышленных устройствах (таких, как ПЛК), которые обеспечивают автоматизацию технологического процесса. Контроль оборудования поддерживается для устройств следующих типов:

- Siemens SIMATIC серий S7-300, S7-400.
- Schneider Electric серии Modicon: M580, M340.
- Emerson DeltaV (поддерживается только в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1).
- Rockwell Automation Allen-Bradley (поддерживается только в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1).

Программа получает сведения об оборудовании промышленных устройств с помощью коннекторов типа **Active poll**. После добавления коннекторов в программу вы можете их использовать для получения сведений в следующих типах заданий для аудита безопасности:

- Задания контроля конфигураций. Рекомендуется использовать этот тип заданий, если вы хотите применять режим обработки конфигураций **Архивирование версий** или **Сравнение с эталоном** в отношении сведений об оборудовании на промышленных устройствах. Для получения сведений об оборудовании вам нужно выбрать тип конфигурации **ПЛК** при добавлении или изменении задания контроля конфигураций.

- Задания активных опросов. Рекомендуется использовать этот тип заданий, если вы хотите совместно со сведениями об оборудовании получать и другую информацию, которая предусмотрена предоставляемыми методами проведения активных опросов. Для получения сведений об оборудовании на промышленных устройствах вам нужно выбрать параметр **Расширенная конфигурация промышленного устройства** и затем выбрать соответствующие методы получения расширенной конфигурации (в зависимости от выбранных устройств) при добавлении или изменении задания активного опроса.

После сканирования промышленного устройства в рамках задания контроля конфигураций или активного опроса программа обновляет сведения об оборудовании этого устройства. Обновление не выполняется для тех сведений, для которых выключено автоматическое изменение при добавлении устройства или при изменении сведений об устройстве. Возможность выключения автоматического изменения доступна не для всех сведений об оборудовании.

Функциональность контроля оборудования на промышленных устройствах позволяет программе получать сведения, перечисленные в таблице ниже.

Сведения, получаемые при контроле оборудования на промышленных устройствах

Тип сведений	Отображается на вкладке в области деталей устройства	Возможность выключить автоматическое изменение
Графическая схема расположения модулей в слотах	**Оборудование**	—
Подробные сведения о каждом модуле	**Оборудование**, **Конфигурации**	—
Расширенные сведения об устройстве в виде записей с ключами и их значениями (например, состояние памяти и параметры безопасности устройства)	**Оборудование**, **Конфигурации**	—
Сведения о проекте ПЛК и блоках проекта	**Конфигурации**	—
Производитель аппаратного обеспечения (аппаратной части)	**Общие**	✓
Модель аппаратного обеспечения (аппаратной части)	**Общие**	✓
Версия аппаратного обеспечения (аппаратной части)	**Общие**	✓
Версия программного обеспечения	**Общие**	✓

В дополнение к перечисленным сведениям в программу также может быть загружено содержимое журналов, хранящихся в модуле центрального процессора (CPU). Если к устройству подключено несколько модулей CPU, загружаются журналы того модуля, с которым установил соединение коннектор Kaspersky Industrial CyberSecurity for Networks. Вы можете скачать файл с журналами устройства по ссылке на вкладке **Оборудование** в области деталей устройства.

Контроль оборудования на Windows- и Linux-устройствах

Kaspersky Industrial CyberSecurity for Networks может контролировать оборудование на устройствах под управлением операционных систем семейств Windows и Linux. При контроле оборудования программа автоматически получает сведения об оборудовании устройств и регистрирует события, если меняется состав оборудования или его характеристики.

Контроль оборудования на Windows- и Linux-устройствах выполняется, если на этих устройствах есть программный компонент Endpoint Agent и настроена интеграция EPP-приложений с Kaspersky Industrial CyberSecurity for Networks. Поэтому для использования функциональности контроля оборудования вам нужно подготовить программу к получению данных от EPP-приложений. При этом на узлах серверов интеграции должны быть включены методы контроля активов для обнаружения активности устройств и обнаружения сведений об устройствах.

Периодичность обновления сведений об оборудовании Windows- или Linux-устройства – один раз в сутки. Обновление не выполняется для тех сведений, для которых выключено автоматическое изменение при добавлении устройства или при изменении сведений об устройстве. Возможность выключения автоматического изменения доступна не для всех сведений об оборудовании.

Функциональность контроля оборудования на Windows- и Linux-устройствах позволяет программе получать сведения, перечисленные в таблице ниже.

Сведения, получаемые при контроле оборудования на Windows- и Linux-устройствах

Тип сведений	Отображается на вкладке в области деталей устройства	Возможность выключить автоматическое изменение
Процессоры	**Оборудование**	—
BIOS	**Оборудование**	—
ОЗУ	**Оборудование**	—
Локальные диски	**Оборудование**	—
Оптические приводы	**Оборудование**	—
USB-устройства	**Оборудование**	—
Сетевые интерфейсы, имеющие MAC-адрес	**Адреса**	✓
Производитель аппаратного обеспечения (аппаратной части)	**Общие**	✓
Модель аппаратного обеспечения (аппаратной части)	**Общие**	✓
Версия аппаратного обеспечения (аппаратной части)	**Общие**	✓

При контроле оборудования на Windows- и Linux-устройствах программа регистрирует события по технологии Контроль активов. Для регистрации используются системные типы событий, которым присвоены следующие коды:

- 4000005015 – для события добавления, изменения или удаления любого из следующих типов сведений:
  - Процессоры.
  - BIOS.
  - ОЗУ.
  - Локальные диски.
  - Оптические приводы.
  - USB-устройства.
- 4000005008 – для события получения новых сведений о сетевом интерфейсе.
- 4000005004 – для события получения новых сведений о производителе, модели или версии аппаратного обеспечения (аппаратной части).

Вы можете настроить доступные параметры для типов событий в разделе **Параметры** → **Типы событий**.

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-интерфейс.

Контроль пользователей на устройствах

Kaspersky Industrial CyberSecurity for Networks может контролировать учетные записи пользователей на устройствах, известных программе. При контроле пользователей программа автоматически получает сведения об учетных записях, зарегистрированных в операционных системах устройств. По полученным сведениям программа формирует таблицы пользователей.

При получении сведений об учетных записях программа контролирует по этим сведениям все учетные записи пользователей на устройствах, за исключением некоторых локальных системных учетных записей, которые могут использовать только системные службы операционной системы. Например, программа не контролирует учетные записи LocalSystem и NetworkService, используемые на устройствах под управлением операционных систем семейства Windows.

Для использования функциональности контроля пользователей должны быть включены методы контроля активов для обнаружения активности устройств и обнаружения сведений об устройствах. Эти методы должны быть включены на всех узлах с установленными компонентами программы, от которых поступают сведения.

Контроль пользователей выполняется на основании данных, поступающих от источников следующих типов:

1. **OVAL-сканирование** – программные компоненты, с помощью которых выполняются сканирования устройств по встроенным OVAL-правилам (EPP-приложения, отправляющие расширенные данные об устройствах по запросам Kaspersky Industrial CyberSecurity for Networks, или узлы с установленными компонентами программы, с которых выполняются удаленные подключения к устройствам при сканировании устройств в рамках заданий контроля конфигураций).

2. **Телеметрия (Endpoint Agent)** – EPP-приложения, отправляющие в Kaspersky Industrial CyberSecurity for Networks основные данные об устройствах и о выполняемых процессах (данные телеметрии).

3. **Трафик** – точки мониторинга, на которых выполняется анализ поступающего трафика по правилам определения сведений об устройствах и протоколов взаимодействия устройств.

4. **Внешний источник** – приложения, использующие Kaspersky Industrial CyberSecurity for Networks API и отправляющие в Kaspersky Industrial CyberSecurity for Networks сведения о пользователях.

Источники перечислены в порядке уменьшения приоритета данных, поступающих от этих источников. Программа обрабатывает сведения о пользователях в соответствии с приоритетом поступивших данных. Сведения о пользователях, полученные от более приоритетного источника, могут заместить собой сведения от других источников. Также программа автоматически удаляет из таблиц учетные записи пользователей, сведения о которых ранее были получены от источников **OVAL-сканирование** и **Внешний источник**, но в новых поступивших данных от этих источников такие пользователи отсутствуют.

При необходимости пользователи с ролью Администратор могут удалять учетные записи пользователей вручную.

Вы можете просматривать сведения о пользователях в разделе **Активы** на вкладке **Пользователи**. При просмотре таблицы пользователей вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Для таблицы всех пользователей действует ограничение по количеству элементов – не более 200 000.

Программа отображает следующие сведения о пользователях устройств в таблице и области деталей выбранного пользователя:

- **ID пользователя** – идентификатор пользователя, присвоенный в Kaspersky Industrial CyberSecurity for Networks.

- **Имя пользователя** – имя учетной записи пользователя без указания домена или сетевого имени устройства.

- **Полное имя** – имя учетной записи пользователя с указанным именем домена или сетевым именем устройства.

- **Группы** – имена групп пользователей, в которые добавлена учетная запись пользователя.

- **Устройство** – имя и адрес устройства.

- **Источник** – тип источника данных о пользователе.

- **SID** – идентификатор безопасности пользователя.

- **Статус учетной записи** – статус, соответствующий полученному значению параметра для включения и выключения использования учетной записи.

- **Блокировка** – статус, соответствующий полученному значению параметра блокировки учетной записи.
- **Смена пароля при следующем входе** – признак включенного или выключенного состояния параметра, определяющего необходимость смены пользователем его пароля при следующем входе в систему.
- **Запрет смены пароля пользователем** – признак включенного или выключенного состояния параметра, определяющего запрет смены пользователем его пароля.
- **Срок действия пароля** – статус, соответствующий полученному значению параметра для включения и выключения ограничения на срок действия пароля пользователя.
- **Данные получены** – дата и время последнего получения сведений об учетной записи.
- **Описание** – описание, заданное для учетной записи.

При контроле пользователей программа регистрирует события по технологии Контроль активов. Для регистрации используется системный тип события, которому присвоен код 4000005600. События регистрируются, если на устройствах автоматически добавлены, изменены или удалены учетные записи пользователей.

Вы можете настроить доступные параметры для типов событий в разделе **Параметры** → **Типы событий**.

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-интерфейс.

Контроль приложений и патчей на устройствах

Kaspersky Industrial CyberSecurity for Networks может контролировать приложения и патчи, которые установлены на устройствах, известных программе. При контроле приложений и патчей программа автоматически получает сведения о программном обеспечении, установленном и зарегистрированном в операционных системах устройств. По полученным сведениям программа формирует таблицы приложений и патчей.

Для использования функциональности контроля приложений и патчей должны быть включены методы контроля активов для обнаружения активности устройств и обнаружения сведений об устройствах. Эти методы должны быть включены на всех узлах с установленными компонентами программы, от которых поступают сведения.

Контроль приложений и патчей выполняется на основании данных, поступающих от источников следующих типов:

1. **OVAL-сканирование** – программные компоненты, с помощью которых выполняются сканирования устройств по встроенным OVAL-правилам (EPP-приложения, отправляющие расширенные данные об устройствах по запросам Kaspersky Industrial CyberSecurity for Networks, или узлы с установленными компонентами программы, с которых выполняются удаленные подключения к устройствам при сканировании устройств в рамках заданий контроля конфигураций).
2. **Внешний источник** – приложения, использующие Kaspersky Industrial CyberSecurity for Networks API и отправляющие в Kaspersky Industrial CyberSecurity for Networks сведения о приложениях и патчах.

Источники перечислены в порядке уменьшения приоритета данных, поступающих от этих источников. Программа обрабатывает сведения о приложениях и патчах в соответствии с приоритетом поступивших данных. Сведения о приложениях или патчах, полученные от более приоритетного источника, могут заместить собой сведения от других источников. Также программа автоматически удаляет из таблиц приложения или патчи, сведения о которых ранее были получены, но в новых поступивших данных от этих источников такие приложения или патчи отсутствуют.

Вы можете просматривать сведения о приложениях и патчах в следующих таблицах:

- Таблица всех приложений в разделе **Активы** на вкладке **Приложения**.

  В этой таблице отображаются сведения обо всех приложениях, данные о которых получены программой. При просмотре таблицы всех приложений вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

- Таблица всех патчей в разделе **Активы** на вкладке **Патчи**.

  В этой таблице отображаются сведения обо всех патчах, данные о которых получены программой. При просмотре таблицы всех патчей вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Для таблиц всех приложений и всех патчей действует ограничение по количеству элементов в каждой таблице – не более 200 000.

Программа отображает следующие сведения о приложениях устройств в таблице и области деталей выбранного приложения:

- **ID приложения** – идентификатор приложения, присвоенный в Kaspersky Industrial CyberSecurity for Networks.
- **Название** – название приложения.
- **Поставщик** – название поставщика приложения.
- **Устройство** – имя и адрес устройства.
- **Источник** – тип источника данных о приложении.
- **Установлено** – дата и время установки приложения.
- **Размер** – объем дискового пространства, занятого файлами приложения.
- **Версия** – номер версии приложения.
- **Данные получены** – дата и время последнего получения сведений о приложении.
- **Описание** – описание, заданное для приложения.

Программа отображает следующие сведения о патчах устройств в таблице и области деталей выбранного патча:

- **ID патча** – идентификатор патча, присвоенный в Kaspersky Industrial CyberSecurity for Networks.
- **Название** – название патча.
- **Продукт** – название программного продукта, для которого установлен патч.

- **Версия** – номер версии патча.
- **Поставщик** – название поставщика патча.
- **Устройство** – имя и адрес устройства.
- **Источник** – тип источника данных о патче.
- **Установлен** – дата и время установки патча.
- **Данные получены** – дата и время последнего получения сведений о патче.
- **Описание** – описание, заданное для патча.

При контроле приложений и патчей программа регистрирует события по технологии Контроль активов. Для регистрации используются системные типы событий, которым присвоены следующие коды:

- 4000005601 – для события добавления или удаления приложений;
- 4000005602 – для события добавления или удаления патчей.

Вы можете настроить доступные параметры для типов событий в разделе **Параметры** → **Типы событий**.

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-интерфейс.

Контроль запусков исполняемых файлов на устройствах

Kaspersky Industrial CyberSecurity for Networks может контролировать запуски исполняемых файлов на устройствах, известных программе. Контроль запусков исполняемых файлов выполняется на основании данных, которые поступают от EPP-приложений и/или от приложений, использующих Kaspersky Industrial CyberSecurity for Networks API. По полученным сведениям программа формирует таблицу исполняемых файлов.

Автоматическое получение сведений о запусках исполняемых файлов возможно для устройств, на которых есть программный компонент Endpoint Agent, взаимодействующий с EPP-приложением и отправляющий в Kaspersky Industrial CyberSecurity for Networks основные данные об устройствах и о выполняемых процессах (данные телеметрии). Для этих сведений в программе указан источник **Телеметрия (Endpoint Agent)**. Если сведения о запуске исполняемого файла поступили только от приложения, использующего Kaspersky Industrial CyberSecurity for Networks API, для этого файла в программе указан источник данных **Внешний источник**.

Для получения сведений о запусках исполняемых файлов от источника **Телеметрия (Endpoint Agent)** должны быть включены методы контроля активов для обнаружения активности устройств и обнаружения сведений об устройствах. Эти методы должны быть включены на всех узлах с установленными компонентами программы, от которых поступают данные от EPP-приложений.

Для таблицы исполняемых файлов действуют следующие ограничения по количеству и времени хранения элементов:

- Общее количество исполняемых файлов – не более 100 тыс.

  Если достигнуто ограничение максимального количества исполняемых файлов, программа автоматически удаляет 10% самых старых записей.

- Максимальное время хранения исполняемого файла до следующего получения данных о запуске этого файла – не более 90 дней.

  Если новые данные о запуске исполняемого файла не были получены до истечения максимального времени хранения, программа автоматически удаляет запись об этом файле.

При необходимости пользователи с ролью Администратор могут удалять исполняемые файлы вручную.

Вы можете просматривать сведения об исполняемых файлах в разделе **Активы** на вкладке **Исполняемые файлы**. При просмотре таблицы исполняемых файлов вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Программа отображает следующие сведения об исполняемых файлах устройств в таблице и области деталей выбранного файла:

- **ID файла** – идентификатор файла, присвоенный в Kaspersky Industrial CyberSecurity for Networks.
- **Устройство** – имя и адрес устройства.
- **Имя** – название и версия приложения или имя файла.
- **Данные получены** – дата и время последнего получения сведений о файле.
- **Продукт** – название программного продукта, сохраненное в операционной системе устройства.
- **Версия продукта** – версия программного продукта, сохраненная в операционной системе устройства.
- **Поставщик** – название поставщика приложения.
- **Путь** – полный путь к файлу.
- **Размер файла** – объем дискового пространства, занятого файлом.
- **Хеш MD5** – контрольная сумма файла, полученная с помощью алгоритма хеширования MD5.
- **Хеш SHA256** – контрольная сумма файла, полученная с помощью алгоритма хеширования SHA256.
- **Подпись** – результат проверки цифровой подписи файла: **Действительная** (если проверка цифровой подписи пройдена успешно) или **Недействительная** (например, если истек срок годности сертификата).
- **Создан** – дата и время создания файла.
- **Изменен** – дата и время последнего изменения файла.
- **Источник** – тип источника данных о файле.
- **Атрибуты** – список атрибутов файла.
- **Описание** – описание, заданное для файла.

Контроль конфигураций устройств

Kaspersky Industrial CyberSecurity for Networks предоставляет возможности для просмотра сведений о конфигурациях устройств, полученных по результатам выполнения заданий контроля конфигураций. Вы можете просматривать сведения о конфигурациях выбранного устройства в области деталей устройства на вкладке **Конфигурации**.

Программа отображает следующие сведения о полученных конфигурациях выбранного устройства в таблице на вкладке **Конфигурации**:

- **Компонент конфигурации** – название полученного компонента конфигурации (например, компонент **Пользователи**, в котором сохранены сведения о пользователях устройства).
- **Дата и время последней** – дата и время последнего получения компонента конфигурации, если включено отображение последних полученных конфигураций.
- **Дата и время эталонной** – дата и время получения компонента эталонной конфигурации, если включено отображение эталонных конфигураций.
- **Архивных записей** (отображается в версии Kaspersky Industrial CyberSecurity for Networks 4.2) – количество записей с уникальными конфигурациями компонента, которые были помещены в архив при выполнении заданий контроля конфигураций в режимах **Архивирование версий** и/или **Сравнение с эталоном**. Количество приводится без учета текущей и эталонной конфигураций.
- **Архивных записей** (отображается в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1) – общее количество конфигураций компонента, полученных при выполнении заданий контроля конфигураций. Количество приводится без учета уникальности данных в этих конфигурациях (конфигурации могут быть одинаковыми и отличаться только временем получения).

Компоненты эталонной конфигурации отмечены значком короны .

При выборе компонента конфигурации появляется окно с подробными сведениями об этом компоненте.

Для удобного просмотра сведений о конфигурациях устройства вы можете сравнивать сохраненные конфигурации с помощью Kaspersky Industrial CyberSecurity for Networks.

При контроле конфигураций устройств программа регистрирует события по технологии Контроль активов. Для регистрации используются системные типы событий, которым присвоены следующие коды:

- 4000005603 – для события обнаружения изменений при сравнении с предыдущей конфигурацией по результатам сканирования устройства (для заданий в режимах обработки конфигураций **Только обновление** и/или **Архивирование версий**);
- 4000005604 – для события обнаружения изменений при сравнении с эталонной конфигурацией по результатам сканирования устройства (для заданий в режиме обработки конфигураций **Сравнение с эталоном**).

Вы можете настроить доступные параметры для типов событий в разделе **Параметры** → **Типы событий**.

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-интерфейс.

Сравнение сохраненных конфигураций устройства

По результатам сканирований устройств в рамках заданий контроля конфигураций программа может сохранять полученные конфигурации для каждого устройства. Вы можете сравнивать сохраненные конфигурации устройства при работе с таблицей устройств.

В отличие от алгоритмов обнаружения изменений и регистрации событий при контроле конфигураций устройств, при использовании функции сравнения сохраненных конфигураций вы можете сравнить любые сохраненные конфигурации устройства (не только последнюю полученную конфигурацию с предыдущей или эталонной). Эта возможность доступна, если для устройства сохранены конфигурации, полученные по результатам выполнения заданий.

При сравнении конфигураций устройства вам нужно учитывать, что полученные программой конфигурации хранятся в хранилищах временно и автоматически удаляются по мере поступления новых конфигураций (периодичность удаления конфигураций зависит от интенсивности и объема поступающих сведений). Автоматическое удаление не затрагивает только эталонные и последние полученные конфигурации. При необходимости пользователи с ролью Администратор могут назначать любые сохраненные конфигурации в качестве эталонных конфигураций.

Чтобы сравнить сохраненные конфигурации устройства:

1. В разделе **Активы** на вкладке **Устройства** выберите нужное устройство.

   В правой части окна веб-интерфейса появится область деталей.

2. На вкладке **Конфигурации** в области деталей выберите строку таблицы с нужным компонентом конфигурации (например, компонент **Локальные пользователи и группы**, в котором сохранены сведения о пользователях устройства). Для выбранного компонента в программе должно быть ненулевое количество уникальных записей, указанное в столбце **Архивных записей** (в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1 – количество 2 или больше в столбце **Архивных записей**).

   Появится окно с подробными сведениями о выбранном компоненте конфигурации.

3. Нажмите на кнопку **Сравнить**.

   Появится окно с результатами сравнения выбранного компонента конфигурации с предыдущей или эталонной конфигурацией. В верхней части окна отображаются дата и время получения сравниваемых конфигураций.

4. Выполните следующие действия:

   - Если вы хотите сравнить с другой сохраненной конфигурацией, выберите дату и время получения этой конфигурации в раскрывающемся списке.

   - При необходимости измените положение сравниваемых конфигураций относительно друг друга. Для этого используйте кнопку между раскрывающимися списками с датами и временем.

   - При необходимости выключите отображение неизмененных блоков в сравниваемых конфигурациях.

Работа с картой сетевых взаимодействий

Карта сетевых взаимодействий – это визуальное отображение обнаруженных взаимодействий между устройствами промышленной сети. С помощью карты сетевых взаимодействий вы можете просматривать сведения о взаимодействиях устройств в различные периоды времени.

На карте сетевых взаимодействий могут отображаться следующие объекты:

- Узлы. Эти объекты обозначают отправителей и получателей сетевых пакетов.
- Группы устройств. Эти объекты соответствуют группам в дереве групп устройств. Группы содержат узлы, представляющие включенные в эти группы устройства, и дочерние группы.
- Соединения. Эти объекты обозначают взаимодействия между узлами.

Узлы и соединения появляются на карте сетевых взаимодействий на основании данных, полученных из трафика или от EPP-приложений за определенный промежуток времени. Группы устройств отображаются постоянно.

При необходимости вы можете использовать фильтрацию узлов и соединений. По умолчанию на карте сетевых взаимодействий в онлайн-режиме отображаются объекты с заданным периодом для фильтрации длительностью один час.

Объекты, требующие внимания, визуально выделяются на карте сетевых взаимодействий. Программа считает требующими внимания следующие объекты:

- Узел, если с этим узлом связаны необработанные события со значением оценки 4.0 и выше, либо если этот узел представляет устройство со статусом *Неразрешенное*.
- Соединение, если к нему относятся события со значением оценки 4.0 и выше. Учитываются события, зарегистрированные в течение заданного периода для фильтрации объектов. При этом текущий статус событий не учитывается.
- Группа, если она содержит устройства, требующие внимания, или есть требующие внимания соединения от узлов этой группы. Рассматриваются объекты как в самой группе, так и в любой дочерней группе всех уровней вложенности.

Узлы на карте сетевых взаимодействий

Узлы на карте сетевых взаимодействий могут быть следующих типов:

- Известное программе устройство. Узел этого типа представляет устройство, входящее в таблицу устройств.
- Неизвестное программе устройство. Узел этого типа представляет устройство с уникальным IP- или MAC-адресом, не входящее в таблицу устройств. Такой узел может появиться на карте сетевых взаимодействий, например, в случае отправки сетевых пакетов с помощью команды `ping` на адрес несуществующего устройства. Узлы неизвестных программе устройств отображаются по отдельности, если их общее количество (в соответствии с текущими параметрами фильтрации на карте сетевых взаимодействий) не превышает 100. Если таких узлов больше, отображается один общий узел неизвестных устройств.
- WAN. Узел этого типа представляет устройства глобальной сети (Wide Area Network), с которыми соединяются устройства из промышленной сети. Устройствами глобальной сети считаются все устройства, у которых IP-адреса принадлежат только известным программе подсетям с типом **Публичная**.

Отображаемая информация на узлах, представляющих известные программе устройства

Для узлов, представляющих известные программе устройства, при максимальном масштабе карты сетевых взаимодействий отображается следующее:

- Заданное имя устройства.
- Значок категории устройства.
- IP-адрес устройства (если IP-адрес не задан, отображается MAC-адрес).
- Различные значки в зависимости от выполнения следующих условий:
  - если для устройства задан признак маршрутизирующего устройства;
  - если на устройстве установлено EPP-приложение (цвет значка зависит от состояния подключения);
  - если устройство имеет статус *Неиспользуемое*.
- Утолщенная линия на левой границе узла одного из следующих цветов в зависимости от состояния безопасности устройства:
  - зеленый цвет – состояние безопасности *OK*;
  - желтый цвет – состояние безопасности *Важное*;
  - красный цвет – состояние безопасности *Критическое*.

Если устройство имеет статус *Неразрешенное* или состояние безопасности устройства отличается от состояния *OK*, фон узла закрашен красным цветом.

Отображаемая информация на узлах, представляющих неизвестные программе устройства

Для узлов, представляющих неизвестные программе устройства, при максимальном масштабе карты сетевых взаимодействий отображается следующее:

- Если узел представляет одно неизвестное устройство, отображается IP- или MAC-адрес устройства. Если узел является общим узлом неизвестных устройств (узел, объединяющий более 100 неизвестных программе устройств), отображается **Неизвестные устройства**.
- Значок неизвестного устройства и его статуса.

Узлы, представляющие неизвестные программе устройства, имеют серый цвет фона.

Отображаемая информация на узлах WAN

Для узлов WAN при максимальном масштабе карты сетевых взаимодействий отображается следующее:

- Имя узла: **WAN**.
- Значок узла WAN.

Группы устройств на карте сетевых взаимодействий

Группы из дерева групп устройств могут отображаться на карте сетевых взаимодействий в свернутом или развернутом состояниях. Свернутые группы отображаются в виде значков, аналогичных узлам. Развернутые группы отображаются в виде окон с включенными в них узлами и другими группами.

Отображаемая информация на свернутых группах

Если группа свернута, при максимальном масштабе карты сетевых взаимодействий отображается следующее:

- Имя группы.
- Количество устройств, удовлетворяющих текущим параметрам фильтрации на карте сетевых взаимодействий. Учитываются устройства в этой группе и в ее дочерних группах всех уровней вложенности.
- Количество дочерних групп всех уровней вложенности.

Если группа содержит устройства или соединения, требующие внимания, (в том числе в дочерних группах любого уровня вложенности), рамка этой группы окрашивается красным цветом.

Отображаемая информация на развернутых группах

Окно развернутой группы содержит заголовок с именем группы и область для отображения объектов. В окне группы отображаются включенные в эту группу устройства, а также дочерние группы следующего уровня вложенности. Из числа устройств, включенных в группу, отображаются только те устройства, которые удовлетворяют текущим параметрам фильтрации на карте сетевых взаимодействий.

Если группа содержит устройства или соединения, требующие внимания, (в том числе в дочерних группах любого уровня вложенности), окно закрашено красным фоном.

Сворачивание и разворачивание групп

Если группа свернута, вы можете ее развернуть двойным щелчком мыши на значке группы. Если группа развернута, вы можете ее свернуть двойным щелчком мыши на заголовке окна этой группы или с помощью кнопки в заголовке.

Чтобы одновременно развернуть несколько свернутых групп:

1. На карте сетевых взаимодействий выберите несколько свернутых групп, выполнив одно из следующих действий:
   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными группами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные свернутые группы с помощью мыши.
2. Нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий (кнопка доступна, если выбрана хотя бы одна свернутая группа).

Чтобы одновременно свернуть все развернутые группы,

нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий (кнопка доступна, если развернута хотя бы одна группа).

Соединения на карте сетевых взаимодействий

Соединения на карте сетевых взаимодействий определяются по обнаруженным сетевым пакетам, в которых адреса отправителей и получателей можно сопоставить с адресами узлов.

Каждое соединение показывает две стороны взаимодействия. Стороной взаимодействия в соединении может быть один из следующих объектов на карте сетевых взаимодействий:

- узел одного из типов:
  - известное программе устройство;
  - неизвестное программе устройство;
  - общий узел неизвестных устройств – если соединение показывает взаимодействие с одним или несколькими неизвестными устройствами этого узла;
  - узел WAN – если соединение показывает взаимодействие, в котором отправителем сетевых пакетов является устройство глобальной сети (IP-адрес принадлежит только известным программе подсетям с типом **Публичная**);
- свернутая группа, если соединение показывает взаимодействие с одним или несколькими устройствами в этой группе.

В зависимости от значений оценок событий, зарегистрированных при обнаружении взаимодействий, линия соединения может быть окрашена следующими цветами:

- Серый цвет – взаимодействие не вызвало регистрацию событий или зарегистрированы только события со значениями оценок 0.0–3.9.
- Красный цвет – взаимодействие вызвало регистрацию событий со значениями оценок 4.0–10.0.

Для соединений учитываются события, зарегистрированные в течение заданного период для фильтрации объектов. При этом текущий статус событий не учитывается.

Программа сохраняет данные о соединениях в базе данных на Сервере. Суммарный объем сохраняемых записей не может превышать заданного ограничения. Если объем превышает заданное ограничение, программа автоматически удаляет 10% самых старых записей. Вы можете задать ограничение максимального объема для карты сетевых взаимодействий при настройке параметров хранения данных на узле Сервера.

Просмотр подробных сведений об объектах

Подробные сведения об объектах, представленных на карте сетевых взаимодействий, отображаются в области деталей. Для отображения подробных сведений вы можете выбрать объект с помощью мыши (если вы хотите просмотреть сведения о группе, требуется сначала свернуть группу).

Для узлов отображаются следующие сведения:

- Если узел представляет известное программе устройство, в области деталей отображаются те же сведения, которые выводятся в таблице устройств.
- Если узел представляет одно неизвестное программе устройство, в области деталей отображаются MAC- и/или IP-адреса устройства (с именами адресных пространств, если в программу добавлены дополнительные адресные пространства).
- Если выбран общий узел неизвестных устройств, отображаются следующие сведения:
  - Количество узлов, которые объединяет этот узел с учетом текущих параметров фильтрации.
  - **IP-адреса** – количество IP-адресов неизвестных устройств и первые 100 IP-адресов (с именами адресных пространств, если в программу добавлены дополнительные адресные пространства). Раздел отображается, если среди узлов неизвестных устройств есть узлы с IP-адресами.
  - **MAC-адреса** – количество MAC-адресов неизвестных устройств и первые 100 MAC-адресов (с именами адресных пространств, если в программу добавлены дополнительные адресные пространства). Раздел отображается, если среди узлов неизвестных устройств есть узлы с MAC-адресами.
- Если выбран узел WAN, отображаются следующие сведения:
  - **Исключить заданные адреса** – признак исключения из группы устройств всех устройств, адреса которых входят в перечисленные подсети.
  - **Подсети** – раздел со списком известных программе подсетей, для которых указан тип **Публичная** (внешние сети).

Для групп отображаются следующие сведения:

- **Родительская группа** – путь к группе в дереве групп устройств. Если группа относится к верхнему уровню иерархии, отображается **отсутствует (эта группа верхнего уровня)**.
- Количество устройств и групп в выбранной группе и в ее дочерних группах всех уровней вложенности.
- Сведения о количестве объектов, требующих внимания, в выбранной группе и в ее дочерних группах всех уровней вложенности. Если таких объектов нет, отображается состояние безопасности *OK*.

Для соединений отображаются следующие сведения:

- **Уровень важности** – значок, соответствующий максимальному уровню критичности событий, связанных с соединением. Если с соединением не связано ни одно событие, отображается **Без событий**. Учитываются события, зарегистрированные в течение заданного период для фильтрации объектов. При этом текущий статус событий не учитывается.
- Разделы с основными сведениями о первой и второй сторонах взаимодействия:
  - Если стороной взаимодействия является узел известного устройства или узел неизвестного устройства, в разделе отображается имя или адрес устройства, категория и адресная информация (при этом для известного программе устройства адресная информация представлена только по тем сетевым интерфейсам, которые использовались при взаимодействии). Для известного устройства также отображается статус устройства.
  - Если стороной взаимодействия является свернутая группа, в разделе отображается имя группы и количество устройств и дочерних групп в ней.
  - Если стороной взаимодействия является общий узел неизвестных устройств, в разделе отображается имя узла **Неизвестные устройства** и количество узлов, объединенных в этом узле.
- **Протоколы** – раздел со списком протоколов, используемых при взаимодействии. Для каждого протокола указан объем переданных данных, вычисленный по обнаруженным сетевым пакетам. Раздел не отображается, если одной из сторон взаимодействия является общий узел неизвестных устройств.

Изменение масштаба карты сетевых взаимодействий

Карта сетевых взаимодействий может отображаться в масштабе 1–100%. Текущее значение масштаба отображается в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий.

Чтобы изменить масштаб карты сетевых взаимодействий,

используйте колесико мыши или кнопки **+** и **-**, расположенные в панели инструментов рядом с текущим значением масштаба.

При уменьшении масштаба карты сетевых взаимодействий сокращается объем выводимой информации в узлах и свернутых группах.

В масштабе отображения менее 25% в узлах и свернутых группах не отображаются значки и текстовая информация. Узлы и свернутые группы видоизменяются следующим образом:

- На узле, представляющем известное программе устройство, в правом верхнем углу отображается статус устройства в виде треугольника одного из следующих цветов:
  - зеленый цвет – устройство имеет статус *Разрешенное*;
  - красный цвет – устройство имеет статус *Неразрешенное*;
  - серый цвет – устройство имеет статус *Неиспользуемое*.
- На узле WAN появляется утолщенная линия черного цвета на левой границе узла.
- На свернутой группе в правом верхнем углу отображается треугольник, который обозначает признак наличия объектов, требующих внимания. Треугольник закрашен одним из следующих цветов:
  - зеленый цвет – группа не содержит объектов, требующих внимания;
  - красный цвет – группа содержит объекты, требующие внимания.

Позиционирование карты сетевых взаимодействий

При необходимости вы можете изменить позиционирование карты сетевых взаимодействий вручную или автоматически. Автоматическое позиционирование позволяет переместить карту сетевых взаимодействий и изменить ее масштаб таким образом, чтобы на экране отображались все узлы, удовлетворяющие заданным параметрам фильтрации, а также все развернутые группы.

Чтобы позиционировать карту сетевых взаимодействий вручную:

1. Наведите курсор мыши на любое место карты сетевых взаимодействий, не занятое объектами.
2. Удерживая нажатой левую кнопку мыши, перетащите изображение карты сетевых взаимодействий.

Чтобы автоматически позиционировать карту сетевых взаимодействий,

нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий.

Позиционирование и масштаб карты сетевых взаимодействий изменятся для отображения всех узлов и развернутых групп.

Закрепление и открепление узлов и групп

По умолчанию узлы и свернутые группы не закреплены на карте сетевых взаимодействий. Незакрепленные узлы и свернутые группы могут автоматически перемещаться для оптимального отображения остальных объектов.

Закрепление узлов и групп происходит при изменении их местоположения вручную или при автоматическом распределении. Также вы можете закрепить текущее местоположение отображаемых объектов, не перемещая их.

Для закрепления и открепления объектов без их перемещения вы можете использовать следующие элементы интерфейса:

- Кнопки в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий. С помощью кнопок и вы можете закрепить и открепить все узлы и группы, отображаемые на карте сетевых взаимодействий (в том числе узлы в развернутых группах).

- Кнопки в заголовке окна развернутой группы. С помощью кнопок и вы можете закрепить и открепить только узлы и группы в окне развернутой группы (но не в окнах вложенных групп).

Кнопки доступны, если на карте сетевых взаимодействий есть объекты, к которым можно применить соответствующие действия.

После того, как местоположение узла или свернутой группы закреплено, в правом верхнем углу этого элемента отображается значок (если для карты сетевых взаимодействий задан масштаб не менее 25%). Вы также можете использовать этот значок для открепления объекта.

Местоположение закрепленного узла или закрепленной группы сохраняется. Если закрепленный узел перестал отображаться на карте сетевых взаимодействий (например, после применения фильтрации), при следующем появлении этот узел отобразится на том же месте.

Изменение местоположения узлов и групп вручную

Вы можете вручную изменять местоположение узлов и групп на карте сетевых взаимодействий, распределяя их наиболее удобным для вас способом.

После перемещения узлы и группы закрепляются на новом местоположении. При необходимости вы можете открепять эти объекты.

Объекты, включенные в группы, можно перемещать только в пределах окон этих групп.

Чтобы изменить местоположение узлов и/или свернутых групп:

1. На карте сетевых взаимодействий выберите один или несколько объектов, представляющих узлы и/или свернутые группы.

   Для выбора нескольких узлов и/или свернутых групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.

   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

2. С помощью мыши перетащите выбранные объекты в нужное место.

   После перемещения узлы и свернутые группы останутся закрепленными. В этих объектах появится значок .

Чтобы изменить местоположение развернутой группы,

наведите курсор на заголовок окна развернутой группы, нажмите на левую кнопку мыши и перетащите окно в нужное место.

Автоматическое распределение узлов и групп

Для оптимального размещения объектов на карте сетевых взаимодействий вы можете использовать алгоритмы автоматического изменения местоположения (распределения) узлов и групп. Предусмотрены следующие алгоритмы:

- распределение по радиальному принципу;
- распределение с выравниванием по сетке.

Вы можете использовать алгоритмы автоматического распределения для следующих объектов:

- Все отображаемые узлы и группы, относящиеся к верхнему уровню иерархии в дереве групп. Автоматическое распределение выполняется с помощью кнопок (для распределения по радиальному принципу) и (для распределения с выравниванием по сетке) в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий.
- Все отображаемые узлы и группы внутри развернутой группы. Автоматическое распределение выполняется с помощью кнопок (для распределения по радиальному принципу) и (для распределения с выравниванием по сетке) в заголовке окна развернутой группы.
- Только выбранные узлы и свернутые группы. Перед автоматическим распределением вам нужно выбрать не менее трех узлов и/или свернутых групп внутри развернутой группы или на верхнем уровне иерархии. Для выбора нескольких объектов вы можете выделить мышью прямоугольную область с нужными объектами, удерживая нажатой клавишу **SHIFT**, или выбрать нужные объекты с помощью мыши, удерживая нажатой клавишу **CTRL**. Автоматическое распределение выполняется с помощью кнопок (для распределения по радиальному принципу) и (для распределения с выравниванием по сетке) в панели инструментов, которая расположена в левой части области отображения карты сетевых взаимодействий.

После автоматического распределения узлы и группы закрепляются на новом месте. В этих объектах появляется значок . При необходимости вы можете открепить эти объекты.

Поиск узлов на карте сетевых взаимодействий

Вы можете выполнять поиск узлов на карте сетевых взаимодействий по сведениям об этих узлах. В поиске участвуют все узлы, удовлетворяющие текущим параметрам фильтрации, в том числе находящиеся в свернутых группах или за пределами отображаемой части карты сетевых взаимодействий.

Для узлов, представляющих известные программе устройства, поиск выполняется по всем столбцам таблицы устройств, кроме столбцов **Статус**, **Состояние безопасности**, **Последнее появление**, **Последнее изменение** и **Создано**. Поиск также выполняется по значениям пользовательских полей для устройств.

Чтобы найти нужные узлы на карте сетевых взаимодействий,

в разделе **Карта сети** введите поисковый запрос в поле **Поиск узлов**. Поиск инициируется по мере ввода символов в строку поиска.

Если найдены узлы, удовлетворяющие поисковому запросу, контуры этих узлов подсвечиваются желтым цветом. Аналогично подсвечиваются контуры свернутых групп, в которых найдены узлы. При этом в правой части поля **Поиск узлов** появляются следующие элементы:

- Порядковый номер текущего выбранного объекта (узла или свернутой группы с найденными узлами) среди результатов поиска.
- Общее количество найденных объектов (узлов и/или свернутых групп с найденными узлами).

  В общем количестве найденных объектов не учитывается количество узлов в свернутых группах. Если вы хотите, чтобы узлы в группах также учитывались в результатах поиска, разверните свернутые группы.

- Стрелки для переходов между найденными объектами. Переходы выполняются в алфавитном порядке имен найденных объектов. При переходе к очередному объекту карта сетевых взаимодействий автоматически позиционируется для отображения этого объекта.

Фильтрация объектов на карте сетевых взаимодействий

Этот раздел содержит инструкции по фильтрации объектов на карте сетевых взаимодействий для ограничения количества отображаемых узлов и соединений.

Комплексная фильтрация узлов и соединений

Этот раздел содержит инструкции по комплексной фильтрации узлов и соединений.

Фильтрация с помощью периода на временной шкале

Для фильтрации узлов и соединений вы можете выбрать нужный период времени на временной шкале. Временная шкала отображается в нижней части вкладки **Карта сетевых взаимодействий** раздела **Карта сети**.

Временная шкала содержит следующие элементы:

- Дата и время начала временной шкалы.
- Периоды, когда были зарегистрированы события со значениями оценок 4.0 и выше. Эти периоды отображаются в виде полос красного цвета в нижней части шкалы. Периоды не отображаются, если для временной шкалы задана длительность более семи суток.
- Период для фильтрации. Этот период отображается в виде желтой полосы, по краям которой находятся кнопки для перемещения границ.

- График объема трафика, обработанного программой. График не отображается, если для временной шкалы задана длительность более семи суток.

- Окончание временной шкалы. В зависимости от размещения периода для фильтрации, окончание временной шкалы отображается в виде даты и времени (если заданы дата и время) или в виде ссылки **Сейчас**.

Предусмотрены следующие типы периодов для фильтрации:

- Период с привязкой к текущему моменту. Правая граница такого периода совпадает с границей временной шкалы, обозначающей текущий момент.

- Период без привязки к текущему моменту. Период этого типа может быть размещен в любой части временной шкалы.

Чтобы настроить фильтрацию объектов по периоду с привязкой к текущему моменту:

1. Нажмите на кнопку **Сейчас** справа от временной шкалы. Кнопка не отображается, если период уже привязан к текущему моменту.

2. Если требуется указать другую длительность периода, выполните одно из следующих действий:

   - Переместите левую границу желтой полосы периода в нужное положение (максимальная длительность периода – 7 дней).

   - Откройте окно настройки с помощью кнопки над желтой полосой периода, установите флажок **Прикреплять к границе**, выберите нужную длительность (**Час**, **День**, **7 дней**) и нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те узлы и соединения, для которых были обнаружены взаимодействия от начала заданного периода и до текущего момента.

Чтобы настроить фильтрацию по периоду без привязки к текущему моменту:

1. Если нужный период не входит в пределы временной шкалы, измените значения даты и времени начала и/или окончания временной шкалы:

   a. Для изменения даты и времени начала временной шкалы откройте окно по ссылке в левой части шкалы и выберите один из следующих вариантов:

      - **День**.
      - **7 дней**.
      - **30 дней**.
      - **Задать дату**. Для этого варианта укажите дату и время в открывшемся поле.

   b. Для изменения даты и времени окончания временной шкалы откройте окно по ссылке в правой части шкалы и выберите один из следующих вариантов:

      - **Сейчас**.
      - **Задать дату**. Для этого варианта укажите дату и время в открывшемся поле.

2. Задайте нужный период. Для этого выполните одно из следующих действий:

   - Переместите период в нужную часть временной шкалы с помощью мыши.
   - Переместите одну или обе границы желтой полосы периода в нужную часть временной шкалы (максимальная длительность периода – 7 дней).
   - Откройте окно настройки с помощью кнопки над желтой полосой периода, выберите нужную длительность (**Час**, **День**, **7 дней**) и нажмите на кнопку **ОК**.

3. Если для периода автоматически устанавливается привязка к текущему моменту (при перемещении периода в крайнее правое положение перестает отображаться кнопка **Сейчас** справа от временной шкалы), выключите режим автоматического прикрепления периода к границе шкалы. Для этого откройте окно настройки с помощью кнопки над желтой полосой периода, снимите флажок **Прикреплять к границе** и нажмите на кнопку **ОК**.

Фильтрация по зарегистрированным событиям

Вы можете отобразить на карте сетевых взаимодействий узлы и соединения, информация о которых сохранена в событиях, связанных с выбранными узлами.

Возможность фильтрации по событиям доступна, если выбрано не более 200 узлов на карте сетевых взаимодействий. Вы можете выбирать нужные узлы как по отдельности, так и в составе свернутых групп, включающих нужные устройства. При выборе свернутой группы в выборку устройств также попадают все устройства в дочерних группах любого уровня вложенности.

Фильтрацию по событиям можно выполнить следующими способами:

- Начальная фильтрация по событиям. Этот способ применяется, если требуется отфильтровать объекты по событиям, связанным только с выбранными узлами.

- Дополнительная фильтрация по событиям. Этот способ применяется, если уже выполнена начальная фильтрация по событиям (например, при переходе на карту сетевых взаимодействий из таблицы событий) и требуется добавить к фильтру события, связанные с дополнительно выбранными узлами из числа отображаемых на карте сетевых взаимодействий.

Чтобы отобразить узлы и соединения с использованием начальной фильтрации по событиям:

1. На карте сетевых взаимодействий выберите один или несколько объектов, представляющих узлы и/или свернутые группы.

   Для выбора нескольких узлов и/или групп выполните одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.

   - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

2. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Фильтр по событиям**.

3. В раскрывающемся списке выберите пункт **Отфильтровать**.

   На карте сетевых взаимодействий отобразятся только те узлы и соединения, информация о которых содержится в событиях, связанных с выбранными узлами. В панели инструментов, которая расположена над картой сетевых взаимодействий, появится список с идентификаторами событий (идентификаторы перечислены в порядке обнаружения связанных событий).

Чтобы добавить к отображаемым объектам узлы и соединения с использованием дополнительной фильтрации по событиям:

1. Убедитесь, что выполнена начальная фильтрация по событиям. Для этого проверьте наличие списка с идентификаторами событий в панели инструментов, которая расположена над картой сетевых взаимодействий.

2. Среди отображаемых узлов на карте сетевых взаимодействий выберите те узлы, для которых вы хотите добавить связанные события к фильтру.

   В правой части окна веб-интерфейса появится область деталей.

3. В панели инструментов. которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Фильтр по событиям**.

4. В раскрывающемся списке выберите пункт **Добавить к фильтру**.

   На карте сетевых взаимодействий дополнительно отобразятся те узлы и соединения, информация о которых содержится в событиях, связанных с выбранными узлами. Идентификаторы обнаруженных событий добавятся в список с идентификаторами в панели инструментов.

Фильтрация узлов

Этот раздел содержит инструкции по фильтрации узлов.

Фильтрация узлов по статусам устройств

Чтобы отфильтровать узлы по статусам устройств:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Статусы устройств**.

   Появится список, содержащий названия статусов для известных программе устройств (*Неразрешенное*, *Разрешенное*, *Неиспользуемое*), а также статус *Неизвестное устройство* для неизвестных программе устройств.

2. В раскрывающемся списке установите флажки для тех статусов, устройства с которыми нужно отобразить на карте сетевых взаимодействий.

3. Нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те узлы, которые представляют устройства с выбранными статусами.

Фильтрация узлов по состояниям безопасности устройств

Чтобы отфильтровать узлы по состояниям безопасности устройств:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Состояния устройств**.

   Появится список, содержащий названия состояний безопасности для устройств (*OK*, *Важное*, *Критическое*).

2. В раскрывающемся списке установите флажки для тех состояний безопасности, узлы с которыми нужно отобразить на карте сетевых взаимодействий.

3. Нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те узлы, которые представляют устройства с выбранными состояниями безопасности.

Фильтрация узлов по категориям устройств

Чтобы отфильтровать узлы по категориям устройств:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Категории устройств**.

   Появится список, содержащий названия категорий для известных программе устройств, а также отдельные категории для неизвестных устройств и узлов WAN.

2. В раскрывающемся списке установите флажки для тех категорий, устройства с которыми нужно отобразить на карте сетевых взаимодействий.

3. Нажмите на кнопку **OK**.

На карте сетевых взаимодействий отобразятся только те узлы, которые представляют устройства выбранных категорий.

Включение и выключение отображения узлов, связанных с отфильтрованными узлами

После фильтрации узлов на карте сетевых взаимодействий отображаются только те узлы, которые удовлетворяют заданным параметрам фильтрации. При этом для отображения узла на карте сетевых взаимодействий требуется, чтобы этот узел имел соединение с другим отображаемым узлом. Если по заданным параметрам фильтрации на карте сетевых взаимодействий не отображаются все узлы, с которыми были обнаружены взаимодействия узла, этот узел также не отображается на карте сетевых взаимодействий. Для узлов, входящих в общий узел неизвестных устройств, фильтрация применяется аналогично: если не отображаются все узлы, с которыми были обнаружены взаимодействия узла неизвестного устройства, этот узел исключается из списка узлов общего узла неизвестных устройств.

При необходимости вы можете включить отображение на карте сетевых взаимодействий всех узлов, связанных с отфильтрованными узлами. Вместе с узлами, удовлетворяющими заданным параметрам фильтрации узлов, на карте сетевых взаимодействий будут отображаться все узлы, с которыми были взаимодействия (независимо от заданных параметров фильтрации).

Например, если включена фильтрация узлов по категории **ПЛК** и вы включили отображение связанных узлов, на карте сетевых взаимодействий отобразятся все узлы, с которыми взаимодействовали устройства категории **ПЛК**. Если отображение связанных узлов выключено, на карте сетевых взаимодействий отображаются узлы только тех устройств категории **ПЛК**, которые взаимодействовали между собой.

Чтобы включить или выключить отображение узлов, связанных с отфильтрованными узлами,

используйте переключатель **Связанные устройства** в панели инструментов, которая расположена над картой сетевых взаимодействий.

Фильтрация соединений

Этот раздел содержит инструкции по фильтрации соединений.

Фильтрация соединений по значениям оценок критичности соединений

Чтобы отфильтровать соединения на карте сетевых взаимодействий по значениям оценок критичности соединений:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Оценки соединений**.

   Появится список, содержащий названия уровней критичности событий с диапазонами их значений (Низкий (0.0 - 3.9), Средний (4.0 - 7.9), Высокий (8.0 - 10.0)), а также элемент **Без событий**, позволяющий выполнить фильтрацию соединений, для которых не зарегистрированы события.

2. В раскрывающемся списке установите флажки для тех уровней критичности, по которым вы хотите выполнить фильтрацию.

3. Нажмите на кнопку **ОК**.

На карте сетевых взаимодействий отобразятся только те соединения, с которыми связаны события с выбранными уровнями критичности.

Фильтрация соединений по протоколам взаимодействий

Чтобы отфильтровать соединения на карте сетевых взаимодействий по протоколам взаимодействий:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Протоколы**.

   Откроется окно с таблицей поддерживаемых протоколов, отображаемых в виде дерева стека протоколов. Вы можете управлять отображением элементов дерева с помощью кнопок **+** и **-** рядом с названиями протоколов, которые содержат протоколы следующих уровней.

   В столбцах таблицы представлена следующая информация:

   - **Протокол** – название протокола в дереве стека протоколов.
   - **EtherType** – номер протокола следующего уровня внутри протокола Ethernet (если протокол имеет заданный номер). Отображается в десятичном формате.
   - **IP-номер** – номер протокола следующего уровня внутри протокола IP (если протокол имеет заданный номер). Указывается только для протоколов, входящих в структуру протокола IP. Отображается в десятичном формате.

2. При необходимости воспользуйтесь поисковой строкой над таблицей, чтобы найти нужные протоколы.

3. В списке протоколов установите флажки напротив протоколов, по которым вы хотите выполнить фильтрацию.

   Если вы устанавливаете или снимаете флажок для протокола, который содержит вложенные протоколы, то для всех вложенных протоколов также автоматически устанавливаются или снимаются флажки.

4. Нажмите на кнопку **OK**.

   На карте сетевых взаимодействий отобразятся только те соединения, в которых использовались выбранные протоколы.

Фильтрация соединений по уровням модели OSI

Вы можете отфильтровать соединения по уровням взаимодействий, соответствующих уровням сетевой модели стека сетевых протоколов OSI (Open Systems Interconnection).

Чтобы отфильтровать соединения на карте сетевых взаимодействий по уровням сетевой модели OSI:

1. В панели инструментов, которая расположена над картой сетевых взаимодействий, откройте раскрывающийся список **Уровни модели OSI**.

   Появится список, содержащий названия уровней модели OSI:

   - **Канальный**. К этому уровню относятся соединения, в которых для связи с устройствами использовались MAC-адреса.
   - **Сетевой**. К этому уровню относятся соединения, в которых для связи с устройствами использовались IP-адреса.

2. В раскрывающемся списке установите флажки для тех уровней модели OSI, для которых нужно отобразить соединения на карте сетевых взаимодействий.

3. Нажмите на кнопку **OK**.

   На карте сетевых взаимодействий отобразятся только те соединения, которые относятся к выбранному уровню модели OSI.

Сброс параметров фильтрации

Вы можете сбросить заданные параметры фильтрации узлов и соединений в состояние по умолчанию.

Чтобы сбросить заданные параметры фильтрации на карте сетевых взаимодействий,

в панели инструментов, которая расположена над картой сетевых взаимодействий, нажмите на кнопку **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации).

На карте сетевых взаимодействий отобразятся все узлы и соединения, для которых были обнаружены взаимодействия в течение времени заданного периода.

Сохранение и загрузка параметров отображения карты сетевых взаимодействий

Этот раздел содержит информацию о функциях для работы с параметрами отображения карты сетевых взаимодействий.

Программа позволяет сохранить текущие параметры отображения карты сетевых взаимодействий. Набор сохраняемых параметров отображения называется *видом*. Вы можете использовать виды для применения сохраненных в них параметров на карте сетевых взаимодействий (например, чтобы быстро восстановить параметры отображения после каких-либо изменений или для работы с картой сетевых взаимодействий на другом компьютере).

При сохранении вида карты сетевых взаимодействий сохраняются следующие параметры отображения:

- масштаб;
- позиционирование карты сетевых взаимодействий;

- местоположение закрепленных узлов и групп;
- фильтрация узлов и соединений.

В программе можно сохранить и использовать не более 10 наборов параметров, представляющих различные виды карты сетевых взаимодействий.

Управлять списком видов карты сетевых взаимодействий (в том числе сохранять текущие параметры отображения) могут только пользователи с ролью Администратор. При этом просматривать список видов и применять сохраненные наборы параметров могут как пользователи с ролью Администратор, так и пользователи с ролью Оператор.

Добавление нового вида с сохранением текущих параметров отображения карты сетевых взаимодействий

Чтобы добавить новый вид с сохранением текущих параметров отображения карты сетевых взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** настройте параметры отображения карты сетевых взаимодействий.
3. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.
4. Нажмите на кнопку **Добавить**.
5. В поле ввода введите имя вида.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя вида должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 100 символов;
   - не совпадает с именем другого вида (регистр символов не учитывается).
6. Нажмите на значок ✓ справа от поля ввода.

Обновление вида с сохранением текущих параметров отображения карты сетевых взаимодействий

Чтобы обновить вид с сохранением текущих параметров отображения карты сетевых взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** настройте параметры отображения карты сетевых взаимодействий.

3. Откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.

4. Выберите вид, в котором вы хотите сохранить текущие параметры отображения карты сетевых взаимодействий.

5. Нажмите на кнопку **Перезаписать**.

   Откроется окно с запросом подтверждения.

6. В окне запроса подтвердите сохранение текущих параметров в выбранном виде.

Переименование вида карты сетевых взаимодействий

Чтобы переименовать вид карты сетевых взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.

3. Выберите вид, который вы хотите переименовать.

4. Нажмите на значок справа от текущего имени вида.

5. В поле ввода введите новое имя вида.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Имя вида должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 100 символов;
   - не совпадает с именем другого вида (регистр символов не учитывается).

6. Нажмите на значок справа от поля ввода.

Удаление вида карты сетевых взаимодействий

Чтобы удалить вид карты сетевых взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.

3. Выберите вид, который вы хотите удалить.

4. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.

5. В окне запроса подтвердите удаление выбранного вида.

Применение на карте сетевых взаимодействий параметров, сохраненных в виде

Чтобы применить параметры, сохраненные в виде, на карте сетевых взаимодействий:

1. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** откройте окно **Настройка видов карты сети** по кнопке **Настроить виды**.

2. Выберите нужный вид в списке.

3. Нажмите на кнопку **Применить**.

   Откроется окно с запросом подтверждения.

4. В окне запроса подтвердите применение вида.

Загрузка трафика при работе с картой сетевых взаимодействий

При работе с картой сетевых взаимодействий вы можете загружать трафик, поступивший в программу через точки мониторинга. Загрузка трафика выполняется в файл формата PCAP. Для загрузки нужных данных вы можете настраивать фильтрацию сетевых пакетов.

Программа загружает трафик из хранилищ с файлами дампа трафика. Для загрузки может использоваться как внутреннее хранилище каждого узла (созданное автоматически при установке компонента программы на узле), так и внешнее хранилище, если оно подключено на узле.

При загрузке трафика вам нужно учитывать следующие особенности:

- Файлы дампа трафика хранятся в хранилищах временно и автоматически удаляются по мере поступления нового трафика (периодичность удаления файлов зависит от интенсивности поступающего трафика и от заданных параметров хранения данных программы). Загрузка трафика невозможна, если соответствующие ему файлы дампа трафика уже удалены из хранилищ.

- Загружать трафик при работе с картой сетевых взаимодействий могут только пользователи с ролью Администратор.

Чтобы загрузить трафик при работе с картой сетевых взаимодействий:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Карта сети** на вкладке **Карта сетевых взаимодействий** нажмите на кнопку **Скачать трафик**.

   В правой части окна веб-интерфейса появится область деталей.

3. Выполните следующие действия:

   - Если вы хотите загрузить трафик за определенный период времени, задайте нужные границы с помощью параметра **Период трафика для скачивания**.

     По умолчанию задан период, равный настроенному периоду для фильтрации на временной шкале.

   - Задайте ограничение максимального объема для загрузки трафика в блоке **Ограничение объема скачивания**.

     Если объем загружаемого трафика превысит заданное ограничение, будет отброшен более поздний трафик.

   - При необходимости включите фильтрацию в блоке **Фильтрация по точкам мониторинга** и укажите точки мониторинга, на которые поступал нужный трафик.

     По умолчанию заданы все точки мониторинга, имеющиеся на узлах с установленными компонентами программы.

   - При необходимости включите фильтрацию в блоке **Фильтрация по адресным пространствам** и укажите адресные пространства, к которым относятся адреса в сетевых пакетах (блок отображается, если в программу добавлены дополнительные адресные пространства).

     По умолчанию заданы все адресные пространства, созданные в программе.

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием BPF** и введите выражение для фильтрации с использованием технологии BPF (Berkley Packet Filter) по адресным параметрам в сетевых пакетах.

     Пример выражения для фильтрации:
     `tcp port 102 or tcp port 502`

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием регулярных выражений** и введите выражение для фильтрации по данным, составляющим полезную нагрузку в сетевых пакетах.

     Пример выражения для фильтрации:
     `^test.+xABxCD`

4. Нажмите на кнопку **Скачать**.

5. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции формирования файла.

   c. Нажмите на кнопку **Скачать файл**.

Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Мониторинг сетевых сеансов

Kaspersky Industrial CyberSecurity for Networks может обнаруживать в трафике промышленной сети сетевые сеансы, создаваемые устройствами для соединений с другими устройствами. Программа регистрирует обнаруженные сетевые сеансы и сохраняет сведения, с помощью которых вы можете анализировать сетевую активность устройств и загружать данные о переданных сетевых пакетах из файлов дампа трафика. В отличие от соединений на карте сетевых взаимодействий, зарегистрированные сетевые сеансы позволяют получить более подробные сведения о взаимодействиях устройств, в том числе за счет раздельной регистрации сеансов для разных портов и протоколов, которые использовались при взаимодействиях.

Программа обнаруживает сетевые сеансы, если включено применение метода Обнаружение сетевых сессий по технологии Контроль активов. Обнаружение сетевых сеансов может выполняться при анализе трафика, поступающего на точки мониторинга, а также при получении данных от EPP-приложений.

Каждый зарегистрированный сетевой сеанс содержит сведения о соединении между двумя устройствами, которые являются сторонами взаимодействия. Сетевой сеанс характеризуется адресной информацией сторон взаимодействия (MAC- и/или IP-адреса), номерами портов и прикладным протоколом, который использовался для соединения. Первым устройством в сетевом сеансе обычно считается устройство, которое инициировало отправку сетевых пакетов на другое устройство.

Сетевой сеанс считается завершенным, если в рамках этого сеанса не отправлялись сетевые пакеты в течение одной минуты или если технология обнаружения сетевых сессий была выключена на соответствующем узле или точке мониторинга.

При обнаружении чрезмерно большого количества сетевых сеансов в программе применяются следующие ограничения для регистрации сеансов:

- количество регистрируемых сеансов между двумя сторонами взаимодействия с использованием одного и того же прикладного протокола – не более 1000 за одну минуту;
- общее количество регистрируемых сеансов между двумя сторонами взаимодействия – не более 5000 за одну минуту.

Программа сохраняет данные о сетевых сеансах в базе данных на Сервере. Суммарный объем сохраняемых записей не может превышать заданного ограничения. Если объем превышает заданное ограничение, программа автоматически удаляет 10% самых старых записей. Вы можете задать ограничение максимального объема для сетевых сеансов при настройке параметров хранения данных на узле Сервера в блоке параметров **Сетевые сессии**.

Вы можете просматривать сведения о сетевых сеансах в разделе **Карта сети** на вкладке **Сетевые сессии**.

Таблица сетевых сеансов

Таблица сетевых сеансов отображается в разделе **Карта сети** на вкладке **Сетевые сессии**.

Таблица сетевых сеансов содержит следующие сведения:

- **Статус** – статус сетевого сеанса. Зарегистрированный сетевой сеанс может иметь один из следующих статусов:
  - **Активна**. Этот статус присваивается при регистрации сетевого сеанса и сохраняется до тех пор, пока в рамках этого сеанса устройства отправляют сетевые пакеты.
  - **Завершена**. Этот статус присваивается сетевому сеансу, если в рамках этого сеанса не отправлялись сетевые пакеты в течение одной минуты или если технология обнаружения сетевых сессий была выключена на соответствующем узле или точке мониторинга.
- **Сторона 1** – MAC- и/или IP-адреса одной из сторон сетевого взаимодействия. Отображение MAC- и IP-адресов можно включать и выключать.
- **Порт стороны 1** – номер порта первой стороны взаимодействия.
- **Сторона 2** – MAC- и/или IP-адреса другой стороны сетевого взаимодействия. Отображение MAC- и IP-адресов можно включать и выключать.
- **Порт стороны 2** – номер порта второй стороны взаимодействия.
- **Устройство 1** – имя известного программе устройства, которому соответствует адресная информация первой стороны взаимодействия.
- **Устройство 2** – имя известного программе устройства, которому соответствует адресная информация второй стороны взаимодействия.
- **Протокол передачи** – название транспортного протокола, который использовался в сетевом сеансе.
- **Протокол приложений** – название протокола прикладного уровня, который использовался в сетевом сеансе.
- **Текущая скорость** – текущая скорость передачи данных в сетевом сеансе.
- **Средняя скорость** – средняя скорость передачи данных в сетевом сеансе.
- **Всего передано** – количество байт, переданных в сетевом сеансе.
- **Точки мониторинга** – имена точек мониторинга, на которые поступил трафик сетевого сеанса.
- **Начало** – дата и время первого сетевого пакета в сетевом сеансе или дата и время начала временного интервала, данные о котором поступили от EPP-приложения.
- **Последнее взаимодействие** – дата и время последнего сетевого пакета в сетевом сеансе или дата и время завершения временного интервала, данные о котором поступили от EPP-приложения (если в сетевом сеансе был получен только один пакет, то значение совпадает со значением параметра **Начало**).
- **Количество пакетов** – количество сетевых пакетов, переданных в сетевом сеансе.

При просмотре таблицы сетевых сеансов вы можете использовать функции настройки, фильтрации и сортировки, а также переходить к связанным элементам и экспортировать данные.

Просмотр сведений о сетевом сеансе

Подробные сведения о сетевом сеансе включают информацию из таблицы сетевых сеансов, а также название приложения, во время работы которого был инициирован сетевой сеанс (если программе удалось определить название приложения).

Чтобы просмотреть сведения о сетевом сеансе,

в разделе **Карта сети** на вкладке **Сетевые сессии** выберите нужный сетевой сеанс.

В правой части окна веб-интерфейса появится область деталей. В области деталей отображаются все полученные сведения о сетевом сеансе.

Загрузка трафика сетевых сеансов

При просмотре таблицы сетевых сеансов вы можете загружать трафик, относящийся к выбранным сетевым сеансам. Загрузка трафика выполняется в файл формата PCAP. Для загрузки нужных данных вы можете настраивать фильтрацию сетевых пакетов.

Программа загружает трафик сетевых сеансов из хранилищ с файлами дампа трафика. Для загрузки может использоваться как внутреннее хранилище узла (созданное автоматически при установке компонента программы на узле), так и внешнее хранилище, если оно подключено на узле.

При загрузке трафика сетевых сеансов вам нужно учитывать следующие особенности:

- Загрузка трафика возможна только для тех сетевых сеансов, которые были зарегистрированы при анализе трафика, поступившего на точки мониторинга. Если сетевой сеанс был зарегистрирован по данным, полученным от EPP-приложения, в программе невозможно загрузить трафик этого сеанса.
- Файлы дампа трафика хранятся в хранилищах временно и автоматически удаляются по мере поступления нового трафика (периодичность удаления файлов зависит от интенсивности поступающего трафика и от заданных параметров хранения данных программы). Загрузка трафика сетевого сеанса невозможна, если соответствующие ему файлы дампа трафика уже удалены из хранилищ.
- Загружать трафик сетевых сеансов могут только пользователи с ролью Администратор.

Чтобы загрузить трафик сетевых сеансов:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** на вкладке **Сетевые сессии** выберите сетевые сеансы, трафик которых вы хотите загрузить.

   Вы можете выбрать не более 100 сетевых сеансов.
3. Нажмите на кнопку **Скачать трафик**.

   В правой части окна веб-интерфейса появится область деталей.

4. Выполните следующие действия:

   - Если вы хотите загрузить трафик за определенный период времени, задайте нужные границы с помощью параметра **Период трафика для скачивания**.

     По умолчанию задан максимально возможный период, начиная от даты и времени начала самого раннего сетевого сеанса и заканчивая датой и временем завершения самого позднего сеанса из числа выбранных сеансов. При необходимости вы можете задать границы внутри этого периода или задать пустое значение для одной из границ (например, для правой границы, чтобы загрузить новый трафик еще не завершенных сеансов).

   - Задайте ограничение максимального объема для загрузки трафика в блоке **Ограничение объема скачивания**.

     Если объем загружаемого трафика превысит заданное ограничение, будет отброшен более поздний трафик.

   - При необходимости включите фильтрацию в блоке **Фильтрация по точкам мониторинга** и укажите точки мониторинга, на которые поступал нужный трафик.

     По умолчанию заданы те точки мониторинга, на которые поступал трафик выбранных сетевых сеансов.

   - При необходимости включите фильтрацию в блоке **Фильтрация по адресным пространствам** и укажите адресные пространства, к которым относятся адреса в сетевых пакетах выбранных сетевых сеансов (блок отображается, если в программу добавлены дополнительные адресные пространства).

     По умолчанию заданы все адресные пространства, созданные в программе.

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием BPF** и введите выражение для фильтрации с использованием технологии BPF (Berkley Packet Filter) по адресным параметрам в сетевых пакетах выбранных сетевых сеансов.

     Пример выражения для фильтрации:
     `tcp port 102 or tcp port 502`

   - При необходимости включите фильтрацию в блоке **Фильтрация с использованием регулярных выражений** и введите выражение для фильтрации по данным, составляющим полезную нагрузку в сетевых пакетах выбранных сетевых сеансов.

     Пример выражения для фильтрации:
     `^test.+xABxCD`

5. Нажмите на кнопку **Скачать**.

6. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции формирования файла.

   c. Нажмите на кнопку **Скачать файл**.

Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Мониторинг событий и инцидентов

При анализе трафика промышленной сети программа регистрирует события и инциденты.

Событие в Kaspersky Industrial CyberSecurity for Networks – это запись, содержащая информацию об обнаружении в трафике промышленной сети определенных изменений или условий, которые требуют внимания специалиста по безопасности АСУ ТП. События регистрируются и передаются на Сервер Kaspersky Industrial CyberSecurity for Networks. Сервер обрабатывает полученные события и сохраняет их в базе данных.

Инцидент – это событие особого типа, которое регистрируется при получении определенной последовательности событий. Инциденты группируют события, имеющие некоторые общие признаки или относящиеся к одному процессу.

Программа регистрирует инциденты по правилам корреляции событий. *Правило корреляции событий* описывает условия для проверки последовательностей событий. При обнаружении последовательности событий, удовлетворяющих условиям правила, программа регистрирует инцидент, в котором указано название сработавшего правила. Для регистрации инцидентов используется системный тип события, которому присвоен код 8000000001.

Правила корреляции событий встроены в программу и применяются независимо от политики безопасности.

После установки программы используются исходные правила корреляции событий. Для повышения эффективности работы правил специалисты "Лаборатории Касперского" регулярно обновляют базы с наборами правил. Вы можете обновлять правила корреляции, устанавливая обновления.

Сервер Kaspersky Industrial CyberSecurity for Networks регистрирует события и инциденты в соответствии с параметрами, заданными для регистрации типов событий. Вы можете настроить эти параметры в разделе Типы событий (для всех типов событий) и при настройке правил контроля процесса (только для событий, регистрируемых при срабатывании правил контроля процесса).

Для сокращения количества часто повторяющихся событий, которые не требуют внимания оператора, предусмотрена возможность создания разрешающих правил на события. События, удовлетворяющие разрешающим правилам, не регистрируются. Например, с помощью разрешающего правила можно временно выключить регистрацию всех событий с определенной точки мониторинга. Вы можете просматривать разрешающие правила для событий в разделе **Разрешающие правила**. Для таких правил указан тип EVT.

Программа сохраняет события и инциденты в базе данных на Сервере. Суммарный объем сохраняемых записей не может превышать заданного ограничения. Если объем превышает заданное ограничение, программа автоматически удаляет 10% самых старых записей. При этом если включено ограничение на минимальное время хранения, при удалении записей, время хранения которых меньше заданного ограничения, в журнале сообщений программы появляется соответствующее сообщение. Вы можете настроить параметры хранения событий и инцидентов.

Файлы базы данных сохраняются на Сервере в директориях СУБД. Удаление или изменение любого файла в этих директориях может привести к нарушению работоспособности программы.

Вы можете просматривать информацию о событиях и инцидентах в следующих разделах веб-интерфейса Kaspersky Industrial CyberSecurity for Networks:

- Раздел **Мониторинг** – отображает общую информацию о последних событиях и инцидентах, зарегистрированных программой.
- Вкладка **События и инциденты** раздела **События** – отображает подробную информацию о событиях и инцидентах и предоставляет возможность загрузки информации из базы данных Сервера за любой период.

Оценки и уровни критичности событий

События и инциденты в Kaspersky Industrial CyberSecurity for Networks оцениваются по шкале от 0.0 до 10.0.

Если событие связано с устройством, программа выполняет расчет числового значения оценки с учетом имеющихся сведений об устройстве. При расчете значения оценки в этом случае программа учитывает уровень значимости устройства и риски, связанные с этим устройством.

В качестве исходного значения для расчета оценки используется *базовая оценка*, заданная для типа события в таблице типов событий или заданная при настройке правил контроля процесса (только для событий, регистрируемых при срабатывании правил контроля процесса).

Если событие не связано с устройством, значение оценки этого события равно значению базовой оценки.

Оценка определяет уровень критичности события. В зависимости от числового значения оценки событие может относиться к одному из следующих уровней критичности:

- *Низкий* (оценки 0.0–3.9).

  События низкого уровня критичности обычно не требуют немедленной реакции.

- *Средний* (оценки 4.0–7.9).

  События среднего уровня критичности содержат сведения, на которые нужно обратить внимание. Эти события могут требовать реакции.

- *Высокий* (оценки 8.0–10.0).

  События высокого уровня критичности содержат сведения, которые могут оказать критическое влияние на технологический процесс. Эти события требуют немедленной реакции.

Для совместимости с *уровнями важности* событий, которые использовались в предыдущих версиях программы, в Kaspersky Industrial CyberSecurity for Networks текущей версии выполняется преобразование уровней важности в следующие значения оценок:

- событиям с уровнем важности *Информационные* присваивается значение оценки 3.0;
- событиям с уровнем важности *Важные* присваивается значение оценки 6.0;
- событиям с уровнем важности *Критические* присваивается значение оценки 9.0.

Технологии регистрации событий

Kaspersky Industrial CyberSecurity for Networks регистрирует события по одной из следующих технологий:

- *Контроль технологического процесса* (DPI).

  По этой технологии регистрируются события, связанные с нарушениями технологического процесса (например, событие при превышении заданного значения температуры).

- *Контроль целостности сети* (NIC).

  По этой технологии регистрируются события, связанные с целостностью промышленной сети или с безопасностью взаимодействий (например, событие при обнаружении взаимодействия устройств в промышленной сети по новому для этих устройств протоколу).

- *Обнаружение вторжений* (IDS).

  По этой технологии регистрируются события, связанные с обнаружением в трафике аномалий, которые являются признаками атак (например, событие при обнаружении признаков ARP-спуфинга).

- *Контроль системных команд* (CC).

  По этой технологии регистрируются события, связанные с обнаружением в трафике системных команд для устройств (например, событие при обнаружении неразрешенной системной команды).

- *Внешние системы* (EXT).

  К этой технологии относятся инциденты, а также события, которые поступают в Kaspersky Industrial CyberSecurity for Networks от сторонних систем с использованием методов Kaspersky Industrial CyberSecurity for Networks API.

- *Контроль активов* (AM).

  По этой технологии регистрируются события, связанные с обнаружением информации об устройствах в трафике или в полученных данных от EPP-приложений (например, событие при обнаружении нового IP-адреса у устройства).

- *Защита конечных устройств* (EPP).

  По этой технологии регистрируются события об угрозах, обнаруженных приложениями "Лаборатории Касперского", которые выполняют функции защиты рабочих станций и серверов (например, событие при обнаружении вредоносной программы).

Статусы событий

Статусы событий и инцидентов позволяют отобразить в программе последовательность обработки полученной информации специалистом по безопасности АСУ ТП.

Событиям и инцидентам могут быть присвоены следующие статусы:

- *Новое*.

  Этот статус присваивается всем событиям и инцидентам при их регистрации в Kaspersky Industrial CyberSecurity for Networks.

- *В обработке*.

  Этот статус вы можете присвоить событиям и инцидентам, которые находятся в обработке (например, во время расследования причин регистрации этих событий и инцидентов).

- *Обработано*.

  Этот статус вы можете присвоить событиям и инцидентам, которые уже обработаны (например, завершено расследование причин их регистрации).

  После присвоения статуса *Обработано* события и инциденты с этим статусом не учитываются программой при определении состояний безопасности устройств, отображаемых в таблице устройств и на карте сетевых взаимодействий.

Изменение статусов событий и инцидентов выполняется вручную. Вы можете последовательно присваивать статусы в порядке от статуса *Новое* до статуса *Обработано* (при этом можно не присваивать промежуточный статус *В обработке*). После изменения статуса события или инцидента ему невозможно присвоить предыдущий статус.

Таблица зарегистрированных событий

Вы можете просмотреть таблицу зарегистрированных событий и инцидентов в разделе **События** на вкладке **События и инциденты**.

По умолчанию таблица зарегистрированных событий и инцидентов обновляется в онлайн-режиме. В начале таблицы отображаются события и инциденты с наиболее поздними значениями даты и времени последнего появления.

Дата и время последнего появления события или инцидента может не совпадать с датой и временем его регистрации (дата и время регистрации отображается в столбце **Начало**). Для события дата и время последнего появления может обновляться в течение времени разрешения повтора для типа этого события. Для инцидента дата и время последнего появления обновляется в соответствии с датой и временем последнего появления событий, входящих в инцидент.

Параметры событий и инцидентов отображаются в следующих столбцах таблицы:

- **Начало**.

  Для события, не являющегося инцидентом – дата и время регистрации события. Для инцидента – дата и время регистрации первого события, включенного в инцидент. Вы можете просматривать в таблице дату совместно со временем, либо только дату или только время. Для выбора отображаемой информации нужно установить флажки напротив параметров **Дата** и/или **Время**.

- **Последнее появление**.

  Для события, не являющегося инцидентом – дата и время последнего появления события. Может содержать дату и время регистрации события или дату и время увеличения счетчика повторов события, если повторились условия для регистрации события в течение времени разрешения повтора. Значение счетчика повторов отображается в столбце **Всего появлений**. Для инцидента – самые поздние дата и время последнего появления событий, входящих в инцидент. Аналогично столбцу **Начало**, вы можете просматривать в таблице дату совместно со временем, либо только дату или только время.

- **Заголовок**.

  Заголовок, заданный для типа события.

- **Оценка**.

  Рассчитанное значение оценки для события. Числовое значение определяет, к какому уровню критичности относится событие. В зависимости от уровня критичности, значение оценки может быть окрашено одним из следующих цветов:

  - Красный – событие с уровнем критичности *Высокий*.
  - Желтый – событие с уровнем критичности *Средний*.
  - Синий – событие с уровнем критичности *Низкий*.

- **Отправитель**.

  Адрес отправителя сетевых пакетов. Отображение адресов и портов адресной информации можно включать и выключать с помощью следующих параметров (в скобках указаны сокращенные названия для отображения в ячейках таблицы): **IP-адрес**, **Номер порта (P)**, **MAC-адрес**, **VLAN ID (VID)**, **Адрес прикладного уровня**. Если в программу добавлены дополнительные адресные пространства, при настройке таблицы устройств можно включать и выключать отображение имен адресных пространств с помощью параметра **Отображать адресные пространства**.

- **Получатель**.

  Адрес получателя сетевых пакетов. Отображение адресной информации можно настраивать аналогично, как для столбца **Отправитель**.

- **Протокол**.

  Протокол прикладного уровня, при отслеживании которого программа зарегистрировала событие.

- **Технология**.

  Значок, соответствующий технологии, которая использовалась для регистрации события.

- **Всего появлений**.

  Для события, не являющегося инцидентом – значение счетчика повторов после регистрации события в течение времени разрешения повтора события. Значение больше 1 означает, что условия для регистрации события повторялись N – 1 раз. Для инцидента в этом столбце отображается значение 1.

- **ID**.

  Уникальный идентификатор зарегистрированного события или инцидента.

- **Приложение**.

  Сведения о приложениях, при работе которых возникли условия для регистрации события. В событии сохраняются данные о приложениях, полученные от EPP-приложений.

- **Пользователь приложения**.

  Сведения о пользователе, от имени которого выполнен запуск приложения, указанного в столбце **Приложение**.

- **Статус**.

  Значок, соответствующий статусу события или инцидента.

- **Описание**.

  Описание, заданное для типа события.

- **Завершение**.

  Для события, не являющегося инцидентом – дата и время присвоения статуса *Обработано*, либо дата и время разрешения повтора события. Для инцидента – самые поздние дата и время завершения событий, входящих в инцидент. Аналогично столбцу **Начало**, вы можете просматривать в таблице дату совместно со временем, либо только дату или только время.

- **Сработавшее правило**.

  Для события, не являющегося инцидентом – имя правила контроля процесса или правила обнаружения вторжений, при срабатывании которого зарегистрировано событие. Для инцидента – имя правила корреляции, при срабатывании которого зарегистрирован инцидент.

- **Точка мониторинга**.

  Точка мониторинга, трафик с которой вызвал регистрацию события.

- **Тип события**.

  Числовой код, присвоенный типу события.

- **Метка**.

  Набор значков, которые вы можете установить для любого события или инцидента, чтобы легко находить события и инциденты по критерию, отсутствующему в таблице.

При просмотре таблицы событий и инцидентов вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Просмотр событий, включенных в инцидент

Для просмотра событий, включенных в инциденты, в таблице событий предусмотрены следующие режимы:

- Простой режим отображения. В этом режиме в таблице событий отображаются все события без учета вложенности событий в инциденты.

- Режим отображения структур. В этом режиме инциденты отображаются в виде структур, которые могут быть свернуты и развернуты с помощью кнопок ⊞ и ⊟ рядом с заголовками инцидентов.

Вы можете изменить режим отображения при настройке таблицы событий.

Просмотр подробных данных о событии

Подробные сведения о событиях и инцидентах отображаются в области деталей в разделе **События** веб-интерфейса программы.

Чтобы просмотреть подробные данные о событии или инциденте,

в разделе **События** на вкладке **События и инциденты** выберите нужное событие или инцидент.

В правой части окна веб-интерфейса появится область деталей, в которой отобразятся подробные сведения о выбранном событии или инциденте.

Изменение статусов событий

Вы можете изменять следующие статусы событий и инцидентов:

- *Новое*. Этот статус можно изменить на статус *В обработке* или на статус *Обработано*;
- *В обработке*. Этот статус можно изменить на статус *Обработано*.

Статус *Обработано* изменить невозможно.

Если событие связано с риском, вы можете присвоить этому событию статус *Обработано* одновременно с изменением статуса риска на статус *Принят*.

Чтобы изменить статус событий или инцидентов при работе с таблицей событий:

1. Выберите вкладку **События и инциденты** в разделе **События**.
2. В таблице событий выберите события и/или инциденты, статус которых вы хотите изменить.
3. Откройте раскрывающийся список **Изменить статус** в панели инструментов.

4. В раскрывающемся списке выберите пункт для присвоения нужного статуса.

   Некоторые пункты раскрывающегося списка недоступны в следующих случаях:

   - Пункт **В обработке** недоступен, если среди выбранных элементов отсутствуют события или инциденты со статусом *Новое*.
   - Пункт **Обработано** недоступен, если среди выбранных элементов отсутствуют события или инциденты со статусами *Новое* или *В обработке*.

   Если выбраны все события и инциденты, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных элементов более 1000, программа не проверяет их статусы. В этом случае доступны оба пункта с названиями статусов **В обработке** и **Обработано**. При этом с помощью пункта **В обработке** вы можете присвоить статус *В обработке* только событиям и инцидентам со статусом *Новое*.

   Откроется окно с запросом подтверждения.

5. Если с выбранными событиями связаны риски и вы хотите одновременно присвоить статус *Принят* всем этим рискам, установите флажок **Присвоить статус Принят для всех рисков, связанных с событием** (если выбрано одно событие) или **Присвоить статус Принят для всех рисков, связанных с событиями** (если выбрано несколько событий).

   Риски могут быть связаны с событиями при регистрации событий некоторых типов по технологии Контроль активов.

6. В окне запроса нажмите на кнопку **ОК**.

Просмотр сведений об инцидентах EDR

События по технологии EPP могут содержать сведения о цепочках развития угроз, полученные от программных компонентов Endpoint Agent. Если для события построена цепочка развития угрозы, в Kaspersky Industrial CyberSecurity for Networks такое событие считается *инцидентом Endpoint Detection and Response* (далее также "инцидент EDR").

Цепочка развития угрозы представляет собой последовательность событий активности на устройстве, имеющих отношение к обнаруженной угрозе. Ключевым событием активности в цепочке развития угрозы является событие активности с объектом обнаружения угрозы. Все остальные события активности в цепочке (предшествующие и последующие по отношению к ключевому событию активности) сохраняются для дальнейшего анализа развития угрозы.

Сведения о построенной цепочке развития угрозы могут добавляться в событие не одновременно с регистрацией этого события. Максимальное время, через которое программа может добавить эти сведения в событие после его регистрации – 10 часов. Сведения не добавляются, если событию присвоен статус *Обработано*.

События, являющиеся инцидентами EDR, отмечены в таблице событий значком **EDR**. Для каждого инцидента EDR вы можете просмотреть сведения о построенной цепочке развития угрозы в области деталей. Сведения отображаются на следующих вкладках области деталей:

- **Граф событий активности** – предоставляет визуальную информацию об объектах, задействованных в цепочке развития угрозы. События активности на графе представлены в виде узлов. Узлы располагаются на разных уровнях в соответствии с выявленным процессом развития угрозы. Ключевое событие активности располагается на нижнем уровне графа. На этом уровне также могут отображаться узлы, в которых сгруппированы другие события активности по их типам. Выше этого уровня программа может отображать до четырех уровней с узлами событий активности.

- **Все события активности** – отображает в табличном виде сведения о всех событиях активности, входящих в цепочку развития угрозы и представленных в виде узлов на графе событий активности.

При просмотре сведений об инциденте EDR вы можете определить состояние возможной угрозы по статусу обработки обнаружения. Программа отображает этот статус для цепочки развития угрозы. Цвет фона для статуса зависит от результата обработки объекта обнаружения угрозы:

- если в результате обработки обнаруженная угроза считается устраненной (например, зараженный объект был вылечен EPP-приложением), программа отображает статус обработки обнаружения на зеленом фоне;

- во всех остальных случаях статус обработки обнаружения отображается на красном фоне.

Ключевое событие активности в графе событий активности окрашено тем же цветом, что и статус обработки обнаружения.

Если статус обработки обнаружения отображается на красном фоне, для предотвращения дальнейшего развития возможной угрозы вы можете, например, запустить действие по реагированию в Kaspersky Industrial CyberSecurity for Networks.

При любых обстоятельствах и независимо от отображаемого статуса обработки обнаружения вам нужно провести расследование причин и возможных последствий возникшего инцидента EDR.

Вы можете просматривать подробные сведения о событиях активности в окнах деталей, которые открываются при выборе событий активности. При просмотре сведений вы можете использовать ссылки с хешами файлов и URL-адресов для получения информации о репутации этих объектов на веб-портале Kaspersky Threat Intelligence Portal.

Если в цепочке развития угрозы присутствуют события активности, возникновение которых вы хотите обнаруживать при следующих проверках EPP-приложений, вы можете экспортировать данные об этих событиях активности в IOC-файл (файл индикаторов компрометации).

Создание разрешающих правил для событий

Если требуется выключить регистрацию событий с определенными признаками (например, все события с точки мониторинга), вы можете создавать разрешающие правила для событий. Этот раздел содержит инструкции по созданию разрешающих правил для событий.

Создавать разрешающие правила для событий могут только пользователи с ролью Администратор.

Создание разрешающего правила с изначально пустыми значениями параметров или со значениями из шаблона

Чтобы создать разрешающее правило с изначально пустыми значениями параметров или со значениями из шаблона:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Разрешающие правила** откройте область деталей по ссылке **Добавить правило**.

3. Если вы хотите задать значения параметров из шаблона, в области деталей нажмите на кнопку **Использовать шаблон**, в открывшемся окне выберите нужный шаблон и нажмите на кнопку **Применить**.

4. В области деталей нажмите на кнопку **EVT**.

5. В поле **Протокол** укажите протокол, который будет указан в событиях.

   При выборе поля **Протокол** откроется окно с таблицей поддерживаемых протоколов, отображаемых в виде дерева стека протоколов. Вы можете управлять отображением элементов дерева с помощью кнопок **+** и **-** рядом с названиями протоколов, которые содержат протоколы следующих уровней.

   При необходимости воспользуйтесь поисковой строкой над таблицей, чтобы найти нужные протоколы.

   Чтобы указать протокол, выполните следующие действия:

   a. В таблице протоколов выберите протокол, который вы хотите указать для правила. Для выбора нужного протокола нажмите на кнопку, которая отображается в левом столбце таблицы протоколов.

   b. Нажмите на кнопку **OK**.

   Если выбран протокол, который программа может определять по содержимому сетевых пакетов, ниже поля **Протокол** появится пояснение об этом.

6. При необходимости введите дополнительную информацию о правиле в поле **Комментарий**.

7. В блоках параметров **Сторона 1** и **Сторона 2** укажите доступную для изменения адресную информацию для сторон сетевого взаимодействия. В зависимости от выбранного протокола (или набора протоколов), адресная информация может содержать MAC-адрес, IP-адрес и/или номер порта. Если в программу добавлены дополнительные адресные пространства, вы можете указать имена адресных пространств для адресов.

   Для автоматического заполнения адресной информации стороны сетевого взаимодействия вы можете выбрать известные программе устройства. Для этого выполните следующие действия:

   a. Откройте окно выбора устройств по ссылке **Указать адреса устройств**.

   b. В окне выбора устройств установите флажки напротив тех устройств, которые вы хотите использовать.

      Окно выбора устройств содержит таблицу, в которой можно настраивать отображение и порядок столбцов, выполнять фильтрацию, поиск и сортировку аналогично таблице устройств в разделе **Активы**.

   c. В окне выбора устройств нажмите на кнопку **OK**.

8. В поле **Тип события** укажите тип события, числовой код которого указывается в событиях.

   При выборе поля **Тип события** откроется окно со списком типов событий, которые могут быть указаны в разрешающих правилах. При необходимости воспользуйтесь поисковой строкой над списком, чтобы найти нужный тип события. Чтобы указать тип события, выберите его в списке и нажмите на кнопку **Применить**.

9. В поле **Точка мониторинга** укажите имя точки мониторинга, которое указывается в событиях.

   При выборе поля **Точка мониторинга** откроется окно со списком всех точек мониторинга на всех узлах с установленными компонентами программы. При необходимости воспользуйтесь поисковой строкой над списком, чтобы найти имя нужной точки мониторинга. Чтобы указать имя точки мониторинга, выберите его в списке и нажмите на кнопку **Применить**.

10. В поле **Правило в событии** введите имя (или часть имени) правила, которое указывается в событиях в качестве сработавшего правила.

11. В области деталей нажмите на кнопку **Сохранить**.

    Новое правило будет добавлено в таблицу разрешающих правил.

Создание разрешающего правила на основе имеющегося правила

Чтобы создать разрешающее правило на основе имеющегося правила:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. В разделе **Разрешающие правила** выберите правило, на основе которого вы хотите создать новое правило.

3. По правой кнопке мыши откройте контекстное меню.

4. В контекстном меню выберите пункт **Копировать правило**.

   В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила. Для параметров нового правила будут заданы значения, полученные из параметров выбранного правила.

5. Измените нужные параметры. Для этого выполните пункты 4–11, описанные в процедуре создания правила с изначально пустыми значениями параметров.

Создание разрешающего правила на основе зарегистрированного события

Чтобы создать разрешающее правило на основе зарегистрированного события:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите вкладку **События и инциденты** в разделе **События**.

3. В таблице зарегистрированных событий выберите событие, на основе которого вы хотите создать разрешающее правило для событий.

   В правой части окна веб-интерфейса появится область деталей.

4. В области деталей нажмите на кнопку **Создать разрешающее правило**.

   В окне браузера откроется раздел **Разрешающие правила**. В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила. Для параметров нового правила будут заданы значения, полученные из сохраненных сведений о событии.

5. При необходимости измените параметры нового правила. Для этого выполните пункты 4–11, описанные в процедуре создания правила с изначально пустыми значениями параметров. Если изменять параметры нового правила не требуется, сохраните правило с помощью кнопки **Сохранить**.

Установка меток

Вы можете присваивать событиям и инцидентам определенные метки в разделе **События** веб-интерфейса программы.

Метка – значок, который позволяет легко находить события и инциденты по критерию, отсутствующему в таблице.

Чтобы установить метку для события или инцидента:

1. В разделе **События** на вкладке **События и инциденты** откройте контекстное меню по левой кнопке мыши в ячейке столбца **Метка** для строки с нужным событием или инцидентом.

2. В контекстном меню выберите метку, которую вы хотите установить для этого события или инцидента.

   Вы можете выбрать одну из семи меток, предусмотренных в программе. Назначение каждой метки вы выбираете самостоятельно.

3. Если вам потребуется снять метку, выберите в контекстном меню пункт **Без метки**.

Копирование событий в текстовый редактор

Вы можете скопировать информацию о событиях и инцидентах, отображаемых в таблице событий, в любой текстовый редактор. Информация копируется из столбцов, отображаемых в таблице в текущий момент.

Возможность копирования доступна, если выбрано не более 200 событий и инцидентов.

Чтобы скопировать события и/или инциденты в текстовый редактор:

1. Выберите вкладку **События и инциденты** в разделе **События**.

2. В таблице событий выберите события и/или инциденты, информацию о которых вы хотите скопировать в текстовый редактор.

3. По правой кнопке мыши откройте контекстное меню одного из выбранных событий.

4. В контекстном меню выберите один из следующих пунктов:

   - **Копировать детали события**, если выбрано одно событие или инцидент.
   - **Копировать детали выбранных событий**, если выбрано несколько событий и/или инцидентов.

5. Откройте любой текстовый редактор.

6. В окне текстового редактора выполните вставку (например, с помощью комбинации клавиш **CTRL+V**).

Скопированная информация о событии будет доступна для изменения в текстовом редакторе. Информация о нескольких событиях будет разделена пустой строкой.

Загрузка трафика для событий

При просмотре таблицы событий вы можете загружать трафик, относящийся к зарегистрированным событиям и/или инцидентам. Загрузка трафика выполняется в файл формата PCAP (при выборе одного события) или в архив формата ZIP, содержащий файлы формата PCAP (при выборе нескольких событий или инцидента).

Возможность загрузки трафика доступна, если в таблице событий выбрано не более 200 событий (в том числе в составе инцидентов).

Трафик для событий загружается из базы данных программы. В базе данных трафик может сохраняться при регистрации событий, для которых включено сохранение трафика. Также программа может сохранять трафик в базе данных непосредственно при запросе на загрузку трафика, используя файлы дампа трафика. Эти файлы предназначены для временного хранения трафика и автоматически удаляются по мере поступления трафика из промышленной сети (периодичность удаления файлов зависит от интенсивности поступающего трафика и от заданных параметров хранения данных программы). Для гарантированной загрузки трафика рекомендуется включить сохранение трафика для нужных типов событий и настроить параметры хранения трафика в базе данных в соответствии с интенсивностью его поступления и регистрации событий.

Чтобы загрузить файл трафика для событий и/или инцидентов:

1. В разделе **События** на вкладке **События и инциденты** выберите события и/или инциденты, для которых вы хотите загрузить трафик.

2. Нажмите на кнопку **Скачать трафик**.

3. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции формирования файла.

   c. Нажмите на кнопку **Скачать файл**.

Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Экспорт данных о событиях активности в файл индикаторов компрометации

При просмотре сведений об инцидентах EDR вы можете экспортировать в IOC-файл данные о событиях активности, если вы хотите обнаружить возникновение таких событий активности при следующих проверках EPP-приложений. Например, полученный IOC-файл вы можете использовать в задачах поиска IOC, выполняемых с помощью программного компонента Endpoint Agent.

Чтобы экспортировать данные о событиях активности в IOC-файл:

1. В разделе **События** на вкладке **События и инциденты** выберите событие, которое является инцидентом EDR (событие отмечено значком **EDR**) и содержит цепочку развития угрозы с нужными событиями активности.

   В правой части окна веб-интерфейса появится область деталей.

2. В области деталей перейдите на вкладку **Все события активности** и выберите нужные события активности.

   Вы можете выбрать события активности с типами **Создание файла**, **Запуск процесса** или **Изменение в реестре**.

3. Нажмите на кнопку **Экспорт в IOC-файл**.

4. В открывшемся окне выберите условие для обнаружения индикаторов компрометации:

   - **ИЛИ (любой IOC обнаружен)** – если вы хотите, чтобы в задаче поиска IOC происходило срабатывание при обнаружении любого индикатора компрометации из IOC-файла.

   - **И (все IOC обнаружены)** – если вы хотите, чтобы в задаче поиска IOC происходило срабатывание при обнаружении всех индикаторов компрометации из IOC-файла.

5. Просмотрите сведения, которые будут экспортированы в IOC-файл.

   Экспорт возможен только при ненулевых значениях счетчиков, отображаемых для любого из параметров **Создание файла**, **Запуск процесса** и **Изменение в реестре**. Параметр **Неэкспортируемые** содержит количество выбранных событий активности, данные о которых невозможно экспортировать в IOC-файл.

6. Нажмите на кнопку **Экспортировать**.

7. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции формирования файла.

   c. Нажмите на кнопку **Скачать файл**.

Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Создание директории для экспорта событий на сетевой ресурс

Вы можете экспортировать события и сохранять файл с экспортированными событиями на сетевом ресурсе компьютера Сервера. Для работы сетевого ресурса вы можете использовать протокол Network File System (NFS), с помощью которого выполняется монтирование общего сетевого ресурса другого компьютера (например, точки экспорта сервера NFS) в локальной файловой системе компьютера Сервера. Создание директории и монтирование общего сетевого ресурса выполняется с помощью стандартных средств операционной системы.

При использовании протокола NFS в операционной системе активируется программный пакет rpcbind. Следует учитывать, что злоумышленники могут попытаться использовать этот программный пакет для проведения некоторых типов DDoS-атак. Для устранения угрозы проникновения требуется выполнить настройку сетевого экрана. В операционной системе CentOS Stream рекомендуется использовать программу настройки сетевой защиты firewalld.

Создание директории и монтирование общего сетевого ресурса вручную

Чтобы создать директорию для сохранения файлов на сетевой ресурс:

1. Откройте консоль операционной системы.

2. Создайте локальную директорию для монтирования общего сетевого ресурса. Для этого введите команду:

   ```
   mkdir <полный путь локальной директории>
   ```

   Например:

   ```
   mkdir ~/nfsshare
   ```

3. После создания директории введите команду монтирования сетевого ресурса:

   ```
   sudo mount -t nfs <имя или IP-адрес удаленного компьютера>:\
   <полный путь общего сетевого ресурса>\
   <полный путь локальной директории>
   ```

   Например:

   ```
   sudo mount -t nfs nfs-server.example:/nfsshare ~/nfsshare
   ```

4. Проверьте результат монтирования с помощью команды:

   ```
   mount | grep <полный путь локальной директории>
   ```

   Например:

   ```
   mount | grep ~/nfsshare
   ```

   При успешном монтировании будут выведены данные, содержащие имя или IP-адрес удаленного компьютера, имя общего сетевого ресурса и имя родительской директории.

Автоматическое монтирование общего сетевого ресурса

Чтобы настроить автоматическое монтирование общего ресурса в операционной системе CentOS,

откройте файл /etc/fstab для редактирования с root-правами и в тексте файла добавьте строку:

```
<имя или IP-адрес удаленного компьютера>:<полный путь общего сетевого ресурса> <полный путь локальной директории> nfs defaults 0 0
```

Например:

```
nfs-server.example:/nfsshare /home/user1/nfsshare nfs defaults 0 0
```

Контроль рисков

Kaspersky Industrial CyberSecurity for Networks может обнаруживать риски, которым подвержены ресурсы информационной системы. Программа определяет риски по результатам анализа трафика и по полученным сведениям об устройствах.

Обнаруживаемые риски могут принадлежать следующим категориям:

- Уязвимость. К этой категории относятся обнаруженные уязвимости устройств.
- Проблемы конфигурации. К этой категории относятся риски для безопасной работы устройств из-за неверно настроенных конфигураций и риски компрометации данных при записи и чтении конфигураций устройств.
- Нарушение ИБ АСУ ТП. К этой категории относятся риски нарушения информационной безопасности в автоматизированной системе управления технологическим процессом.
- Небезопасная архитектура сети. К этой категории относятся риски, связанные с обнаружением небезопасных сетевых взаимодействий, устройств, протоколов и программного обеспечения, риски из-за прекратившейся активности разрешенных устройств, а также риски из-за отсутствия или неполноценной работы EPP-приложений на устройствах.

Каждый риск оценивается по шкале от 0.0 до 10.0. Программа выполняет расчет числового значения оценки для риска с учетом имеющихся сведений об устройстве, с которым связан обнаруженный риск. При расчете значения оценки программа учитывает уровень значимости устройства, а также другие риски, связанные с этим устройством. В качестве исходного значения для расчета используется *базовая оценка*. Базовые оценки рисков категории Уязвимость определяются по общей системе оценки уязвимостей (Common Vulnerability Scoring System – CVSS). Для остальных категорий рисков используются базовые оценки, заданные в таблице типов рисков.

Информация о рисках загружается в базу данных обнаруженных рисков на Сервере Kaspersky Industrial CyberSecurity for Networks. Суммарный объем сохраняемых записей в базе данных не может превышать заданное ограничение. Если объем превышает заданное ограничение, программа автоматически удаляет 10% самых старых записей. Вы можете задать ограничение максимального объема для обнаруженных рисков при настройке параметров хранения данных на узле Сервера.

Содержимое базы данных обнаруженных рисков отображается в разделе **Риски** веб-интерфейса программы. Вы также можете просматривать общие сведения о наличии рисков, связанных с устройствами, в разделе **Активы** на вкладке **Устройства**.

О рисках категории Уязвимость

Риски категории Уязвимость регистрируются при обнаружении уязвимостей в контролируемых устройствах промышленной сети. *Уязвимость* – это недостаток в программном или аппаратном обеспечении устройства, используя который злоумышленник может повлиять на работу информационной системы или получить несанкционированный доступ к информации.

Программа обнаруживает уязвимости, анализируя имеющиеся сведения об устройствах. Сведения, по которым можно найти известную уязвимость для устройства, сравниваются с определенными полями в *базе данных известных уязвимостей*. База данных известных уязвимостей встроена в программу. Эту базу данных формируют специалисты "Лаборатории Касперского", размещая в ней сведения о наиболее актуальных или часто встречающихся уязвимостях устройств в промышленных сетях.

База данных известных уязвимостей содержит описания уязвимостей, а также устройств, которые подвержены этим уязвимостям. Кроме того, эта база данных содержит рекомендации для защиты системы в виде текстов или ссылок на общедоступные ресурсы. В базу данных известных уязвимостей загружены описания и рекомендации из различных источников, среди которых могут быть производители устройств и программного обеспечения, а также различные организации, специализирующиеся в области промышленной безопасности. Описания и рекомендации в базе данных приводятся на английском языке.

После установки программы используется исходная база данных известных уязвимостей. Вы можете поддерживать базу данных в актуальном состоянии, устанавливая обновления.

Kaspersky Industrial CyberSecurity for Networks сравнивает имеющиеся сведения об устройствах с полями в базе данных известных уязвимостей, которые описывают устройства, подверженные уязвимостям. Для обнаружения уязвимостей программа использует следующие сведения об устройствах:

- **Производитель аппаратной части**.
- **Модель аппаратной части**.
- **Версия аппаратной части**.
- **Производитель ПО**. Если в сведениях об устройстве не была обнаружена информация о производителе ПО, Kaspersky Industrial CyberSecurity for Networks переиспользует значение параметра **Производитель аппаратной части**.
- **Название ПО**. Если в сведениях об устройстве не было обнаружено название ПО, Kaspersky Industrial CyberSecurity for Networks переиспользует значение параметра **Модель аппаратной части**.
- **Версия ПО**.

В базе данных известных уязвимостей описания устройств хранятся в формате языка CPE (Common Platform Enumeration). Программа сравнивает имеющиеся сведения об устройствах с этими описаниями, автоматически преобразовывая сведения в формат языка CPE.

Для каждой уязвимости содержимое совпавших описаний приводится в области деталей риска в разделе **Совпавшие CPE**.

Если сведения об устройстве совпадают с соответствующими полями в базе данных известных уязвимостей, программа регистрирует риск категории Уязвимость и загружает информацию об уязвимости в базу данных обнаруженных рисков.

Основным параметром, который идентифицирует уязвимость, является ее идентификационный номер в списке общеизвестных уязвимостей и рисков (Common Vulnerabilities and Exposures – CVE). Этот идентификационный номер называется *CVE-идентификатором*. Если уязвимости еще не присвоен CVE-идентификатор, для нее указывается идентификационный номер, полученный в других общедоступных ресурсах с описаниями уязвимостей.

В Kaspersky Industrial CyberSecurity for Networks поддерживается получение идентификаторов и ссылок на описания уязвимостей, предоставляемых Федеральной службой по техническому и экспортному контролю (ФСТЭК) России в Банке данных угроз безопасности информации (далее также "БДУ"). Если загружаемая информация об уязвимости содержит такие сведения из БДУ ФСТЭК, программа отображает эти сведения в виде соответствующих идентификаторов в формате BDU:<год>-<номер>.

Сценарий реализации для процесса непрерывного управления рисками

Функциональность обнаружения рисков позволяет реализовать непрерывное (циклическое) управление рисками в вашей информационной системе. Для управления рисками Kaspersky Industrial CyberSecurity for Networks предоставляет информацию об обнаруженных рисках, на основе которой вы можете предпринять нужные меры по их устранению или минимизации.

Сценарий реализации для процесса непрерывного управления рисками состоит из следующих этапов:

1. **Инвентаризация устройств**

   Этот этап реализуется с использованием методов обнаружения активности устройств и обнаружения сведений об устройствах (применение методов должно быть включено). На этом этапе программа автоматически обнаруживает новые устройства и обновляет сведения об устройствах. Если в промышленной сети есть устройства, которые не были обнаружены автоматически, вам нужно добавить их вручную или импортировать из внешних проектов.

   Для всех сведений, определяющих классификацию и эксплуатационные особенности устройств (например, информация о модели и версии программного обеспечения на устройстве), требуется включить автоматическое изменение в параметрах устройств. Если автоматическое изменение таких сведений не может выполняться по каким-либо причинам, эти сведения следует актуализировать вручную.

2. **Обнаружение рисков при пассивном и активном сканировании**

   Программа выполняет пассивное сканирование устройств на наличие рисков, используя имеющиеся сведения об устройствах. Также для обнаружения рисков программа анализирует сетевые взаимодействия в трафике промышленной сети. Обнаружение рисков реализуется с использованием метода обнаружения рисков (применение метода должно быть включено).

   Вы также можете выполнять активный опрос устройств для быстрого получения сведений от этих устройств. При активном опросе устройств дополнительно предоставляются возможности обнаружения некоторых типов рисков, если выбраны соответствующие методы для анализа рисков. Для проведения активного опроса устройств вам нужно добавить в программу один или несколько коннекторов типа **Active poll**.

   Обнаружение рисков категории Уязвимость происходит автоматически после обновления базы данных известных уязвимостей в программе или после добавления/изменения тех сведений об устройствах, которые используются для сравнения (например, после сохранения информации о модели и версии программного обеспечения на устройстве).

3. **Оценка обнаруженных рисков и их классификация**

   Для каждого обнаруженного риска программа выполняет расчет значения оценки. Оценка определяет уровень критичности риска. В зависимости от числового значения оценки риск может относиться к уровням критичности *Низкий* (оценки 0.0–3.9), *Средний* (оценки 4.0–7.9) или *Высокий* (оценки 8.0–10.0).

На основании уровней критичности со значениями оценок, а также с учетом факторов, связанных с особенностями использования устройств в вашей информационной системе, вы можете классифицировать обнаруженные риски по их значимости. Если вы оцениваете риск как незначительный, его статус можно вручную изменить со статуса *Актуальный* (присвоен риску по умолчанию после обнаружения) на статус *Принят*, например, в случае, если условия для эксплуатации уязвимости не могут быть воспроизведены. При изменении статуса риска рекомендуется добавить или изменить комментарий к нему.

Все риски, по которым требуется выполнить какие-либо дополнительные действия, следует оставить со статусом *Актуальный*.

4. **Устранение рисков**

На этом этапе вам нужно выполнить действия, которые позволят устранить обнаруженные риски или минимизировать угрозы, связанные с возможной реализацией этих рисков. Для этого проверьте все обнаруженные риски со статусом *Актуальный*, начиная с рисков, имеющих наибольшие значения оценок. Выполните нужные действия в вашей информационной системе (например, для устранения уязвимости устройства установите необходимое обновление программного обеспечения, а если это невозможно, то изолируйте это устройство от внешних сетей). Для некоторых рисков (например, для уязвимостей) представлена информация о рекомендуемых действиях.

> Действия по устранению обнаруженных рисков выполняются без участия Kaspersky Industrial CyberSecurity for Networks.

5. **Проверка устранения рисков**

Этот этап аналогичен этапу обнаружения рисков при сканировании. В результате выполнения этого этапа в таблице рисков не должно остаться рисков со статусом *Актуальный*.

Для большинства рисков, которые программа обнаруживает при пассивном сканировании (например, уязвимости), программа автоматически присваивает статус *Устранен*, если перестали выполняться условия для обнаружения этих рисков. Например, после изменения сведений о версии программного обеспечения на устройстве программа присваивает статус *Устранен* риску категории Уязвимость, который был зарегистрирован из-за указанной ранее уязвимой версии программного обеспечения. Статус *Устранен* также присваивается тем рискам, для которых больше нет описания в базе данных известных уязвимостей (в случае удаления описания из базы данных после загрузки обновлений).

При удалении устройств программа удаляет и риски, которые были связаны с этими устройствами.

Если после выполнения действий по устранению риска не изменились условия для его обнаружения (например, уязвимое устройство изолировано от внешних сетей, но сведения об этом устройстве не изменились), вы можете вручную присвоить этому риску статус *Принят*. При изменении статуса риска рекомендуется добавить или изменить комментарий к нему.

Некоторые риски не предусматривают автоматического присвоения статуса *Устранен* (например, автоматическое присвоение статуса *Устранен* не выполняется для рисков, обнаруженных при активном опросе устройств). Для таких рисков также требуется вручную присвоить статус *Принят* после выполнения действий по устранению риска.

Если риск связан с событием, вы можете присвоить этому риску статус *Принят* одновременно с изменением статуса события на статус *Обработано*.

Просмотр таблицы рисков

Таблица рисков отображается в разделе **Риски** веб-интерфейса программы.

Параметры рисков отображаются в следующих столбцах таблицы:

- **Категория**.

  Название категории риска.

- **Название**.

  Название риска. Для риска категории Уязвимость используется CVE-идентификатор обнаруженной уязвимости (если CVE-идентификатор отсутствует, отображается идентификационный номер, полученный в других общедоступных ресурсах с описаниями уязвимостей).

- **CVE**.

  Для риска категории Уязвимость: CVE-идентификатор обнаруженной уязвимости.

- **БДУ**.

  Для риска категории Уязвимость: идентификатор уязвимости в базе БДУ. Если одной уязвимости с CVE-идентификатором соответствуют несколько уязвимостей с разными идентификаторами в базе БДУ, столбец содержит все такие идентификаторы.

- **ID риска**.

  Уникальный идентификатор риска.

- **Оценка**.

  Рассчитанное значение оценки для риска. Числовое значение определяет, к какому уровню критичности относится риск. В зависимости от уровня критичности, значение оценки может быть окрашено одним из следующих цветов:

  - Красный – риск с уровнем критичности *Высокий*.
  - Желтый – риск с уровнем критичности *Средний*.
  - Синий – риск с уровнем критичности *Низкий*.

  Для рисков со статусом *Актуальный* значение оценки окрашено ярким цветом. Если риску присвоен статус *Устранен* или *Принят*, его значение оценки окрашено бледным цветом.

  В области деталей этот параметр называется **Базовая оценка**.

- **Сторона 1**.

  Адресная информация одной из сторон сетевого взаимодействия (указывается для некоторых типов рисков). Отображение MAC- и IP-адресов можно включать и выключать по отдельности. Если в программу добавлены дополнительные адресные пространства, при настройке таблицы рисков можно включать и выключать отображение имен адресных пространств с помощью параметра **Отображать адресные пространства**.

- **Сторона 2**.

  Адресная информация другой стороны сетевого взаимодействия (указывается для некоторых типов рисков). Отображение адресной информации можно настраивать аналогично, как для столбца **Сторона 1**.

- **Группа устройств**.

  Имя группы, в которую помещено устройство с обнаруженным риском (содержит имя самой группы и имена всех ее родительских групп).

- **Устройство**.

  Имя и адрес устройства.

- **Источник**.

  Для риска категории Уязвимость: название источника, из которого загружены сведения в базу данных известных уязвимостей. В области деталей этот параметр называется **Источник уязвимости**.

- **Статус**.

  Текущий статус риска. Предусмотрены следующие статусы:

  - *Актуальный* – статус по умолчанию при первом обнаружении риска (а также при повторном обнаружении, если риску был присвоен статус *Устранен*). Также риску можно вручную присвоить статус *Актуальный*, если его текущий статус *Принят*.

  - *Устранен* – автоматически присваиваемый статус, если перестали выполняться условия для обнаружения риска.

  - *Принят* – статус, присваиваемый риску вручную, если риск оценивается как незначительный или если действия по устранению риска не привели к автоматическому присвоению статуса *Устранен*.

- **Обнаружен**.

  Дата и время обнаружения риска.

- **Последнее изменение статуса**.

  Дата и время последнего изменения статуса риска.

- **Совпавшие CPE**.

  Для риска категории Уязвимость: описания устройств, хранящиеся в базе данных известных уязвимостей. Приводятся описания, которые совпали со сведениями об устройстве в таблице устройств.

При просмотре таблицы рисков вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Просмотр сведений о риске

Подробные сведения о риске включают информацию из таблицы рисков, а также следующие поля:

- **Тип риска** – код типа риска.

- **Описание** – описание, заданное для типа риска или для уязвимости.

- **Базовая оценка** – исходное значение для расчета числового значения оценки риска.

Для риска категории Уязвимость выводится дополнительная информация в следующих полях и группах полей:

- **Вектор CVSS** – запись метрик для вычисления оценки уязвимости по системе CVSS.

- **Условия эксплуатации уязвимости** – описание условий эксплуатации уязвимости.

- **Возможные последствия** – описание возможных последствий при эксплуатации уязвимости.

- **Рекомендации** – рекомендации по устранению уязвимости (например, сведения о том, какую версию программного обеспечения рекомендуется установить на устройстве).
- **Ссылки** – ссылки на общедоступные ресурсы с дополнительными сведениями об уязвимости.
- **История CVE** – даты этапов выявления, подтверждения и публикации уязвимости в общедоступных источниках.

Чтобы просмотреть сведения о риске,

выберите нужный риск в таблице рисков.

В правой части окна веб-интерфейса появится область деталей с подробными сведениями о риске.

*Чтобы просмотреть сведения о риске категории Уязвимость в разделе **Активы** на вкладке **Устройства**,*

нажмите на название уязвимости (в виде CVE-идентификатора или другого идентификационного номера уязвимости) в столбце **Риски** или в области деталей устройства с этим риском.

Появится окно с подробными сведениями об уязвимости.

Изменение статусов рисков вручную

При работе в разделе **Риски** вы можете вручную изменять статусы любых рисков со статуса *Актуальный* на статус *Принят* и обратно. При работе в разделе **Активы** вы можете менять статус только рисков категории Уязвимость и только со статуса *Актуальный* на статус *Принят*.

Также вы можете присвоить риску статус *Принят* при присвоении статуса *Обработано* событиям, которые связаны с этим риском.

Чтобы изменить статус риска вручную:

1. Откройте область деталей риска или окно с подробными сведениями о риске.
2. Откройте раскрывающийся список **Изменить статус**.
3. В зависимости от того, какой статус вы хотите присвоить риску, в раскрывающемся списке выберите один из следующих пунктов:
   - **Принят** – если вы хотите изменить статус риска со статуса *Актуальный* на статус *Принят*.
   - **Актуальный** – если вы хотите вернуть риску статус *Актуальный*.

   Откроется окно с запросом подтверждения.
4. Если с выбранным риском связаны события и вы хотите одновременно присвоить статус *Обработано* всем этим событиям, установите флажок **Присвоить статус Обработано всем связанным событиям**.

   Риски могут быть связаны с событиями при регистрации событий некоторых типов по технологии Контроль активов.
5. В окне запроса нажмите на кнопку **ОК**.

Просмотр сведений о рисках при работе с таблицей устройств

При работе с таблицей устройств вы можете просматривать сведения о рисках, которые были обнаружены на устройствах. Для каждого устройства с рисками категории Уязвимость отображаются названия обнаруженных уязвимостей (в виде CVE-идентификаторов или других идентификационных номеров уязвимостей). Если на устройстве обнаружены риски других категорий, для этого устройства отображаются названия этих категорий рисков. Названия уязвимостей и категорий рисков отображаются в столбце **Риски** и в области деталей при выборе устройства.

По умолчанию в таблице устройств отображаются сведения только о тех рисках, которым присвоен статус *Актуальный*. При необходимости вы можете включить отображение сведений обо всех рисках, установив флажок **Отображать устраненные и принятые риски** при настройке таблицы устройств.

Для обозначения уровней критичности рисков названия уязвимостей и категорий окрашиваются одним из следующих цветов:

- Красный – риски с уровнем критичности *Высокий*.
- Желтый – риски с уровнем критичности *Средний*.
- Синий – риски с уровнем критичности *Низкий*.

Для рисков со статусом *Актуальный* названия окрашены ярким цветом. Для рисков со статусом *Устранен* или *Принят* названия окрашены бледным цветом.

Если с устройством связаны риски одной и той же категории, название этой категории окрашивается цветом наиболее высокого уровня критичности из всех этих рисков.

Если вы хотите просмотреть подробные сведения о рисках, вы можете использовать отображаемые названия уязвимостей и категорий рисков. При нажатии на название уязвимости (в виде CVE-идентификатора или другого идентификационного номера уязвимости) открывается окно деталей уязвимости. При нажатии на название категории риска программа выполняет переход к таблице рисков и применяет фильтрацию для отображения рисков выбранной категории, связанных с устройством.

При просмотре таблицы устройств вы можете настроить параметры фильтрации устройств по связанным с ними рискам. Также вы можете выполнять поиск устройств по названиям уязвимостей (в виде CVE-идентификаторов или других идентификационных номеров уязвимостей).

Контроль технологического процесса

Kaspersky Industrial CyberSecurity for Networks позволяет контролировать технологический процесс, предоставляя информацию о параметрах технологического процесса и полученных системных командах, передаваемых в трафике промышленной сети. Программа отслеживает эти данные для устройств, представленных в таблице устройств и имеющих заданные параметры контроля процесса.

Вы можете просматривать контролируемые теги и имеющиеся правила контроля процесса на странице веб-интерфейса Сервера в разделе **Контроль процесса**. Параметры контроля процесса для устройств доступны при выборе устройств в разделах **Активы** и **Карта сети**.

Мониторинг значений параметров технологического процесса

Kaspersky Industrial CyberSecurity for Networks может отображать значения параметров технологического процесса (тегов) в онлайн-режиме.

Для отображения значений требуется добавить нужные теги в программу. Добавление тегов выполняется при настройке контроля процесса.

Программа не сохраняет значения тегов, которые отображаются в онлайн-режиме. Имена и значения тегов могут сохраняться в событиях, зарегистрированных по технологии Контроль технологического процесса (в событии сохраняются значения тегов, полученные на момент регистрации события). Для сохранения имен и значений тегов необходимо наличие переменной $tags в параметрах типов событий.

Чтобы просматривать значения параметров технологического процесса,

подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс и в разделе **Контроль процесса** выберите вкладку **Теги**.

В окне браузера отобразится таблица с тегами и их текущими значениями. Оперативно изменяемые значения отображаются в следующих параметрах тегов:

- **Базовый тип данных**.
- **Чтение/запись**.
- **Получено**.
- **Метка времени**.
- **Статус метки времени**.
- **Статус данных**.
- **Инициатор**.
- **Значение**.
- **Структурные значения**.
- **Причина передачи**.

Для мониторинга значений тегов вы можете использовать все функции, доступные при просмотре таблицы тегов.

Параметры тегов

Параметры тегов, используемые при контроле процесса, отображаются в таблице тегов и в области деталей при выборе тега.

В зависимости от того, какие столбцы выбраны для отображения, в таблице тегов могут отображаться следующие параметры:

- **Группа устройств** – имя группы, в которую помещено связанное с тегом устройство (содержит имя самой группы и имена всех ее родительских групп в дереве групп устройств). В области деталей этот параметр называется **Группа**.
- **Устройство** – имя связанного с тегом устройства.
- **Протокол** – название протокола, по которому передается тег.
- **Имя тега** – заданное имя тега.
- **Тип данных протокола** – тип данных тега, указывающий специфическое название операции по протоколу (если поддерживаются такие названия в протоколе – например, для протоколов стандартов IEC 60870-5-104 и IEC 60870-5-101), или обозначенный стандартным именем типа данных (например, int32).
- **Единица измерения** – единица измерения параметра технологического процесса, который представлен тегом.
- **Базовый тип данных** – тип данных для значения, которое является основным в структуре полей тега (обозначается стандартным именем типа данных).
- **Чтение/запись** – направление передачи, при котором получено значение тега (R – при чтении из устройства, W – при записи в устройство, RW – любое направление).
- **В избранных** – признак включения тега в список избранных.
- **Описание** – дополнительные сведения о теге.
- **Адрес тега** – физический адрес тега в памяти устройства.
- **Идентификатор тега** – порядковый номер тега. Идентификатор тега задается автоматически. В области деталей этот параметр называется **Идентификатор**.
- **Получено** – дата и время последнего получения значения тега программой.
- **Метка времени** – дата и время последнего изменения/обновления значения тега (полученное из трафика).
- **Статус метки времени** – текущий статус для даты и времени последнего изменения/обновления значения тега.
- **Статус данных** – текущий статус для полученного значения тега.
- **Инициатор** – название источника, от которого получено значение тега или передана команда.
- **Значение** – оперативно изменяемое значение тега.
- **Масштабируемый тег** – признак масштабирования тега в пределах минимумов и максимумов для входных и выходных значений.
- **Вход (минимально)** – минимальный предел для входного значения.
- **Вход (максимально)** – максимальный предел для входного значения.

- **Выход (минимально)** – минимальный предел для выходного значения.
- **Выход (максимально)** – максимальный предел для выходного значения.
- **Структурные значения** – список имен и значений всех полей тега. Элементы списка разделяются запятой с пробелом (например: `field1: <значение1>, field2: <значение2>`). Имена вложенных полей составляются из имен всех родительских полей, и имени самого поля, разделенных двоеточием (например: `parent1:parent2:field: <значение>`). Строковые значения должны быть заключены в кавычки.
- **Причина передачи** – причина изменения или отправки значения тега (полученная из трафика).
- **Источник** – сведения об источнике создания тега. При автоматическом создании тега параметру **Источник** присваивается значение **Система**. Если тег был создан или изменен пользователем, параметру **Источник** присваивается значение **Пользователь**.

В области деталей для выбранного тега дополнительно могут отображаться другие параметры, определяемые в зависимости от устройства и протокола (например: **Номер блока**, **Область памяти**).

Для контроля технологического процесса на устройствах, которые взаимодействуют по протоколам стандартов IEC 60870-5-104 и IEC 60870-5-101, поддерживаются типы кадров, представляющие блоки данных прикладного уровня (ASDU). Сведения о поддерживаемых типах кадров ASDU в этих протоколах см. в Приложении.

Просмотр таблицы тегов

Таблица тегов отображается в разделе **Контроль процесса** на вкладке **Теги**. В таблице представлены общие параметры тегов, а также устройств, к которым относятся теги.

При просмотре таблицы тегов вы можете использовать функции настройки, фильтрации, поиска и сортировки, а также переходить к связанным элементам.

Обнаружение паролей по умолчанию при подключении к устройствам

При отслеживании взаимодействий устройств для контроля процесса Kaspersky Industrial CyberSecurity for Networks может определять используемые пароли по умолчанию. Если при подключении к устройству использован пароль, который задан для этого типа устройств как пароль по умолчанию, программа зарегистрирует соответствующее событие. Для регистрации событий обнаружения паролей по умолчанию используется системный тип события обнаружения системных команд.

Kaspersky Industrial CyberSecurity for Networks обнаруживает пароли по умолчанию в следующих случаях:

- Попытка использования пароля по умолчанию завершена успешно или не определен результат этой попытки. В этом случае регистрируется событие обнаружения системной команды DEFAULT PASSWORD ENTRY.

- Установка нового пароля, совпадающего с паролем по умолчанию. В этом случае регистрируется событие обнаружения системной команды DEFAULT PASSWORD SET.

- Получение пароля по умолчанию при чтении из устройства учетных данных для подключения. В этом случае регистрируется событие обнаружения системной команды DEFAULT PASSWORD READ или DEFAULT PASSWORD READ WITH TYPE (если в сведениях о пароле указан его тип, определяющий возможные операции с устройством с использованием этого пароля).

Обнаружение паролей по умолчанию поддерживается для устройств определенных типов и протоколов прикладного уровня (см. таблицу ниже).

Поддерживаемые устройства и протоколы с паролями по умолчанию

Устройства	Протоколы	Системные команды
ABB серии Relion: RED670, REL670, RET670	ABB SPA-Bus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD SET
BECKHOFF® серий CX	BECKHOFF ADS/AMS	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
Emerson серии ControlWave	Emerson ControlWave Designer	DEFAULT PASSWORD ENTRY
General Electric серии Multilin: B30, C60	Modbus TCP	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD READ WITH TYPE DEFAULT PASSWORD SET
Mitsubishi System Q E71	Mitsubishi MELSEC System Q	DEFAULT PASSWORD SET
Schneider Electric серии Modicon: M580, M340	Modbus TCP	DEFAULT PASSWORD READ WITH TYPE
Siemens SIMATIC серий S7-200, S7-300, S7-400	Siemens Industrial Ethernet Siemens S7comm	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ
Siemens SIMATIC серий S7-1200, S7-1500	Siemens Industrial Ethernet Siemens S7comm-plus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
ПЛК с системой исполнения для CODESYS V3 (например, Прософт-Системы Regul R500)	CODESYS V3 Gateway	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
ЭКРА серии 200	Modbus TCP для устройств ЭКРА серии 200	DEFAULT PASSWORD READ DEFAULT PASSWORD SET
ЭКРА серий БЭ2502, БЭ2704	ABB SPA-Bus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD SET

Для регистрации событий обнаружения паролей по умолчанию должны выполняться следующие условия:

- Контроль взаимодействий включен в режиме наблюдения с применением технологии Контроль системных команд.
- В таблице разрешающих правил отсутствуют правила для технологии Контроль системных команд, которые разрешают системные команды с паролями по умолчанию. Например, программа может автоматически создать такие правила в режиме обучения контроля взаимодействий. Если такие правила присутствуют в таблице разрешающих правил, рекомендуется их выключить.
- Для нужных устройств включено отслеживание системных команд с паролями по умолчанию.

Получение отчетов

С помощью Kaspersky Industrial CyberSecurity for Networks вы можете получать отчеты с различными сведениями, сохраненными программой. Kaspersky Industrial CyberSecurity for Networks формирует отчеты в виде файлов в формате PDF. Программа может отправлять файлы с отчетами на адреса электронной почты, указанные пользователем с ролью Администратор. Также вы можете загружать отчеты на странице веб-интерфейса Сервера.

В Kaspersky Industrial CyberSecurity for Networks предусмотрены следующие виды отчетов:

- Отчеты по шаблонам.

  Эти отчеты содержат накопленную информацию об устройствах и их состояниях, о безопасности системы, об отслеживаемых параметрах технологического процесса и системных командах, а также об обнаруженных рисках и взаимодействиях со сторонними устройствами.

- Отчеты по заданиям аудита настроек и уязвимостей.

  Эти отчеты содержат информацию о результатах выполнения заданий аудита настроек и уязвимостей.

Вы можете просматривать информацию о сформированных отчетах и экспортировать их в файлы в разделе **Отчеты** на вкладке **Сформированные отчеты**.

Просмотр таблицы отчетов

Вы можете просмотреть таблицу отчетов в разделе **Отчеты** на вкладке **Сформированные отчеты** веб-интерфейса программы.

Параметры отчетов отображаются в следующих столбцах таблицы:

- **ID**.

  Уникальный идентификатор отчета.

- **Имя отчета**.

  Название сформированного отчета.

- **Имя шаблона**.

  Название шаблона, по которому был сформирован отчет.

- **Запуск**.

  Дата и время запуска формирования отчета.

- **Статус**.

  Статус выполнения отчета. Предусмотрены следующие статусы выполнения отчета:

  - **Ожидание**. Отчет находится в очереди на формирование. Отчет может иметь статус *В ожидании* при формировании нескольких отчетов одновременно.
  - **Формируется**. Отчет находится в процессе формирования.
  - **Ошибка**. При формировании отчета произошла ошибка.
  - **Готово**. Формирование отчета завершено.
  - **Отменяется**. Формирование отчета находится в процессе отмены.
  - **Отменено**. Формирование отчета было отменено.

- **Пользователь**.

  Имя пользователя, запустившего формирование отчета или настроившего расписание запуска отчета по шаблону.

- **Тип запуска**.

  Тип запуска формирования отчета: вручную или по расписанию.

- **Завершен**.

  Дата и время завершения формирования отчета.

При просмотре таблицы отчетов вы можете использовать функции настройки, фильтрации и сортировки.

Экспорт отчета в файл

Вы можете экспортировать сформированный отчет в файл в формате PDF.

Чтобы экспортировать отчет в файл:

1. Выберите раздел **Отчеты**.
2. На вкладке **Сформированные отчеты** выберите нужный отчет.

   Отчеты отфильтрованы по идентификаторам отчетов, запущенных последними в текущем сеансе подключения к Серверу. Для отображения всех сформированных отчетов сбросьте параметры фильтрации с помощью кнопки **Фильтр по умолчанию**. Если требуется, вы можете настроить фильтрацию по нужному периоду времени.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Экспорт**.

Браузер сохранит файл отчета. По умолчанию файл отчета имеет название в формате `<название отчета>_<дата и время формирования отчета>`. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Отчеты по шаблонам

Шаблоны отчетов в Kaspersky Industrial CyberSecurity for Networks могут быть следующих типов:

- Системные шаблоны – создаются автоматически при установке программы. В таблице шаблонов отчетов системные шаблоны отображаются со значком . Вы не можете удалять системные шаблоны.

  Kaspersky Industrial CyberSecurity for Networks поддерживает следующие системные шаблоны для формирования отчетов:

  - **Отчет об активах**.

    Отчет, содержащий информацию об устройствах, отслеживаемых параметрах технологического процесса и системных командах, а также используемых протоколах и обнаруженных рисках на устройствах.

  - **Отчет о безопасности системы**.

    Отчет, содержащий информацию о состоянии безопасности устройств, зарегистрированных событиях, обнаруженных рисках и взаимодействиях с устройствами внешних сетей.

  - **Краткий отчет**.

    Отчет, содержащий краткую информацию об устройствах и состоянии безопасности системы.

  - **Полный отчет**.

    Отчет, содержащий полную информацию об устройствах и состоянии безопасности системы.

- Пользовательские шаблоны – создаются вручную путем дублирования шаблонов. Дублировать можно как системные, так и пользовательские шаблоны. Дублировать шаблоны могут только пользователи с ролью Администратор.

Данные в отчетах представлены в виде отдельных информационных блоков. Для каждого отчета Kaspersky Industrial CyberSecurity for Networks используется фиксированный набор и порядок расположения информационных блоков. Информационные блоки, которые используются в отчетах, и их описания приведены в таблице ниже.

Использование информационных блоков в отчетах

Название информационного блока	Отчет об активах	Отчет о безопасности системы	Краткий отчет	Полный отчет
Категории устройств	✓	–	✓	✓
Производители устройств	✓	–	✓	✓
Операционные системы на устройствах	✓	–	✓	✓
Отслеживаемые параметры технологического процесса	✓	–	–	✓
Устройства с наибольшим количеством рисков	✓	✓	–	✓
Наиболее уязвимые промышленные устройства	✓	✓	–	✓
Источники системных команд	✓	–	–	✓
Ситуационная осведомленность	–	✓	✓	✓
Новые устройства в сети	✓	–	–	✓

Название информационного блока	Отчет об активах	Отчет о безопасности системы	Краткий отчет	Полный отчет
Протоколы с наибольшим объемом трафика	✓	—	—	✓
Устройства с наибольшим количеством соединений с другими узлами	✓	—	—	✓
Объем сетевого трафика	✓	—	✓	✓
Протоколы общего применения	✓	—	✓	✓
Индустриальные протоколы	✓	—	✓	✓
Получатели системных команд	✓	—	—	✓
Состояния безопасности устройств	—	✓	✓	✓
Распределение устройств по статусам	—	✓	—	✓
Статистика по событиям	—	✓	—	✓
Распределение событий по технологиям обнаружения	—	✓	—	✓
Устройства с наибольшим количеством событий	—	✓	—	✓
Самые критичные события	—	✓	—	✓
Наиболее частые срабатывания правил обнаружения вредоносной активности	—	✓	—	✓
Нехарактерные протоколы в промышленной сети	—	✓	—	✓
Устройства с признаками доступа к публичным ресурсам	—	✓	—	✓
Подключения по протоколам удаленного управления	—	✓	—	✓
Изменения программ промышленных устройств	—	✓	—	✓
Актуальные риски	—	✓	✓	✓

Просмотр таблицы шаблонов отчетов

Вы можете просмотреть таблицу шаблонов отчетов в разделе **Отчеты** на вкладке **Шаблоны отчетов** веб-интерфейса программы.

Параметры шаблонов отчетов отображаются в следующих столбцах таблицы:

- **Имя**.

  Название шаблона отчета. Рядом с названиями системных шаблонов отчетов отображается значок .

- **Расписание**.

  Информация о расписании, по которому Kaspersky Industrial CyberSecurity for Networks автоматически запускает формирование отчета по шаблону. Информация о расписании отображается, если пользователь с ролью Администратор настроил параметры расписания в шаблоне отчета. Если параметры расписания не заданы, в столбце отображается значение **Выключено**.

- **Тип/пользователь**.

  Имя пользователя, внесшего последние изменения в шаблон отчета. Для системных шаблонов с параметрами по умолчанию отображается значение **Системный**.

- **Последний отчет**.

  Дата и время последнего запуска формирования отчета по шаблону отчета.

- **Получатели**.

  Значок, соответствующий наличию получателей отчетов по электронной почте. Предусмотрены следующие значки:

  - – получатели отчетов заданы.
  - – получатели отчетов не заданы.

При просмотре таблицы шаблонов отчетов вы можете использовать функции настройки и сортировки.

Просмотр сведений о шаблоне отчета

Чтобы просмотреть сведения о шаблоне отчета,

в разделе **Отчеты** на вкладке **Шаблоны отчетов** выберите нужный шаблон.

В правой части окна веб-интерфейса появится область деталей. В области деталей отображаются все сведения, для которых заданы значения.

Подробные сведения о шаблоне отчета включают следующие поля:

- **Имя** – название шаблона отчета.
- **Тип/пользователь** – имя пользователя, внесшего последние изменения в шаблон отчета. Для системных шаблонов с параметрами по умолчанию отображается значение **Системный**.
- **Период** – период времени, за который Kaspersky Industrial CyberSecurity for Networks формирует отчет по шаблону.
- **Изменен** – время последнего изменения шаблона.
- **Последний отчет** – время последнего запуска формирования отчета по шаблону.
- **Следующий запуск (локальное время)** – время следующего запуска формирования отчета по шаблону. Этот параметр отображается, если для шаблона отчета заданы параметры расписания.
- **Расписание** – информация о расписании, по которому Kaspersky Industrial CyberSecurity for Networks автоматически запускает формирование отчета по шаблону. Этот параметр отображается, если для шаблона отчета заданы параметры расписания.
- **Адреса получателей** – адреса электронной почту, на которые Kaspersky Industrial CyberSecurity for Networks отправляет сформированные отчеты. Этот параметр отображается, если для шаблона отчета заданы адреса получателей.

Формирование отчета по шаблону вручную

Вы можете запустить формирование отчета по шаблону вручную. Запускать формирование отчетов вручную могут как пользователи с ролью Администратор, так и пользователи с ролью Оператор.

Чтобы запустить формирование отчета:

1. Выберите раздел **Отчеты**.
2. На вкладке **Шаблоны отчетов** выберите один или несколько шаблонов, по которым вы хотите сформировать отчеты.

   При выборе нескольких шаблонов программа формирует по ним отчеты одновременно. Вы можете выбрать не более 10 шаблонов.
3. Нажмите на кнопку **Получить отчеты** в панели инструментов, которая расположена над таблицей шаблонов отчетов.

   Kaspersky Industrial CyberSecurity for Networks запустит процесс формирования отчета. Если требуется, вы можете обратиться к пользователю с ролью Администратор для отмены формирования отчета.

Вы перейдете на вкладку **Сформированные отчеты**, на которой отобразится статус выполнения запущенных отчетов. После завершения формирования отчетов Kaspersky Industrial CyberSecurity for Networks отправит файлы с отчетами в формате PDF на адреса электронной почты, указанные в шаблоне отчета. Если адрес электронной почты не задан в шаблоне отчета, вы можете экспортировать сформированные отчеты в файлы по отдельности вручную на вкладке **Сформированные отчеты**. Максимальный размер файла отчета – 10 МБ.

Отчеты по заданиям аудита настроек и уязвимостей

Kaspersky Industrial CyberSecurity for Networks может формировать отчеты со сведениями о результатах выполнения заданий аудита настроек и уязвимостей. Пользователь с ролью Администратор может настроить автоматическую отправку отчетов по электронной почте. При необходимости вы можете вручную сформировать отчет для завершенного запуска задания или для завершенного сканирования устройства и затем экспортировать отчет в файл.

Формирование отчета о запуске задания вручную

Вы можете вручную запустить формирование отчета для запуска задания аудита настроек и уязвимостей. Отчет формируется по результатам выполненных проверок на устройствах с использованием правил аудита настроек и уязвимостей, которые выбраны в параметрах задания.

Предусмотрены следующие формы отчетов о запусках заданий аудита настроек и уязвимостей:

- **Полный отчет**.

  Этот отчет содержит детальную информацию о выполненных проверках и об использованных правилах аудита настроек и уязвимостей.
- **Краткий отчет**.

  Этот отчет содержит сводную информацию о наиболее важных результатах проверок.

Для формирования отчета запуск задания аудита настроек и уязвимостей должен иметь один из следующих статусов: **Завершено**, **Не все успешно**, **Отменено** или **Ошибка**.

Чтобы запустить формирование отчета:

1. Выберите раздел **Аудит безопасности**.
2. На вкладке **Аудит настроек и уязвимостей** выберите задание, о выполнении которого вы хотите получить отчет.

   В правой части окна веб-интерфейса появится область деталей.
3. В области деталей перейдите на вкладку **Запуски**.
4. Выберите нужный запуск задания.
5. В появившейся области деталей запуска откройте раскрывающийся список **Получить отчет** и выберите нужную форму отчета: **Полный отчет** или **Краткий отчет** (раскрывающийся список отсутствует, если получение отчета невозможно в текущий момент).

   Kaspersky Industrial CyberSecurity for Networks запустит процесс формирования отчета.

Вы перейдете на вкладку **Сформированные отчеты** в разделе **Отчеты**. В таблице сформированных отчетов отобразится отчет аудита настроек и уязвимостей. После успешного завершения формирования отчета вы можете экспортировать сформированный отчет в файл.

Формирование отчета о сканировании устройства вручную

Вы можете вручную запустить формирование отчета о сканировании устройства в задании аудита настроек и уязвимостей. Отчет формируется по результатам выполненных проверок на устройстве с использованием правил аудита настроек и уязвимостей, которые выбраны в параметрах задания. Отчет содержит детальную информацию о выполненных проверках и об использованных правилах аудита настроек и уязвимостей.

Для формирования отчета сканирование устройства должно иметь один из следующих статусов: **Завершено**, **Отменено** или **Ошибка**.

Чтобы запустить формирование отчета:

1. Выберите раздел **Аудит безопасности**.
2. На вкладке **Аудит настроек и уязвимостей** выберите задание, в котором выполнено нужное сканирование устройства.

   В правой части окна веб-интерфейса появится область деталей.
3. В области деталей перейдите на вкладку **Запуски**.
4. Выберите нужное сканирование и нажмите на кнопку **Получить отчет** в появившейся области деталей сканирования (кнопка отсутствует, если получение отчета невозможно в текущий момент).

   Kaspersky Industrial CyberSecurity for Networks запустит процесс формирования отчета.

Вы перейдете на вкладку **Сформированные отчеты** в разделе **Отчеты**. В таблице сформированных отчетов отобразится отчет аудита настроек и уязвимостей. После успешного завершения формирования отчета вы можете экспортировать сформированный отчет в файл.

Обнаружение проблем безопасности в протоколах шифрования

Если в промышленной сети используются протоколы шифрования (например, SSL/TLS или SSH), Kaspersky Industrial CyberSecurity for Networks может обнаруживать различные проблемы безопасности в сетевых взаимодействиях по этим протоколам. При обнаружении проблемы безопасности программа регистрирует соответствующее событие. Для регистрации таких событий используется системный тип события обнаружения системных команд.

Программа регистрирует события при обнаружении следующих проблем безопасности в протоколе шифрования:

- Использование устаревшей версии протокола шифрования (DEPRECATED PROTOCOL VERSION).
- Использование слабого алгоритма шифрования (WEAK CIPHER TYPE).
- Использование просроченного сертификата (OUTDATED CERTIFICATE).
- Использование самоподписанного сертификата (SELF-SIGNED CERTIFICATE).

Перечень обнаруживаемых проблем безопасности зависит от протокола шифрования.

После установки программы используются исходные модули обработки протоколов, обеспечивающие поддержку ограниченного количества протоколов шифрования. Вы можете обновлять модули обработки протоколов, устанавливая обновления.

Для обнаружения проблем безопасности в протоколах шифрования не требуется добавлять параметры контроля процесса для устройств. Программа анализирует протоколы шифрования во всех обнаруженных взаимодействиях.

Для регистрации событий обнаружения проблем безопасности должны выполняться следующие условия:

- Контроль взаимодействий включен в режиме наблюдения с применением технологии Контроль системных команд.
- В таблице разрешающих правил отсутствуют правила для технологии Контроль системных команд, которые блокируют регистрацию событий о проблемах безопасности в протоколах шифрования. Например, программа может автоматически создать такие правила в режиме обучения контроля взаимодействий. Если такие правила присутствуют в таблице разрешающих правил, рекомендуется их выключить.

Типовые действия при работе с таблицами данных

Этот раздел содержит информацию о типовых действиях при работе с таблицами данных, которые отображаются в разделах веб-интерфейса программы (такие, как таблица устройств, таблица событий или таблица тегов).

Просмотр таблицы данных

Этот раздел содержит информацию о функциях, доступных при просмотре таблиц данных в разделах веб-интерфейса программы.

Настройка отображения и порядка столбцов

В зависимости от раздела веб-интерфейса программы вы можете включать и выключать отображение определенных данных в таблице, а также настраивать состав и порядок отображаемых столбцов.

Чтобы настроить параметры отображения таблицы:

1. Откройте окно для настройки отображения таблицы по значку .
2. Если в таблице можно включать и выключать отображение определенных данных (например, отображение устраненных и принятых рисков в таблице устройств), настройте эти параметры в верхней части окна.
3. В блоке **Отображаемые столбцы** установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр.
4. Если вы хотите изменить порядок отображения столбцов, выделите название столбца, который требуется разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

Выбранные столбцы отобразятся в таблице в указанном вами порядке.

Фильтрация по стандартным периодам времени

Чтобы отфильтровать таблицу данных по стандартным периодам времени:

1. При работе с таблицей в разделе веб-интерфейса программы откройте раскрывающийся список **Период**, **Период обнаружения** или **Период запуска** в панели инструментов.
2. В раскрывающемся списке выберите один из стандартных периодов (например, **Последние 24 часа**).

В таблице отобразятся данные за указанный вами период.

Фильтрация по заданному периоду времени

Чтобы отфильтровать таблицу данных по заданному периоду времени:

1. В таблице раздела веб-интерфейса программы откройте раскрывающийся список **Период**, **Период обнаружения** или **Период запуска** в панели инструментов.
2. В раскрывающемся списке выберите **Задать период**.

   Справа от раскрывающегося списка отобразятся начальная и конечная дата и время периода фильтрации.

3. Нажмите на дату начала или окончания периода.

   Откроется календарь.

4. В календаре задайте дату начальной и конечной границ периода фильтрации. Для этого выберите дату в календаре (при этом будет указано текущее время) или введите значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс. Если указывать дату и время конечной границы периода фильтрации не требуется, вы можете не выбирать дату или удалить текущее значение.

5. Нажмите на кнопку **OK**.

В таблице отобразятся данные за указанный вами период.

Фильтрация по столбцам

Чтобы отфильтровать таблицу по столбцу:

1. В таблице раздела веб-интерфейса программы нажмите на значок фильтрации в нужном столбце.

   Откроется окно фильтрации.

2. Используя элементы интерфейса в окне фильтрации, настройте параметры нужным образом. Особенности настройки фильтрации в некоторых столбцах приведены ниже.

3. Нажмите на кнопку **OK**.

При наличии в окне фильтрации параметра **Комплексный**

С помощью параметра **Комплексный** вы можете указать несколько значений, объединенных логическим оператором И. Для добавления значений разных типов используйте кнопку **Добавить условие (И)**.

При наличии столбца для групп устройств

1. В окне фильтрации нажмите на значок в правой части поля, чтобы указать группу.

   Появится окно **Выбор группы в дереве**.

2. В дереве групп устройств выберите нужную группу и нажмите на кнопку **Выбрать**.

   Путь к выбранной группе отобразится в поле в окне фильтрации.

При наличии столбца для рисков, связанных с устройствами

1. В окне фильтрации с помощью переключателя **Исключить устройства с рисками** настройте отображение устройств в таблице:

   - Если вы хотите просматривать только устройства без рисков, включите переключатель.

   - Если вы хотите просматривать устройства с рисками и настроить параметры фильтрации по рискам, выключите переключатель.

2. При необходимости настройте параметры фильтрации устройств с рисками с помощью следующих элементов управления:

   - **Оценка рисков** – позволяет задать диапазон значений оценок рисков для отображения устройств с рисками, у которых значение оценки входит в указанный диапазон.

   - **Статус** – группирует кнопки для включения и выключения фильтрации по статусам рисков (кнопки отображаются, если в параметрах отображения таблицы устройств установлен флажок **Отображать устраненные и принятые риски**).

При наличии столбца **Протокол** с отображением поддерживаемых протоколов прикладного уровня

1. В окне фильтрации в поле **Протоколы** укажите нужный протокол. Для этого начните вводить название протокола и выберите нужный протокол в раскрывающемся списке (список подходящих протоколов автоматически раскрывается при изменении значения в поле **Протоколы**).

2. При необходимости отсортируйте открывшийся список протоколов с помощью ссылки **Сортировка**.

3. Если вы хотите добавить еще один протокол, нажмите на кнопку **Добавить протокол** и укажите другой протокол в открывшемся поле.

4. Если вы хотите удалить один из указанных протоколов, в окне фильтрации нажмите на значок . Вы также можете удалить все указанные протоколы с помощью ссылки **Фильтр по умолчанию** в окне фильтрации.

При наличии столбца **Протокол** с отображением всех поддерживаемых протоколов в виде дерева стека протоколов

1. В окне фильтрации настройте отображение нужных элементов дерева с помощью кнопок **+** и **-** рядом с названиями протоколов, которые содержат протоколы следующих уровней.

   В столбцах таблицы представлена следующая информация:

   - **Протокол** – название протокола в дереве стека протоколов.
   - **EtherType** – номер протокола следующего уровня внутри протокола Ethernet (если протокол имеет заданный номер). Отображается в десятичном формате.
   - **IP-номер** – номер протокола следующего уровня внутри протокола IP (если протокол имеет заданный номер). Указывается только для протоколов, входящих в структуру протокола IP. Отображается в десятичном формате.

2. При необходимости воспользуйтесь поисковой строкой над таблицей, чтобы найти нужные протоколы.
3. В списке протоколов установите флажки напротив протоколов, по которым вы хотите выполнить фильтрацию.

   Если вы устанавливаете или снимаете флажок для протокола, который содержит вложенные протоколы, то для всех вложенных протоколов также автоматически устанавливаются или снимаются флажки.

При поддерживаемой возможности фильтрации по значениям в ячейках таблицы

1. Выберите нужные элементы в таблице данных.
2. Наведите курсор мыши на ячейку нужного столбца одного из выбранных элементов.
3. По правой кнопке мыши откройте контекстное меню.
4. В контекстном меню выберите команду, которая позволяет показать все элементы с этим значением или с этими значениями параметра.

Режимы фильтрации событий в инцидентах

При фильтрации таблицы событий в режиме отображения структур инциденты, удовлетворяющие параметрам фильтрации, могут быть представлены в следующих вариантах:

- со всеми вложенными элементами;
- только с теми вложенными элементами, которые также удовлетворяют заданным параметрам фильтрации.

Вы можете выбрать нужный вариант представления инцидентов с помощью флажка **Показывать вложенные при фильтрации** при настройке таблицы.

Поиск в таблице

В таблице раздела веб-интерфейса программы вы можете найти нужные элементы с помощью поля **Поиск <тип отображаемых элементов>**. Поле отображается в правой части раздела.

Поиск может выполняться не по всем столбцам таблицы.

Сброс заданных параметров фильтрации и поиска

В таблице раздела веб-интерфейса программы вы можете сбросить заданные параметры фильтрации и поиска с помощью кнопки **Фильтр по умолчанию** в панели инструментов. Кнопка отображается, если заданы параметры фильтрации или поиска.

Сортировка таблицы

Чтобы отсортировать таблицу:

1. В таблице раздела веб-интерфейса программы нажмите на заголовок столбца, по которому вы хотите выполнить сортировку.

   Заголовки столбцов, в которых поддерживается сортировка, отображаются в виде ссылок.

2. Если сортировка выполняется по столбцу, в котором отображаются значения разных типов (например, столбец **Сторона 1** в разделе **Риски**), в раскрывающемся списке заголовка столбца выберите параметр, по которому будет выполняться сортировка.

3. Если требуется отсортировать таблицу по нескольким столбцам, нажмите на клавишу **SHIFT** и, удерживая ее нажатой, нажмите на заголовки столбцов, по которым нужно выполнить сортировку.

Таблица будет отсортирована по выбранному столбцу. При сортировке по нескольким столбцам строки таблицы сортируются в соответствии с последовательностью выбора столбцов. Рядом с заголовками столбцов, по которым выполнена сортировка, отображаются значки, показывающие текущий порядок сортировки: по возрастанию или по убыванию значений.

Выбор элементов в таблице данных

В таблице раздела веб-интерфейса программы вы можете выбирать отображаемые элементы для просмотра сведений и для работы с этими элементами. При выборе элемента в таблице появляется область деталей в правой части окна веб-интерфейса.

Чтобы выбрать нужные элементы в таблице, выполните одно из следующих действий:

- Если вы хотите выбрать один элемент, установите флажок на левой границе строки с этим элементом или выберите строку таблицы с помощью мыши.

- Если вы хотите выбрать несколько элементов, установите флажки на левой границе строк с нужными элементами или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**.

- Если вы хотите выбрать все элементы, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:

  - выберите любой элемент в таблице и нажмите комбинацию клавиш **CTRL+A**;

  - установите флажок в заголовке левого крайнего столбца таблицы.

При выборе нескольких элементов в правом верхнем углу страницы веб-интерфейса могут отображаться данные об их количестве. Точное количество выбранных элементов отображается вплоть до достижения некоторого предела (например, до 2000 элементов). Если выбрано больше элементов, точное количество не отображается (в приведенном примере будет отображаться строка `2000+`). Если в таблице не выполнялся выбор элементов, в правом верхнем углу страницы отображаются данные об общем количестве элементов в таблице данных.

В заголовке левого крайнего столбца таблицы отображается флажок выбора элементов. В зависимости от количества выбранных элементов флажок может быть в одном из следующих состояний:

- ☐ – в таблице не выполнялся выбор всех элементов, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбран один элемент или могут быть выбраны несколько элементов с помощью флажков на левой границе строк или с использованием клавиш **CTRL** или **SHIFT**.
- ☑ – в таблице выбраны все элементы, удовлетворяющие текущим параметрам фильтрации и поиска.
- ▣ – в таблице были выбраны все элементы, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых элементов были сняты флажки. Это состояние сохраняется и в случае, если флажки сняты для всех элементов, выбранных таким способом (из-за того, что количество выбранных элементов может измениться).

Если выбраны все элементы, удовлетворяющие параметрам фильтрации и поиска, количество выбранных элементов может автоматически изменяться. Например, в результате действий пользователя программы в другом сеансе подключения или при появлении (обнаружении) новых элементов. Рекомендуется настраивать параметры фильтрации и поиска таким образом, чтобы в выборку попали только нужные элементы.

Переходы к связанным элементам в других разделах веб-интерфейса

Элементы в одних разделах веб-интерфейса программы (в частности, в таблицах данных) могут быть связаны с элементами в других разделах, содержащих таблицы или структуры данных. Например, события могут быть связаны с устройствами или с рисками. При работе с такими элементами вы можете переходить к связанным элементам в других разделах для просмотра подробных сведений.

Чтобы просмотреть сведения о связанных элементах:

1. Выберите те элементы, для которых вы хотите просмотреть сведения о связанных элементах.

   Рекомендуется выбрать ограниченное количество элементов (до 200). При выборе большого количества элементов возможность перехода для просмотра связанных элементов может быть недоступна.

2. Откройте раскрывающийся список **Показать связи** в панели инструментов.

3. В раскрывающемся списке выберите нужный тип элементов (например, **Устройства**).

   Откроется раздел, который содержит элементы выбранного типа (в приведенном примере – таблица устройств в разделе **Активы**). Для отображения связанных элементов будет применена соответствующая фильтрация.

Экспорт данных из таблицы в файл

В таблицах данных некоторых разделов веб-интерфейса программы предусмотрены возможности экспорта данных в файлы следующих форматов:

- Формат CSV.

  При экспорте в этот формат в файле сохраняется информация из столбцов, отображаемых в таблице в текущий момент. Также в этом файле могут сохраняться некоторые данные, не отображаемые в таблице (например, дополнительные поля и параметры контроля процесса в сведениях об устройствах).

- Формат JSON.

  При экспорте в этот формат в файле сохраняются все данные об элементах в таблице, включая служебную информацию из базы данных (например, сведения о событиях, с которыми связаны устройства).

Экспорт можно выполнять для всех элементов, удовлетворяющих текущим параметрам фильтрации и поиска, или выборочно для элементов, отображаемых в таблице.

Чтобы экспортировать данные обо всех элементах, удовлетворяющих текущим параметрам фильтрации и поиска:

1. По ссылке **Экспорт** в панели инструментов над таблицей данных откройте меню и выберите пункт с нужным форматом файла: CSV или JSON.

2. Если для экспорта доступен выбор варианта сохранения дополнительных параметров, в появившемся окне установите флажки для тех параметров, которые вы хотите экспортировать.

   Запустится процесс формирования файла.

3. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:

   a. Нажмите на кнопку в меню веб-интерфейса программы.

      Откроется список фоновых операций.

   b. Дождитесь завершения операции формирования файла.

   c. Нажмите на кнопку **Скачать файл**.

Браузер сохранит загруженный файл. В зависимости от параметров, заданных в браузере, на экране может появиться окно для изменения пути и имени сохраняемого файла.

Чтобы экспортировать данные о выбранных элементах:

1. Выберите элементы, информацию о которых вы хотите экспортировать в файл.

2. По правой кнопке мыши откройте контекстное меню одного из выбранных элементов.

3. В контекстном меню выберите пункт с нужным форматом файла: CSV или JSON.

4. Если для экспорта доступен выбор варианта сохранения дополнительных параметров, в появившемся окне установите флажки для тех параметров, которые вы хотите экспортировать.

   Запустится процесс формирования файла.

5. Если формирование файла занимает длительное время (более 15 секунд), выполните действия пункта 3, описанные в процедуре экспорта данных обо всех элементах.

Обновление таблицы данных

Отображаемые данные в таблице раздела веб-интерфейса программы могут быть изменены на Сервере в то время, когда вы просматриваете таблицу (например, при регистрации новых элементов или если данные изменены в другом сеансе подключения к Серверу). В некоторых таблицах поддерживается автоматическое обновление данных.

Чтобы включить или выключить автоматическое обновление данных в таблице,

в панели инструментов над таблицей данных используйте переключатель **Обновление**.

Управление программой через Kaspersky Security Center

Этот раздел содержит информацию о настройке взаимодействия программы с Kaspersky Security Center и об использовании функций Kaspersky Security Center для работы с Kaspersky Industrial CyberSecurity for Networks. С помощью Kaspersky Security Center вы можете выполнять следующие действия:

- добавлять лицензионный ключ в Kaspersky Industrial CyberSecurity for Networks;
- загружать в Kaspersky Industrial CyberSecurity for Networks обновления баз и программных модулей;
- просматривать события Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования Kaspersky Security Center;
- контролировать состояние безопасности АСУ ТП в Консоли администрирования или в SCADA-системе;
- удаленно подключаться к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks;
- использовать расширенные возможности централизованного контроля систем с Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console;
- использовать технологию единого входа для аутентификации пользователей Kaspersky Security Center Web Console при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс.

Состав доступных для выполнения действий зависит от возможностей используемой версии Kaspersky Security Center. Вы можете просмотреть сведения об основных возможностях различных версий Kaspersky Security Center в справочной системе для Kaspersky Security Center.

Для взаимодействия Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center должны быть выполнены следующие условия:

- При установке Сервера Kaspersky Industrial CyberSecurity for Networks добавлена функциональность взаимодействия программы с Kaspersky Security Center.
- В Kaspersky Industrial CyberSecurity for Networks включена и настроена функциональность взаимодействия с Kaspersky Security Center.
- В Kaspersky Security Center Windows установлен плагин управления Kaspersky Industrial CyberSecurity for Networks.
- В Kaspersky Security Center Web Console установлен веб-плагин управления Kaspersky Industrial CyberSecurity for Networks (для использования в Kaspersky Security Center Linux, а также для реализации расширенных возможностей централизованного контроля и использования технологии единого входа в Kaspersky Security Center Windows).

- Компьютер, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, включен в группу администрирования Kaspersky Security Center (в группу **Управляемые устройства** или в ее подгруппу). Вы можете переместить устройство в группу администрирования при работе в Консоли администрирования на основе MMC или при регистрации Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console.

- Доступны определенные порты и протоколы, используемые для подключений и взаимодействий Сервера Kaspersky Industrial CyberSecurity for Networks с Сервером администрирования Kaspersky Security Center и Kaspersky Security Center Web Console.

Включение и настройка функциональности взаимодействия с Kaspersky Security Center

После добавления в программу функциональности взаимодействия с Kaspersky Security Center эта функциональность по умолчанию выключена.

Чтобы включить и настроить функциональность взаимодействия программы с Kaspersky Security Center:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.

2. Выберите раздел **Параметры** → **Kaspersky Security Center**.

3. Включите взаимодействие с Kaspersky Security Center с помощью переключателя **Включено**.

4. В блоке **Параметры коннектора** настройте параметры **Kaspersky Security Center Connector**:

   - IP-адрес / сетевое имя компьютера с Сервером администрирования Kaspersky Security Center.

   - SSL-порт для подключения.

   - Максимальное количество передаваемых событий за сутки, начиная с нуля часов в часовом поясе Сервера Kaspersky Industrial CyberSecurity for Networks.

5. В блоке **Параметры веб-плагина для Kaspersky Security Center Web Console** настройте параметры подключений из Kaspersky Security Center Web Console:

   - Имя пользователя Kaspersky Industrial CyberSecurity for Networks, который будет указан в записях журнала аудита при регистрации действий из Kaspersky Security Center Web Console.

   - IP-адрес / сетевое имя веб-сервера.

   - IP-адрес / сетевое имя сервера REST API.

6. Нажмите на кнопку **Применить**.

Добавление лицензионного ключа в Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center

Вы можете добавить лицензионный ключ в Kaspersky Industrial CyberSecurity for Networks с использованием функциональности автоматического распространения лицензионных ключей в Kaspersky Security Center. Лицензионный ключ, полученный таким способом, обрабатывается в Kaspersky Industrial CyberSecurity for Networks так же, как и при добавлении ключа вручную в программе.

Автоматическое распространение лицензионного ключа работает, если выполнены все условия для взаимодействия Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center.

Для распространения лицензионного ключа вам нужно добавить его в хранилище Сервера администрирования Kaspersky Security Center. Вы можете добавить лицензионный ключ в хранилище при работе в Консоли администрирования на основе MMC или при работе в Kaspersky Security Center Web Console. Для добавления используйте файл лицензионного ключа.

После добавления лицензионного ключа в хранилище Сервера администрирования вы можете создать задачу распространения лицензионного ключа при работе в Консоли администрирования на основе MMC или при работе в Kaspersky Security Center Web Console.

Получение обновлений с Сервера администрирования Kaspersky Security Center

Вы можете использовать Сервер администрирования Kaspersky Security Center в качестве источника обновлений баз и программных модулей Kaspersky Industrial CyberSecurity for Networks. Такой способ получения обновлений может потребоваться, например, для загрузки обновлений с серверов "Лаборатории Касперского" при отсутствии доступа в интернет на компьютере Сервера Kaspersky Industrial CyberSecurity for Networks.

Сценарий подготовки к использованию Сервера администрирования Kaspersky Security Center в качестве источника обновлений состоит из следующих этапов:

1. **Создание задачи в Kaspersky Security Center для загрузки обновлений в хранилище Сервера администрирования**

   Вы можете создать задачу при работе в Консоли администрирования на основе MMC или при работе в Kaspersky Security Center Web Console.

2. **Выбор Сервера администрирования в качестве источника обновлений в Kaspersky Industrial CyberSecurity for Networks**

   При подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс вы можете выбрать Сервер администрирования Kaspersky Security Center в качестве источника обновлений при запуске обновления вручную и/или при настройке автоматического обновления.

Мониторинг событий через Kaspersky Security Center

В Kaspersky Security Center сведения о событиях Kaspersky Industrial CyberSecurity for Networks отображаются в следующих столбцах таблицы событий:

- **Время** или **Событие произошло** – время регистрации события Kaspersky Industrial CyberSecurity for Networks в часовом поясе компьютера, на котором установлен Kaspersky Security Center.
- **Устройство** – имя управляемого устройства в Kaspersky Security Center (компьютер, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks).
- **Событие** – название типа события в Kaspersky Security Center, заданное для событий Kaspersky Industrial CyberSecurity for Networks.
- **Описание** – заголовок и краткое описание события Kaspersky Industrial CyberSecurity for Networks.
- **Группа** или **Группа администрирования** – имя группы администрирования, к которой относится компьютер Сервера Kaspersky Industrial CyberSecurity for Networks, в папке **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
- **Программа** – название программы (Kaspersky Industrial CyberSecurity for Networks).
- **Номер версии** – номер версии программы.
- **Уровень важности** или **Уровень критичности** – уровень важности события в соответствии с типизацией Kaspersky Security Center.
- **Зарегистрировано** или **Событие зарегистрировано** – время регистрации события в базе данных Kaspersky Security Center.

Значения параметров событий, передаваемых из Kaspersky Industrial CyberSecurity for Networks, отображаются согласно параметрам локализации Kaspersky Industrial CyberSecurity for Networks. Язык локализации Kaspersky Security Center для этих параметров не учитывается.

Если событие Kaspersky Industrial CyberSecurity for Networks содержит сведения о нескольких сетевых взаимодействиях, это событие преобразуется в отдельные элементы таблицы событий Kaspersky Security Center. Таким образом, для каждого сетевого взаимодействия, указанного в событии Kaspersky Industrial CyberSecurity for Networks, создаются отдельные события в Kaspersky Security Center.

Чтобы события Kaspersky Industrial CyberSecurity for Networks отображались в таблице событий Kaspersky Security Center:

1. Убедитесь, что в Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center установлены необходимые компоненты.
2. Убедитесь, что на компьютере Сервера Kaspersky Industrial CyberSecurity for Networks доступен порт для подключения к компьютеру с Kaspersky Security Center.

3. При настройке параметров политики Агента администрирования в Kaspersky Security Center включите сохранение нужных событий в базе данных Сервера администрирования и задайте срок хранения событий.

   Вы можете настроить регистрацию и хранение событий в параметрах политики Агента администрирования при работе в Консоли администрирования на основе MMC или при работе в Kaspersky Security Center Web Console.

4. В Kaspersky Industrial CyberSecurity for Networks настройте передачу событий через коннектор **Kaspersky Security Center Connector**.

При регистрации в Kaspersky Industrial CyberSecurity for Networks указанных типов событий эти события также будут отображаться в таблице событий Kaspersky Security Center.

Типы событий в Kaspersky Security Center для событий Kaspersky Industrial CyberSecurity for Networks

Для получения событий Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center используется фиксированный набор типов событий. Типы событий в Kaspersky Security Center соответствуют определенным типам событий в Kaspersky Industrial CyberSecurity for Networks и в зависимости от уровней важности событий могут регистрироваться в качестве инцидентов Kaspersky Security Center (см. таблицу ниже).

Типы событий в Kaspersky Security Center для получения событий Kaspersky Industrial CyberSecurity for Networks

Отображаемое имя типа события	Код типа события в Kaspersky Security Center	Регистрация в качестве инцидента Kaspersky Security Center	Соответствующий код типа события в Kaspersky Industrial CyberSecurity for Networks
Достигнуто максимальное количество переданных событий	32769	да, с уровнем важности *Предупреждение*	–
Тестовое событие (DPI)	32770	нет	4000000001
Тестовое событие (NIC)	32771	нет	4000000002
Тестовое событие (IDS)	32772	нет	4000000003
Тестовое событие (AM)	32773	нет	4000000004
Обнаружено неразрешенное сетевое взаимодействие	32774	нет	4000002601
Обнаружена системная команда	32775	только события с уровнем важности *Критические события*	4000002602
Отсутствует трафик на точке мониторинга	32776	нет	4000002700
Обнаружена аномалия в протоколе TCP: подмена содержимого в перекрывающихся TCP-сегментах	32777	нет	4000002701
Нарушено правило контроля процесса	32778	только события с уровнем важности *Критические события*	4000002900
Сработало правило обнаружения вторжений из системного набора правил	32779	нет	4000003000
Сработало правило обнаружения вторжений из пользовательского набора правил	32780	нет	4000003001
Обнаружены признаки ARP-спуфинга в ARP-ответах	32781	да	4000004001
Обнаружены признаки ARP-спуфинга в ARP-запросах	32782	да	4000004002

Отображаемое имя типа события	Код типа события в Kaspersky Security Center	Регистрация в качестве инцидента Kaspersky Security Center	Соответствующий код типа события в Kaspersky Industrial CyberSecurity for Networks
Обнаружено новое устройство в сети	32783	да	4000005003
Обнаружены новые параметры устройства	32784	нет	4000005004
Обнаружен конфликт IP-адреса	32785	да	4000005005
Обнаружена активность устройства со статусом Неиспользуемое	32786	нет	4000005006
Обнаружен новый IP-адрес устройства	32787	да	4000005007
Обнаружен новый MAC-адрес устройства	32788	да	4000005010
Добавлен MAC-адрес устройству	32789	нет	4000005008
Добавлен IP-адрес устройству	32790	нет	4000005009
Контроль проектов ПЛК: обнаружено чтение неизвестного блока из ПЛК	32791	нет	4000005200
Контроль проектов ПЛК: обнаружено чтение известного блока из ПЛК	32792	нет	4000005201
Контроль проектов ПЛК: обнаружена запись нового блока в ПЛК	32793	нет	4000005202
Контроль проектов ПЛК: обнаружена запись известного блока в ПЛК	32794	нет	4000005203
Контроль проектов ПЛК: обнаружено чтение неизвестного проекта из ПЛК	32795	нет	4000005204
Контроль проектов ПЛК: обнаружено чтение известного проекта из ПЛК	32796	нет	4000005205
Контроль проектов ПЛК: обнаружена запись нового проекта в ПЛК	32797	нет	4000005206
Контроль проектов ПЛК: обнаружена запись известного проекта в ПЛК	32798	нет	4000005207
Обнаружена аномалия в протоколе IP: конфликт данных при сборке IP-пакета	32799	нет	4000005100
Обнаружена аномалия в протоколе IP: превышение размера фрагментированного IP-пакета	32800	нет	4000005101
Обнаружена аномалия в протоколе IP: размер начального фрагмента IP-пакета меньше ожидаемого	32801	нет	4000005102
Обнаружена аномалия в протоколе IP: несоответствие фрагментов IP-пакета (mis-associated fragments)	32802	нет	4000005103
Зарегистрировано событие по правилу корреляции	32803	только события с уровнем важности *Критические события*	8000000001
Событие от внешней системы	32804	только события с уровнем важности *Критические события*	4000005400
Обнаружен другой MAC-адрес устройства в полученных данных от EPP-приложения	32805	да	4000005011
Обнаружена новая адресная информация устройства в полученных данных от EPP-приложения	32806	да	4000005012
Обнаружен конфликт в адресах устройств после получения данных от EPP-приложения	32807	да	4000005013

Отображаемое имя типа события	Код типа события в Kaspersky Security Center	Регистрация в качестве инцидента Kaspersky Security Center	Соответствующий код типа события в Kaspersky Industrial CyberSecurity for Networks
Добавлена подсеть по данным от EPP-приложения	32808	да	4000005014
Обнаружено изменение оборудования устройства	32809	нет	4000005015

Соответствие уровней важности событий в Kaspersky Security Center

Уровни важности событий в Kaspersky Security Center соответствуют уровням критичности событий Kaspersky Industrial CyberSecurity for Networks (см. таблицу ниже). Для уровней критичности событий Kaspersky Industrial CyberSecurity for Networks приведены соответствующие названия уровней важности, которые использовались в предыдущих версиях программы.

Соответствие уровней важности событий

Уровни важности событий Kaspersky Security Center	Уровни критичности событий Kaspersky Industrial CyberSecurity for Networks
Информационное сообщение	*Низкий* (*Информационные*)
Предупреждение	*Средний* (*Важные*)
Критическое событие	*Высокий* (*Критические*)

Контроль состояния безопасности АСУ ТП: Kaspersky Security Center и SCADA

Kaspersky Industrial CyberSecurity for Networks может передавать данные о состоянии безопасности АСУ ТП в Kaspersky Security Center. Для передачи данных в Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center должны быть установлены необходимые компоненты.

Если настроена передача данных о состоянии безопасности АСУ ТП в Kaspersky Security Center, вы можете настроить в SCADA-системе получение соответствующей информации из Kaspersky Security Center.

Чтобы настроить получение и отображение состояния безопасности АСУ ТП в SCADA-системе:

1. На компьютере с Kaspersky Security Center установите Kaspersky Security Gateway.

   Вы можете найти подробную информацию об установке и настройке Kaspersky Security Gateway в документе *Руководство администратора Kaspersky Security Gateway*.

2. В SCADA-системе создайте элемент управления, отображающий состояние компьютера с Kaspersky Industrial CyberSecurity for Networks.

3. Настройте созданный элемент управления на получение данных по протоколу OPC DA 2.0 или IEC 60870-5-104.

   Способ настройки элемента управления описан в документе *Руководство администратора Kaspersky Security Gateway*.

Подключение к компьютеру Сервера из Kaspersky Security Center

Вы можете удаленно подключаться к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks из Консоли администрирования Kaspersky Security Center. Для этого требуется использовать Консоль администрирования на основе MMC. Подключение выполняется с помощью системы удаленного доступа к рабочему столу Virtual Network Computing (далее VNC).

Для подключения вам необходимо установить и настроить следующие компоненты VNC:

- VNC-сервер. Устанавливается на компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks. При настройке VNC-сервера нужно задать пароль для VNC-подключения. Дополнительно, если на этом компьютере включен межсетевой экран, нужно открыть порты для протоколов VNC и SSH.

- VNC-клиент. Устанавливается на компьютере с Консолью администрирования Kaspersky Security Center.

Чтобы получить доступ к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве Консоли администрирования Kaspersky Security Center в папке **Управляемые устройства** выберите группу администрирования, содержащую компьютер, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.

3. В рабочей области на вкладке **Устройства** выберите компьютер, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, и в контекстном меню компьютера выберите пункт **Внешние инструменты → VNC**.

   По умолчанию инструмент VNC отсутствует в списке внешних инструментов. Для добавления инструмента в контекстном меню компьютера выберите пункт **Внешние инструменты → Настроить внешние инструменты**. В окне **Внешние инструменты** нажмите на кнопку **Добавить** и укажите следующие значения параметров:

   - В поле **Имя инструмента** введите произвольное имя инструмента (например, `VNC`).

   - В поле **Имя исполняемого файла** введите полный путь к исполняемому файлу VNC-клиента (например, `C:\Program Files\TightVNC\tvnviewer.exe`).

   - В поле **Рабочая папка** введите полный путь к рабочей папке VNC-клиента (например, `C:\Program Files\TightVNC\`).

   - В поле **Командная строка** введите значение: `<A>:<P>`.

   - Установите флажок **Создать туннель для заданного ниже TCP-порта** и введите номер VNC-порта на VNC-сервере (например, если VNC-сервер использует экран :3, введите номер VNC-порта `5903`).

4. После запуска внешнего инструмента VNC отобразится окно с запросом пароля. Введите пароль для VNC-подключения.

В открывшемся окне отобразится рабочий стол компьютера, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.

Централизованный контроль систем с Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (далее также Web Console) предоставляет расширенные возможности для централизованного контроля состояния безопасности информационных систем, в которых функционирует Kaspersky Industrial CyberSecurity for Networks. Расширенные возможности реализуются при использовании веб-плагина управления Kaspersky Industrial CyberSecurity for Networks (далее также "веб-плагин") в Web Console. Для использования веб-плагина его требуется установить на компьютер с установленной программой Kaspersky Security Center Web Console.

После установки и настройки веб-плагина вы можете выполнять в Web Console следующие действия:

- мониторинг систем, контролируемых Kaspersky Industrial CyberSecurity for Networks, а также Серверов Kaspersky Industrial CyberSecurity for Networks, с помощью веб-виджетов, предназначенных только для работы с Kaspersky Industrial CyberSecurity for Networks;
- поиск устройств и событий по базам данных выбранных Серверов Kaspersky Industrial CyberSecurity for Networks с использованием различных критериев фильтрации;
- размещение компонентов и групп компонентов Kaspersky Industrial CyberSecurity for Networks на картах (географических, схематических или на любых других изображениях) для распределения объектов по территориальному признаку;
- группирование компонентов Kaspersky Industrial CyberSecurity for Networks в организационных единицах (далее также "подразделениях"), логически разграничивающих зоны контроля и/или развертывания Kaspersky Industrial CyberSecurity for Networks.

При использовании перечисленных функций вы можете выполнять быстрые переходы из Web Console для подключения к нужным Серверам Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс. При этом если используется технология единого входа, то при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks не обязательно указывать учетные данные только тех пользователей, которые созданы в Kaspersky Industrial CyberSecurity for Networks. Аутентификацию могут также пройти пользователи, выполнившие вход в Web Console.

О веб-плагине управления Kaspersky Industrial CyberSecurity for Networks

Веб-плагин управления Kaspersky Industrial CyberSecurity for Networks обеспечивает взаимодействие программы с Kaspersky Security Center Web Console.

Веб-плагин по умолчанию не установлен в Web Console. В отличие от плагина управления для Консоли администрирования Kaspersky Security Center, который устанавливается на рабочее место администратора, веб-плагин требуется установить на компьютер с установленной программой Kaspersky Security Center Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Web Console в браузере.

Вы можете просмотреть список установленных веб-плагинов в интерфейсе Web Console: **Параметры консоли → Веб-плагины**.

Установка веб-плагина

Вы можете установить веб-плагин следующими способами:

- Установить веб-плагин из списка доступных дистрибутивов в Web Console.

  Для установки веб-плагина выберите дистрибутив веб-плагина в интерфейсе Web Console: **Параметры консоли → Веб-плагины**. Список доступных дистрибутивов обновляется автоматически после выпуска новых версий программ "Лаборатории Касперского".

- Загрузить дистрибутив в Web Console из стороннего источника.

  Для установки веб-плагина добавьте ZIP-архив дистрибутива веб-плагина в интерфейсе Web Console: **Параметры консоли → Веб-плагины**. Дистрибутив веб-плагина можно загрузить, например, на веб-сайте "Лаборатории Касперского". Для локальной версии программы вам также нужно загрузить текстовый файл, содержащий сигнатуру.

- Загрузить дистрибутив из списка доступных дистрибутивов, плагинов и патчей для Kaspersky Security Center.

  Для установки веб-плагина выберите дистрибутив веб-плагина в интерфейсе Web Console: **Операции → Программы "Лаборатории Касперского" → Текущие версии программ**. Список доступных дистрибутивов обновляется автоматически после выпуска новых версий программ "Лаборатории Касперского".

Обновление веб-плагина

При появлении новой версии веб-плагина Web Console отобразит уведомление *Доступны обновления для используемых плагинов*. Вы можете перейти к обновлению версии веб-плагина из уведомления Web Console. Также вы можете проверить наличие обновлений веб-плагина вручную в интерфейсе Web Console (**Параметры консоли → Веб-плагины**). Предыдущая версия веб-плагина будет автоматически удалена во время обновления.

При обновлении веб-плагина сохраняются уже существующие элементы (например, добавленные виджеты или изображения карт). Новые параметры элементов, реализующие новые функции Kaspersky Industrial CyberSecurity for Networks, будут иметь значения по умолчанию.

Вы можете обновить веб-плагин следующими способами:

- Обновить веб-плагин в списке веб-плагинов в онлайн-режиме.

  Для обновления веб-плагина требуется выбрать дистрибутив веб-плагина Kaspersky Industrial CyberSecurity for Networks в интерфейсе Web Console и запустить обновление (**Параметры консоли** → **Веб-плагины**). Web Console проверит наличие обновлений на серверах "Лаборатории Касперского" и загрузит необходимые обновления.

- Обновить веб-плагин из файла.

  Для обновления веб-плагина требуется выбрать ZIP-архив дистрибутива веб-плагина Kaspersky Industrial CyberSecurity for Networks в интерфейсе Web Console: **Параметры консоли** → **Веб-плагины**. Дистрибутив веб-плагина можно загрузить, например, на веб-сайте "Лаборатории Касперского". Для локальной версии программы вам также нужно загрузить текстовый файл, содержащий сигнатуру.

  Вы можете обновить веб-плагин только до более новой версии. Обновить веб-плагин до более старой версии невозможно.

Сценарий подготовки к использованию технологии единого входа (SSO)

При совместной работе с Kaspersky Security Center вы можете использовать технологию единого входа (англ. Single Sign-On, SSO), которая позволяет пользователям, выполнившим вход в Kaspersky Security Center Web Console, пройти аутентификацию при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс. Таким образом, любые учетные записи пользователей, которым доступна возможность работы с Kaspersky Security Center Web Console (включая пользователей Active Directory®), могут подключаться к Серверу со своими учетными данными.

Технология единого входа доступна для использования с Kaspersky Industrial CyberSecurity for Networks в совместимых версиях Kaspersky Security Center:

Сценарий подготовки к использованию технологии единого входа состоит из следующих этапов:

1. **Проверка и выполнение необходимых условий для взаимодействия Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center**

   На этом этапе вам нужно проверить выполнение всех условий для взаимодействия Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center. Если какое-то из условий не выполнено, обеспечьте выполнение этого условия. Например, если в Kaspersky Industrial CyberSecurity for Networks не настроена функциональность взаимодействия с Kaspersky Security Center, то включите и настройте эту функциональность.

2. **Включение и настройка компонента Kaspersky Security Center Web Console Identity and Access Manager (IAM)**

   На этом этапе выполняется сценарий включения компонента Identity and Access Manager, описанный в справочной системе Kaspersky Security Center.

   При настройке компонента IAM рекомендуется указывать DNS-имя компьютера в качестве сетевого имени устройства только в том случае, если компьютер доступен по этому имени с компьютера Сервера Kaspersky Industrial CyberSecurity for Networks. Если доступ возможен только по IP-адресу, укажите этот IP-адрес вместо DNS-имени.

3. **Регистрация Сервера Kaspersky Industrial CyberSecurity for Networks в качестве клиента для компонента IAM**

На этом этапе компонент IAM обнаруживает Серверы Kaspersky Industrial CyberSecurity for Networks, готовые для регистрации в качестве клиентов для этого компонента. Вам нужно принять запрос на регистрацию Сервера после его обнаружения. Обнаруженные и зарегистрированные клиенты компонента IAM отображаются в таблице, которую вы можете открыть в Kaspersky Security Center Web Console в разделе **Параметры консоли** → **Интеграция** → **Identity and Access Manager**. Для того, чтобы зарегистрировать Серверы, откройте таблицу по ссылке **Параметры** в блоке с информацией о зарегистрированных клиентах, установите флажки рядом с нужными Серверами и нажмите на кнопку **Одобрить**.

После того, как вы подтвердили регистрацию клиента компонента IAM, вам нужно дождаться завершения процесса подготовки к работе. По окончании синхронизации между компонентом IAM и клиентом, для этого клиента отобразится статус готовности к работе. Если статус не изменился, нажмите на кнопку **Обновить**.

Компоненту IAM требуется некоторое время на обнаружение клиентов и синхронизацию с ними. В зависимости от загруженности Сервера администрирования Kaspersky Security Center и Сервера Kaspersky Industrial CyberSecurity for Networks, выполнение этих действий может занять до 15 минут.

4. **Подготовка пользователей с правами доступа для подключения к Kaspersky Industrial CyberSecurity for Networks**

   На этом этапе вам нужно предоставить права доступа пользователям Kaspersky Security Center, соответствующие ролям Администратор и Оператор Kaspersky Industrial CyberSecurity for Networks. Вы можете использовать для этого как уже существующие учетные записи, так и новые учетные записи пользователей и групп, созданные для предоставления только таких прав.

В результате выполнения сценария в Kaspersky Industrial CyberSecurity for Networks появится возможность подключения к Серверу через веб-интерфейс с учетными данными пользователей Kaspersky Security Center. Для этого вы можете использовать кнопку **Пользователь Kaspersky Security Center** на странице ввода учетных данных веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Если при настройке параметров подключений из Kaspersky Security Center Web Console было указано полное доменное имя (FQDN) для веб-сервера и сервера REST API, то при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks с использованием технологии единого входа пользователю также нужно указывать это имя в адресной строке браузера.

Предоставление пользователям Kaspersky Security Center прав доступа, соответствующих ролям пользователей в Kaspersky Industrial CyberSecurity for Networks

Для использования технологии единого входа и для выполнения некоторых действий в Web Console пользователям Kaspersky Security Center требуется предоставить права доступа, соответствующие ролям пользователей в Kaspersky Industrial CyberSecurity for Networks. Вы можете предоставлять такие права после того, как на Сервер администрирования Kaspersky Security Center загружен файл, содержащий конфигурацию модели управления доступом на основе ролей (RBAC) для Kaspersky Industrial CyberSecurity for Networks.

Конфигурация загружается автоматически при установке веб-плагина управления Kaspersky Industrial CyberSecurity for Networks. Если конфигурация загружена на Сервер администрирования, то в папке %ProgramData%\KasperskyLab\adminkit\1093\dat\rbac\ сохраняется файл KICS4NET_<номер версии файла>.conf. При отсутствии в указанной папке файла KICS4NET_<номер версии файла>.conf создайте и настройте задачу Загрузка обновлений в хранилище Сервера администрирования. В качестве источника обновлений вы можете выбрать Серверы обновлений "Лаборатории Касперского".

После загрузки конфигурации RBAC для Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center появляется возможность назначения пользователям прав, соответствующих ролям Администратор и Оператор Kaspersky Industrial CyberSecurity for Networks.

Ролям пользователей в Kaspersky Industrial CyberSecurity for Networks соответствуют следующие права доступа в Kaspersky Security Center из функциональной области **Kaspersky Industrial CyberSecurity for Networks: Общий функционал**:

- **Чтение** – соответствует роли Оператор.
- **Запись** – соответствует роли Администратор.

Совместно с этими правами пользователям должны быть назначены все права из функциональной области **Сервер администрирования Kaspersky Security Center: Общий функционал: Базовая функциональность** (в эту функциональную область входят права **Чтение**, **Запись**, **Выполнение** и **Выполнение операций с выборками устройств**).

Если права доступа назначаются пользователям с помощью ролей Kaspersky Security Center, то для роли пользователя требуется добавить в область действия роли группу администрирования, содержащую компьютер, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks. Для этого в мастере назначения роли выберите группу администрирования **Управляемые устройства** на странице **Определение области**.

Веб-виджеты для мониторинга систем и Серверов Kaspersky Industrial CyberSecurity for Networks

Для мониторинга систем, контролируемых Kaspersky Industrial CyberSecurity for Networks, а также Серверов Kaspersky Industrial CyberSecurity for Networks, вы можете использовать веб-виджеты. Kaspersky Security Center Web Console отображает веб-виджеты в панели мониторинга (раздел **Мониторинг и отчеты** → **Панель мониторинга**). По умолчанию веб-виджеты для Kaspersky Industrial CyberSecurity for Networks не отображаются в панели мониторинга. Вы можете добавить нужные веб-виджеты после установки веб-плагина управления Kaspersky Industrial CyberSecurity for Networks.

Веб-виджеты позволяют разместить в панели мониторинга следующую информацию:

- Статусы KICS for Networks.
- Критические события KICS for Networks.
- Устройства, требующие внимания в KICS for Networks.
- Актуальные события KICS for Networks.
- Карта размещения KICS for Networks.
- Информация о Серверах KICS for Networks.

Веб-виджеты для Kaspersky Industrial CyberSecurity for Networks входят в категорию **Другие** в списке доступных веб-виджетов Web Console.

Отображаемая информация на веб-виджетах автоматически обновляется каждые 1–2 минуты. Если данные от Сервера не поступают дольше двух минут, устаревшие данные на веб-виджетах скрываются. При необходимости вы можете обновить отображаемую информацию вручную, используя соответствующий пункт в меню веб-виджета.

Веб-виджет Статусы KICS for Networks

В веб-виджете **Статусы KICS for Networks** для Web Console отображается количественное соотношение текущих статусов, присвоенных Серверам Kaspersky Industrial CyberSecurity for Networks. Сведения представлены только по актуальным статусам (если нет Серверов с каким-либо статусом, этот статус не отображается в веб-виджете).

Для Серверов в веб-виджете предусмотрены следующие статусы:

- *Критический*.

  Этот статус присваивается Серверу, если выполняется хотя бы одно из следующих условий:

  - на Сервере есть сообщения о нарушении работы программы;
  - в базе данных Сервера есть необработанные события с уровнем важности *Критические*;
  - есть устройства со статусом *Неразрешенное*;
  - закончился срок годности лицензионного ключа.

- *Важный*.

  Этот статус присваивается Серверу, если не выполняются условия для присвоения статуса *Критический* и при этом выполняется хотя бы одно из следующих условий:

  - на Сервере есть сообщения о некритических сбоях;
  - в базе данных Сервера есть необработанные события с уровнем важности *Важные*;
  - до окончания срока годности лицензионного ключа осталось менее 14 дней.

- *OK*.

  Этот статус присваивается Серверу во всех остальных случаях (при доступности Сервера и поступлении данных для обработки).

- *Обслуживание*.

  Этот статус присваивается Серверу, если программа находится в режиме обслуживания (например, во время импорта политики безопасности).

Если статус Сервера определить невозможно, для этого Сервера отображается статус *Неизвестно*.

По умолчанию в веб-виджете отображается информация о статусах всех Серверов в группах администрирования Kaspersky Security Center. Если данные от какого-либо Сервера не поступают дольше двух минут, устаревшая информация перестает отображаться в веб-виджете. При необходимости в меню параметров веб-виджета вы можете выбрать Серверы, данные от которых должны отображаться в веб-виджете.

Веб-виджет Критические события KICS for Networks

В веб-виджете **Критические события KICS for Networks** для Web Console отображается количественное соотношение необработанных событий с уровнем критичности *Высокий* (соответствует уровню важности *Критические*) на Серверах Kaspersky Industrial CyberSecurity for Networks. Для каждого Сервера, в базе данных которого есть необработанные события с уровнем критичности *Высокий* (соответствует уровню важности *Критические*), указывается количество этих событий.

Цветовое оформление представленных данных в веб-виджете не соответствует уровням важности событий. Цвета на диаграмме веб-виджета используются только для визуального разделения событий от разных Серверов.

По умолчанию в веб-виджете отображается информация по данным, поступающим в Web Console от всех Серверов в группах администрирования Kaspersky Security Center. Если данные от какого-либо Сервера не поступают дольше двух минут, устаревшая информация перестает отображаться в веб-виджете. При необходимости в меню параметров веб-виджета вы можете выбрать Серверы, данные от которых должны отображаться в веб-виджете.

Веб-виджет Устройства, требующие внимания в KICS for Networks

В веб-виджете **Устройства, требующие внимания в KICS for Networks** для Web Console отображается информация об устройствах, которые были обнаружены программами Kaspersky Industrial CyberSecurity for Networks и требуют внимания. Устройство считается требующим внимания в любом из следующих случаев:

- состояние безопасности устройства отличается от *OK*;
- устройство имеет статус *Неразрешенное*.

При наличии устройств, требующих внимания, веб-виджет содержит следующую информацию:

- Количество устройств, требующих внимания, в каждой категории. Эти данные отображаются в верхней части веб-виджета под значками категорий устройств. Количество отображаемых категорий зависит от свободного пространства в виджете. Если категорий для отображения больше, вы можете открыть окно со всеми категориями с помощью значка **Показать все**.
- Список категорий устройств, требующих внимания. Эти данные отображаются в средней части виджета. Для каждой категории в списке отображается следующая информация:
  - Строка со значком категории и комментарием. В конце строки отображается ссылка с количеством устройств, требующих внимания.
  - Строка с графическими элементами, представляющими устройства. Строка отображается, если достаточно свободного пространства в виджете. Если устройств, требующих внимания, больше чем отображаемых графических элементов в строке, то справа отображается количество скрытых устройств в формате `+<количество устройств>`.

По умолчанию в веб-виджете отображается информация по данным, поступающим в Web Console от всех Серверов в группах администрирования Kaspersky Security Center. Если данные от какого-либо Сервера не поступают дольше двух минут, устаревшая информация перестает отображаться в веб-виджете. При необходимости в меню параметров веб-виджета вы можете выбрать Серверы, данные от которых должны отображаться в веб-виджете.

Графические элементы устройств

Графические элементы, представляющие устройства, содержат следующую информацию:

- Имя устройства.
- Статус устройства. Отображается в виде значка, если устройство имеет статус *Неразрешенное*.
- Состояние безопасности устройства. Отображается в виде цветной линии на левой границе графического элемента. Цвет линии соответствует состояниям *OK*, *Важное* или *Критическое*.

Графические элементы отображаются в следующем порядке:

1. Устройства с присвоенным статусом *Неразрешенное*.
2. Устройства, имеющие состояние безопасности *Критическое*.
3. Устройства, имеющие состояние безопасности *Важное*.

Переходы из веб-виджета

С помощью элементов интерфейса веб-виджета вы можете выполнять переходы для отображения подробных сведений об устройствах. Для этого предусмотрены возможности, описанные ниже.

Переход для вывода сведений о выбранном устройстве в таблице устройств на странице веб-интерфейса Сервера

В веб-виджете **Устройства, требующие внимания в KICS for Networks** нажмите на графический элемент, представляющий нужное устройство.

В окне браузера на новой вкладке откроется страница веб-интерфейса Сервера Kaspersky Industrial CyberSecurity for Networks. В названии открывшейся вкладки будет указано имя Сервера, заданное во время начальной настройки программы после установки.

Если используется технология единого входа и пользователь Web Console обладает правами для подключения к этому Серверу, то доступ к веб-интерфейсу Сервера будет предоставлен без запроса учетных данных пользователя.

На странице веб-интерфейса Сервера автоматически откроется раздел **Активы** с таблицей устройств. В таблице будет применена фильтрация по идентификатору устройства.

Переход для вывода сведений об устройствах выбранной категории в таблице результатов поискового запроса в Web Console

Чтобы вывести сведения обо всех устройствах выбранной категории,

в верхней части веб-виджета **Устройства, требующие внимания в KICS for Networks** нажмите на значок нужной категории.

Откроется раздел Web Console **KICS for Networks** → **Поиск** с таблицей результатов поискового запроса по устройствам. В таблице будет применена фильтрация по следующим критериям:

- выбранная категория устройств;
- все Серверы, данные от которых учитываются в веб-виджете.

Чтобы вывести сведения обо всех устройствах, требующих внимания и относящихся к определенной категории,

в списке категорий с устройствами, требующими внимания, воспользуйтесь ссылкой с количеством устройств нужной категории.

Откроется раздел Web Console **KICS for Networks** → **Поиск** с таблицей результатов поискового запроса по устройствам. В таблице будет применена фильтрация по следующим критериям:

- выбранная категория устройств;
- все Серверы, данные от которых учитываются в веб-виджете;
- признак устройств, требующих внимания.

Переход для вывода сведений обо всех устройствах в таблице результатов поискового запроса в Web Console

Выполните переход по ссылке **Показать все устройства** в веб-виджете **Устройства, требующие внимания в KICS for Networks**.

Откроется раздел Web Console **KICS for Networks** → **Поиск** с таблицей результатов поискового запроса по устройствам. В таблице будет применена фильтрация по всем Серверам, данные от которых учитываются для отображения в веб-виджете.

Веб-виджет Актуальные события KICS for Networks

В веб-виджете **Актуальные события KICS for Networks** для Web Console отображается общая информация о событиях Kaspersky Industrial CyberSecurity for Networks, имеющих наиболее поздние значения даты и времени последнего появления.

Веб-виджет содержит следующую информацию:

- Гистограмма событий за выбранный период. Эти данные отображаются в верхней части веб-виджета. Гистограмма отображает распределение событий по уровням критичности (уровням важности).
- Список зарегистрированных событий. Эти данные отображаются в средней части веб-виджета. События отсортированы по дате и времени последнего появления.

По умолчанию в веб-виджете отображается информация по данным, поступающим в Web Console от всех Серверов в группах администрирования Kaspersky Security Center. Если данные от какого-либо Сервера не поступают дольше двух минут, устаревшая информация перестает отображаться в веб-виджете. При необходимости в меню параметров веб-виджета вы можете выбрать Серверы, данные от которых должны отображаться в веб-виджете.

Гистограмма событий

На гистограмме распределения событий столбцы соответствуют суммарному количеству событий за каждый интервал времени. Внутри столбцов цветом обозначены уровни важности событий. Уровням важности соответствуют следующие цвета:

- Синий цвет – события с уровнем критичности *Низкий* (соответствует уровню важности *Информационные*).
- Желтый цвет – события с уровнем критичности *Средний* (соответствует уровню важности *Важные*).
- Красный цвет – события с уровнем критичности *Высокий* (соответствует уровню важности *Критические*).

При наведении курсора мыши на столбец гистограммы во всплывающем окне отображаются сведения о количестве событий по уровням критичности (уровням важности).

Длительность интервалов времени зависит от выбранного периода для отображения. Для построения гистограммы вы можете выбрать в меню веб-виджета один из следующих периодов:

- 1 час. Этот период делится на интервалы по одной минуте.
- 12 часов, 24 часа. Эти периоды делятся на интервалы по одному часу.
- 7 дней. Этот период делится на интервалы по 12 часов.

Список событий

Количество отображаемых элементов списка событий ограничено размером веб-виджета.

Для каждого события представлены следующие сведения:

- заголовок события;
- уровень критичности (уровень важности);
- имя компьютера с установленным Сервером Kaspersky Industrial CyberSecurity for Networks.

Переходы из веб-виджета

С помощью элементов интерфейса веб-виджета вы можете выполнять переходы для отображения подробных сведений о событиях. Для этого предусмотрены возможности, описанные ниже.

Переход для вывода сведений о выбранном событии в таблице событий на странице веб-интерфейса Сервера

В веб-виджете **Актуальные события KICS for Networks** нажмите на нужное событие.

В окне браузера на новой вкладке откроется страница веб-интерфейса Сервера Kaspersky Industrial CyberSecurity for Networks. В названии открывшейся вкладки будет указано имя Сервера, заданное во время начальной настройки программы после установки.

Если используется технология единого входа и пользователь Web Console обладает правами для подключения к этому Серверу, то доступ к веб-интерфейсу Сервера будет предоставлен без запроса учетных данных пользователя.

На странице веб-интерфейса Сервера автоматически откроется раздел **События** с таблицей событий. В таблице будет применена фильтрация по идентификатору выбранного события. Также для фильтрации будет задан период от даты и времени регистрации события до текущего момента (без указания конечной границы периода).

Переход для вывода сведений обо всех событиях за выбранный период в таблице результатов поискового запроса в Web Console

Выполните переход по ссылке **Показать все события** в веб-виджете **Актуальные события KICS for Networks**.

Откроется раздел Web Console **KICS for Networks** → **Поиск** с таблицей результатов поискового запроса по событиям. В таблице будет применена фильтрация по следующим критериям:

- текущий выбранный период для построения гистограммы в веб-виджете;
- все Серверы, данные от которых учитываются в веб-виджете.

Веб-виджет Карта размещения KICS for Networks

В веб-виджете **Карта размещения KICS for Networks** для Web Console отображается карта территориального распределения подразделений, в которых сгруппированы компоненты Kaspersky Industrial CyberSecurity for Networks. В веб-виджете используется уменьшенная копия общей карты, которая доступна в разделе Web Console **KICS for Networks** → **Карта**.

Подразделения на карте обозначены значками, цвета которых зависят от статусов подразделений. Для подразделений предусмотрены следующие статусы:

- *Критический*.

  Этот статус присваивается подразделению, если оно содержит хотя бы один Сервер со статусом *Критический*.

- *Важный*.

  Этот статус присваивается подразделению, если оно содержит хотя бы один Сервер со статусом *Важный* и не содержит Серверы со статусами *Критический* или *Неизвестно*.

- *OK*.

  Этот статус присваивается подразделению, если оно содержит хотя бы один Сервер со статусом *OK* и не содержит Серверы со статусами *Критический*, *Важный*, *Неизвестно* или *Обслуживание*.

- *Обслуживание*.

  Этот статус присваивается подразделению, если оно содержит хотя бы один Сервер со статусом *Обслуживание* и не содержит Серверы со статусами *Критический*, *Важный* или *Неизвестно*.

- *Без мониторинга*.

  Этот статус присваивается подразделению, если оно содержит только Серверы со статусом *Без мониторинга*.

- *Неизвестно*.

  Этот статус присваивается подразделению, если оно содержит хотя бы один Сервер со статусом *Неизвестно* и не содержит Серверы со статусом *Критический*.

- *Без Серверов*.

  Этот статус присваивается подразделению, если оно не содержит Серверы.

Вы можете перейти к общей карте в разделе Web Console **KICS for Networks** → **Карта**, нажав на любую часть карты, кроме значков подразделений.

Вы можете перейти к карте подразделения, нажав на значок этого подразделения в веб-виджете.

Веб-виджет Информация о Серверах KICS for Networks

В веб-виджете **Информация о Серверах KICS for Networks** для Web Console отображаются основные сведения о текущем состоянии Серверов Kaspersky Industrial CyberSecurity for Networks.

Для каждого Сервера представлены следующие сведения:

- **Имя Сервера** – имя, под которым Сервер представлен в Kaspersky Security Center (имя устройства в группе администрирования).

- **Функции** – информация о текущем состоянии функций защиты в Kaspersky Industrial CyberSecurity for Networks. Возможны следующие значения:

  - **Все ВКЛ** – работают все технологии и методы, предназначенные для постоянного использования, а также включены все созданные точки мониторинга.

  - **Не все ВКЛ** – некоторые функции защиты выключены или включены в режиме обучения, либо включены не все точки мониторинга.

- **Статус** – текущий статус Сервера.

- **Сообщение программы** – последнее сообщение программы или дополнительные сведения о статусе.

По умолчанию в веб-виджете отображается информация по данным, поступающим в Web Console от всех Серверов в группах администрирования Kaspersky Security Center. При необходимости в меню параметров веб-виджета вы можете выбрать Серверы, данные от которых должны отображаться в веб-виджете.

По ссылке с именем Сервера вы можете открыть в браузере страницу веб-интерфейса выбранного Сервера Kaspersky Industrial CyberSecurity for Networks. В названии открывшейся вкладки браузера будет указано имя Сервера, заданное во время начальной настройки программы после установки.

Если используется технология единого входа и пользователь Web Console обладает правами для подключения к этому Серверу, то доступ к веб-интерфейсу Сервера будет предоставлен без запроса учетных данных пользователя.

Поиск устройств и событий по базам данных Серверов Kaspersky Industrial CyberSecurity for Networks

В Kaspersky Security Center Web Console вы можете создавать запросы для получения выборок устройств и событий с помощью веб-плагина Kaspersky Industrial CyberSecurity for Networks. По таким запросам поиск выполняется непосредственно в базах данных Серверов Kaspersky Industrial CyberSecurity for Networks. В этом состоит основное отличие от функциональности поиска с использованием штатных средств получения выборок устройств и событий в Web Console (например, в разделах **Устройства** → **Выборки устройств** и **Мониторинг и отчеты** → **Выборки событий**). При использовании штатных средств в Web Console выполняется поиск устройств и событий в базе данных Сервера администрирования.

Для настройки параметров поисковых запросов к Серверам Kaspersky Industrial CyberSecurity for Networks и для вывода результатов поиска используется раздел Web Console **KICS for Networks** → **Поиск**. Поисковые запросы требуется формировать отдельно для поиска устройств или для поиска событий.

Серверы Kaspersky Industrial CyberSecurity for Networks обрабатывают поисковые запросы и предоставляют сведения по ним со следующими ограничениями:

- количество возвращаемых элементов, удовлетворяющих поисковому запросу (устройств или событий) от каждого Сервера – не более 200;
- предоставляются только те сведения, по которым может выполняться поиск – например, результаты поиска устройств будут содержать MAC- и IP-адреса устройств, но не будут содержать сведения о моделях и производителях устройств.

Во всех случаях, когда вам требуется получить полную информацию о найденных устройствах или событиях, вы можете перейти на страницу веб-интерфейса Сервера с помощью элементов интерфейса в разделе **KICS for Networks** → **Поиск**. На странице веб-интерфейса Сервера автоматически откроется соответствующий раздел (**Активы** или **События**), в котором будет применена фильтрация с критериями поискового запроса или полученных результатов.

Настройка параметров для поиска устройств

Вы можете настроить параметры запроса для поиска устройств вручную или использовать автоматически применяемые критерии фильтрации при переходах из веб-виджета **Устройства, требующие внимания в KICS for Networks**.

Для настройки параметров вручную вам нужно открыть вкладку **Устройства** в области деталей поискового запроса.

*Чтобы открыть вкладку **Устройства** в области деталей поискового запроса:*

1. Перейдите в раздел Web Console **KICS for Networks** → **Поиск**.
2. Выполните одно из следующих действий:
   - Если в текущем сеансе не создавался поисковый запрос и в разделе не отображается таблица результатов поискового запроса, нажмите на кнопку **Найти события или устройства**.
   - Если в текущем сеансе был создан поисковый запрос и в разделе отображается таблица результатов поискового запроса, нажмите на кнопку **Поиск** в панели инструментов.

     На кнопке **Поиск** отображается количество критериев фильтрации (заданных параметров) текущего поискового запроса.
3. В области деталей поискового запроса перейдите на вкладку **Устройства**.

После настройки параметров вы можете начать поиск устройств в базах данных Серверов с помощью кнопки **Найти**.

Для поиска устройств вы можете настроить следующие параметры в поисковом запросе:

- **Имя** – имя, под которым устройство представлено в таблице устройств Сервера Kaspersky Industrial CyberSecurity for Networks. Имя требуется указывать полностью.
- **Серверы** – имена, под которыми Серверы представлены в Kaspersky Security Center (имена устройств в группах администрирования).
- **Адреса** – MAC- и/или IP-адреса устройств. Адреса требуется указывать полностью.
- **Статусы** – статусы устройств, определяющие разрешение активности устройств в промышленной сети.
- **Состояния безопасности** – состояния безопасности устройств, определяемые по наличию связанных с устройством событий и актуальных уязвимостей.
- **Категории** – названия категорий, определяющих функциональное назначение устройств.
- **Требующие внимания** – наличие или отсутствие признака устройства, требующего внимания.

Вы можете сбросить заданные параметры в поисковом запросе с помощью кнопки **Очистить фильтры**.

Настройка параметров для поиска событий

Вы можете настроить параметры запроса для поиска событий вручную или использовать автоматически применяемые критерии фильтрации при переходе из веб-виджета **Актуальные события KICS for Networks**.

Для настройки параметров вручную вам нужно открыть вкладку **События** в области деталей поискового запроса.

*Чтобы открыть вкладку **События** в области деталей поискового запроса:*

1. Перейдите в раздел Web Console **KICS for Networks → Поиск**.
2. Выполните одно из следующих действий:
   - Если в текущем сеансе не создавался поисковый запрос и в разделе не отображается таблица результатов поискового запроса, нажмите на кнопку **Найти события или устройства**.
   - Если в текущем сеансе был создан поисковый запрос и в разделе отображается таблица результатов поискового запроса, нажмите на кнопку **Поиск** в панели инструментов.

     На кнопке **Поиск** отображается количество критериев фильтрации (заданных параметров) текущего поискового запроса.
3. В области деталей поискового запроса перейдите на вкладку **События**.

После настройки параметров вы можете начать поиск событий в базах данных Серверов с помощью кнопки **Найти**.

Для поиска событий вы можете настроить следующие параметры в поисковом запросе:

- **Заголовок** – заголовок, заданный для типа события в Kaspersky Industrial CyberSecurity for Networks. Заголовок требуется указывать полностью.
- **Серверы** – имена, под которыми Серверы представлены в Kaspersky Security Center (имена устройств в группах администрирования).
- **Последнее появление** – период для фильтрации событий по дате и времени последнего появления.
- **Отправитель** – адресная информация (MAC-, IP-адреса или номера портов) отправителей сетевых пакетов.
- **Получатель** – адресная информация (MAC-, IP-адреса или номера портов) получателей сетевых пакетов.
- **Технологии** – значки и названия технологий, которые использовались для регистрации событий.
- **Важность** – значки и названия уровней критичности (уровней важности) событий.

Вы можете сбросить заданные параметры в поисковом запросе с помощью кнопки **Очистить фильтры**.

Просмотр таблицы с результатами поискового запроса

Таблица результатов поискового запроса по устройствам или событиям отображается в разделе Web Console **KICS for Networks → Поиск**. В таблице представлены сведения, по которым может выполняться поиск устройств или поиск событий. Найденные элементы сгруппированы по Серверам, к которым они относятся.

При просмотре таблицы вы можете использовать следующие функции:

- Фильтрация результатов поиска.

  Для фильтрации таблицы результатов поискового запроса вы можете воспользоваться следующими элементами интерфейса в панели инструментов:

  - **Состояния безопасности**.

    Этот фильтр доступен в таблице результатов поискового запроса по устройствам. С помощью кнопок фильтра можно скрыть найденные устройства в зависимости от их состояний безопасности.

  - **Важность**.

    Этот фильтр доступен в таблице результатов поискового запроса по событиям. С помощью кнопок фильтра можно скрыть найденные события в зависимости от их уровней критичности (уровней важности).

  - **Технологии**.

    Этот фильтр доступен в таблице результатов поискового запроса по событиям. С помощью кнопок фильтра можно скрыть найденные события в зависимости от технологий регистрации событий.

  - **Серверы**.

    Этот раскрывающийся список позволяет выбрать Серверы для отображения результатов поискового запроса.

- Обновление результатов поиска.

  Сведения об устройствах или событиях могут быть изменены на Серверах в то время, когда вы просматриваете таблицу результатов поискового запроса. Информация о дате и времени последней загрузки результатов отображается в поле **Последнее обновление**.

  Вы можете повторить поисковый запрос для обновления результатов с помощью кнопки **Обновить** в панели инструментов.

- Переходы для вывода сведений на страницах веб-интерфейса Серверов.

  Выполните одно из следующих действий:

  - для получения подробных сведений об одном из найденных элементов откройте страницу веб-интерфейса соответствующего Сервера по ссылке с именем устройства или с заголовком события;

  - для получения сведений обо всех найденных элементах, удовлетворяющих параметрам поискового запроса, откройте страницу веб-интерфейса соответствующего Сервера по ссылке **Перейти к Серверу**.

  В окне браузера на новой вкладке откроется страница веб-интерфейса Сервера Kaspersky Industrial CyberSecurity for Networks. В названии открывшейся вкладки будет указано имя Сервера, заданное во время начальной настройки программы после установки.

  Если используется технология единого входа и пользователь Web Console обладает правами для подключения к этому Серверу, то доступ к веб-интерфейсу Сервера будет предоставлен без запроса учетных данных пользователя.

  На странице веб-интерфейса Сервера автоматически откроется соответствующий раздел с таблицей устройств или таблицей событий. В таблице будет применена фильтрация с соответствующими критериями.

Размещение компонентов Kaspersky Industrial CyberSecurity for Networks на картах

Веб-плагин позволяет создавать в Kaspersky Security Center Web Console карты расположения Серверов и сенсоров Kaspersky Industrial CyberSecurity for Networks. Вы можете использовать карты для распределения этих объектов по территориальному признаку и для контроля их состояния в удобном для вас отображении.

Для работы с картами предназначен раздел Web Console **KICS for Networks → Карта**. В этом разделе отображаются следующие карты (в каждый момент только одна выбранная карта):

- Общая карта. На этой карте представлены подразделения (организационные единицы для группирования компонентов Kaspersky Industrial CyberSecurity for Networks). Серверы и сенсоры на этом уровне не отображаются.

- Карты подразделений. Каждая карта подразделения содержит компоненты программы (Серверы и сенсоры), которые включены в это подразделение.

Подразделения и компоненты программы представлены на картах в виде значков с названиями этих объектов. Длинные названия сокращаются до первых символов.

Фоновые изображения карт могут отображаться в разном масштабе. Для управления масштабом вы можете использовать панель инструментов, которая отображается в верхней части раздела Web Console **KICS for Networks → Карта**.

После перехода из общей карты на карту подразделения вы можете вернуться на общую карту с помощью кнопки с изображением стрелки.

Возможности создания карт и распределения на них объектов доступны только пользователям Kaspersky Security Center, которым предоставлены права доступа для роли Администратор в Kaspersky Industrial CyberSecurity for Networks. По окончании настройки пользователи с правами доступа для роли Оператор могут наблюдать за состоянием объектов с помощью карт как в разделе Web Console **KICS for Networks → Карта**, так и в веб-виджете **Карта размещения KICS for Networks**.

Формирование списка подразделений для общей карты

Этот раздел содержит информацию о функциях, доступных для формирования списка подразделений для общей карты.

При работе с общей картой в разделе Web Console **KICS for Networks → Карта** вы можете сформировать список подразделений, с помощью которых будут логически разграничены зоны контроля и/или развертывания Kaspersky Industrial CyberSecurity for Networks. В созданные подразделения вы сможете добавить нужные Серверы и выполнять действия с этими Серверами и их сенсорами внутри подразделений.

Максимальное количество подразделений – 100.

Формировать список подразделений могут только пользователи Kaspersky Security Center, которым предоставлены права доступа, соответствующие роли Администратор в Kaspersky Industrial CyberSecurity for Networks.

Добавление подразделения

Чтобы добавить подразделение для общей карты:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.
2. Выберите раздел **KICS for Networks** → **Карта**.
3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.
4. Нажмите на кнопку **Добавить**.

   Появится окно для ввода названия подразделения.
5. Введите название подразделения.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Название подразделения должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 255 символов;
   - не совпадает с названием другого подразделения.

   В окне **Подразделения** появится строка с названием нового подразделения.
6. Если строка с названием подразделения не появилась в списке, это может быть связано с действием фильтра по статусам подразделений. В этом случае включите отображение всех подразделений с помощью кнопки **Все статусы** или отображение подразделений без Серверов с помощью кнопки **Без Серверов**.
7. Добавьте подразделение на общую карту. Для этого наведите курсор на строку с названием подразделения и нажмите на кнопку .
8. Переместите значок подразделения в нужное место карты.

Переименование подразделения

Чтобы переименовать подразделение для общей карты:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.
2. Выберите раздел **KICS for Networks** → **Карта**.
3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.

4. Если строка с названием нужного подразделения не отображается в списке, это может быть связано с действием фильтра по статусам подразделений. В этом случае включите отображение всех подразделений с помощью кнопки **Все статусы** или нажмите на кнопку с названием того статуса, который присвоен нужному подразделению.

5. Наведите курсор на строку с названием подразделения и нажмите на кнопку .

   Появится окно для ввода названия подразделения.

6. Введите название подразделения.

   Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   Название подразделения должно удовлетворять следующим требованиям:

   - начинается и заканчивается любым символом, кроме пробела;
   - содержит до 255 символов;
   - не совпадает с названием другого подразделения.

Удаление подразделения

Чтобы удалить подразделение для общей карты:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.

2. Выберите раздел **KICS for Networks** → **Карта**.

3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.

4. Если строка с названием нужного подразделения не отображается в списке, это может быть связано с действием фильтра по статусам подразделений. В этом случае включите отображение всех подразделений с помощью кнопки **Все статусы** или нажмите на кнопку с названием того статуса, который присвоен нужному подразделению.

5. Наведите курсор на строку с названием подразделения и нажмите на кнопку ×.

6. В окне запроса на подтверждение операции нажмите на кнопку **OK**.

Замена фонового изображения для карты

После создания карты используется фоновое изображение по умолчанию. Вы можете заменить фоновое изображение на любое другое по вашему усмотрению. Например, для общей карты можно использовать изображение географической карты какой-либо территории, а для карт подразделений загрузить схемы расположения оборудования в цехах или на площадках.

В качестве фона для карт вы можете использовать изображения, загружаемые из файлов форматов JPG или PNG. Максимальный размер файла для загрузки – 50 МБ. Минимальный размер изображения в файле – 600x600 пикселей. После загрузки нового изображения удаляется старое изображение и сбрасывается положение всех объектов на карте.

Выполнять замену фонового изображения на картах могут только пользователи Kaspersky Security Center, которым предоставлены права доступа, соответствующие роли Администратор в Kaspersky Industrial CyberSecurity for Networks.

Чтобы заменить фоновое изображение для общей карты:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.
2. Выберите раздел **KICS for Networks** → **Карта**.
3. Нажмите на кнопку **Заменить изображение**.

   Появится окно с предложением перетащить файл с изображением или выбрать файл.
4. Загрузите файл удобным для вас способом.

Чтобы заменить фоновое изображение для карты подразделения:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.
2. Выберите раздел **KICS for Networks** → **Карта**.
3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.
4. Нажмите на строку с названием нужного подразделения.

   Откроется карта подразделения.
5. Нажмите на кнопку **Заменить изображение**.

   Появится окно с предложением перетащить файл с изображением или выбрать файл.
6. Загрузите файл удобным для вас способом.

Формирование списков Серверов в подразделениях

Этот раздел содержит информацию о функциях, доступных для формирования списков Серверов в подразделениях.

На картах созданных подразделений в разделе Web Console **KICS for Networks** → **Карта** вам нужно сформировать списки Серверов, которые относятся к этим подразделениям в соответствии с логикой разграничения зон контроля и/или развертывания Kaspersky Industrial CyberSecurity for Networks. Вместе с Серверами в те же подразделения включаются и сенсоры, которые связаны с этими Серверами.

Каждый Сервер Kaspersky Industrial CyberSecurity for Networks может быть включен только в одно подразделение. До тех пор, пока Сервер не включен в какое-либо подразделение, он находится в списке **Вне подразделений**.

Формировать списки Серверов в подразделениях могут только пользователи Kaspersky Security Center, которым предоставлены права доступа, соответствующие роли Администратор в Kaspersky Industrial CyberSecurity for Networks.

Добавление Сервера в подразделение

Чтобы добавить Сервер в подразделение:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.
2. Выберите раздел **KICS for Networks** → **Карта**.
3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.
4. Нажмите на строку с названием нужного подразделения.

   Откроется карта подразделения.
5. Нажмите на кнопку **Показать список Серверов**.

   В правой части раздела появится окно с названием подразделения.
6. Перейдите на вкладку **Вне подразделений**.
7. Если строка с нужным Сервером не отображается в списке, это может быть связано с действием фильтра по статусам Серверов. В этом случае включите отображение всех Серверов с помощью кнопки **Все статусы** или нажмите на кнопку с названием того статуса, который присвоен нужному Серверу.
8. Наведите курсор на строку с именем Сервера и нажмите на кнопку +.

   Строка Сервера перестанет отображаться на вкладке **Вне подразделений**.
9. Перейдите на вкладку **В подразделении**.
10. Если строка с добавленным Сервером не отображается в списке, это может быть связано с действием фильтра по статусам Серверов. В этом случае включите отображение всех Серверов с помощью кнопки **Все статусы** или нажмите на кнопку с названием того статуса, который присвоен Серверу.
11. Добавьте Сервер на карту подразделения. Для этого наведите курсор на строку с именем Сервера и нажмите на кнопку .

    После выполнения действия изменится яркость значка в кнопке.
12. Если с Сервером связаны сенсоры и вы хотите включить отображение этих сенсоров, раскройте список **Сенсоры** и добавьте их с помощью кнопок .
13. Переместите значки объектов в нужные места карты.

Удаление Сервера из подразделения

Чтобы удалить Сервер из подразделения:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.
2. Выберите раздел **KICS for Networks** → **Карта**.

3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.

4. Нажмите на строку с названием нужного подразделения.

   Откроется карта подразделения.

5. Нажмите на кнопку **Показать список Серверов**.

   В правой части раздела появится окно с названием подразделения.

6. Перейдите на вкладку **В подразделении**.

7. Если строка с нужным Сервером не отображается в списке, это может быть связано с действием фильтра по статусам Серверов. В этом случае включите отображение всех Серверов с помощью кнопки **Все статусы** или нажмите на кнопку с названием того статуса, который присвоен нужному Серверу.

8. Наведите курсор на строку с именем Сервера и нажмите на кнопку ×.

   Сервер появится на вкладке **Вне подразделений**.

Управление размещением объектов на картах

В разделе Web Console **KICS for Networks → Карта** подразделения и компоненты Kaspersky Industrial CyberSecurity for Networks представлены на картах в виде значков.

Управлять размещением объектов на картах могут только пользователи Kaspersky Security Center, которым предоставлены права доступа, соответствующие роли Администратор в Kaspersky Industrial CyberSecurity for Networks.

Вы можете перемещать значки объектов на нужные места на картах. При этом все значки на карте должны отображаться по отдельности, без полного наложения друг на друга.

При необходимости вы можете выключить отображение ненужного объекта на карте. После выключения отображения объект не удаляется из списка объектов карты. Позже вы можете снова включить отображение этого объекта.

Чтобы включить или выключить отображение подразделения на общей карте:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.

2. Выберите раздел **KICS for Networks → Карта**.

3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.

4. Если строка с названием нужного подразделения не отображается в списке, это может быть связано с действием фильтра по статусам подразделений. В этом случае включите отображение всех подразделений с помощью кнопки **Все статусы** или нажмите на кнопку с названием того статуса, который присвоен нужному подразделению.

5. Наведите курсор на строку с названием подразделения и нажмите на кнопку .

   После выполнения действия изменится яркость значка в кнопке.

Чтобы включить или выключить отображение Сервера или сенсора на карте подразделения:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.

2. Выберите раздел **KICS for Networks → Карта**.

3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.

4. Нажмите на строку с названием нужного подразделения.

   Откроется карта подразделения.

5. Нажмите на кнопку **Показать список Серверов**.

   В правой части раздела появится окно с названием подразделения.

6. Перейдите на вкладку **В подразделении**.

7. Если строка с нужным Сервером не отображается в списке, это может быть связано с действием фильтра по статусам Серверов. В этом случае включите отображение всех Серверов с помощью кнопки **Все статусы** или нажмите на кнопку с названием того статуса, который присвоен нужному Серверу.

8. Если с Сервером связаны сенсоры и вы хотите включить или выключить отображение этих сенсоров, раскройте список **Сенсоры** в строке с именем нужного Сервера.

9. Наведите курсор на строку с именем нужного Сервера или сенсора и нажмите на кнопку .

   Если вы выключили отображение Сервера, то одновременно выключается отображение и всех сенсоров, которые связаны с этим Сервером.

   После выполнения действия изменится яркость значка в кнопке.

Исключение Сервера из мониторинга в Web Console

Если в Kaspersky Security Center Web Console поступают данные от нескольких Серверов Kaspersky Industrial CyberSecurity for Networks и данные от какого-либо Сервера временно не нуждаются в мониторинге (например, во время профилактических и пусконаладочных работ в АСУ ТП), вы можете исключить этот Сервер из мониторинга. После исключения Сервера из мониторинга Web Console перестает принимать данные от этого Сервера и присваивает ему статус *Без мониторинга*. При этом Сервер администрирования Kaspersky Security Center продолжает получать и сохранять данные от этого Сервера (в том числе события).

Сервер остается исключенным из мониторинга до тех пор, пока вы снова не включите мониторинг для этого Сервера.

Исключать Серверы из мониторинга и включать мониторинг могут только пользователи Kaspersky Security Center, которым предоставлены права доступа, соответствующие роли Администратор в Kaspersky Industrial CyberSecurity for Networks.

Чтобы исключить Сервер из мониторинга или включить мониторинг для Сервера:

1. Войдите в Kaspersky Security Center Web Console под учетной записью с правами Администратора в Kaspersky Industrial CyberSecurity for Networks.

2. Выберите раздел **KICS for Networks → Карта**.

3. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.

4. Нажмите на строку с названием нужного подразделения.

   Откроется карта подразделения.

5. Нажмите на кнопку **Показать список Серверов**.

   В правой части раздела появится окно с названием подразделения.

6. Нажмите на строку с именем нужного Сервера.

   В правой части раздела появится окно с подробной информацией о Сервере.

7. Если вы хотите исключить Сервер из мониторинга, нажмите на кнопку **Исключить из мониторинга**. Если Сервер уже исключен из мониторинга и вы хотите включить мониторинг, нажмите на кнопку **Включить мониторинг**.

8. В окне запроса на подтверждение операции нажмите на кнопку **ОК**.

Просмотр информации о Серверах на картах

Статусы Серверов Kaspersky Industrial CyberSecurity for Networks влияют на цвета отображаемых значков Серверов и значков подразделений на картах в разделе Web Console **KICS for Networks → Карта**. Если на карте подразделения отображаются значки сенсоров, цвета этих значков зависят от текущего состояния узлов с сенсорами. Таким образом, по цветам значков объектов на картах вы можете наблюдать за статусами компонентов Kaspersky Industrial CyberSecurity for Networks.

При необходимости вы можете просмотреть подробную информацию о любом Сервере. В окне с подробной информацией представлены основные сведения о текущем состоянии Сервера, а также сведения об установленных обновлениях баз и программных модулей, сведения об использовании аппаратных ресурсов и о лицензионном ключе.

Чтобы просмотреть подробную информацию о Сервере:

1. Выберите раздел **KICS for Networks → Карта**.

2. Нажмите на кнопку **Показать список подразделений**.

   В правой части раздела появится окно **Подразделения**.

3. Нажмите на строку с названием нужного подразделения.

   Откроется карта подразделения.

4. Нажмите на кнопку **Показать список Серверов**.

   В правой части раздела появится окно с названием подразделения.

5. Нажмите на строку с именем нужного Сервера.

   В правой части раздела появится окно с подробной информацией о Сервере.

6. Если вы хотите перейти на страницу веб-интерфейса Сервера, нажмите на кнопку **Перейти к Серверу**.

   В браузере откроется вкладка, в названии которой будет указано имя Сервера, заданное во время начальной настройки программы после установки.

Устранение неисправностей

Этот раздел содержит описание возможных неисправностей в работе Kaspersky Industrial CyberSecurity for Networks и способов их устранения.

Не выполняется установка программы из-за недоступного репозитория для DNF

Проблема

При установке программы на компьютере с операционной системой CentOS выводится сообщение о недоступности репозитория для системного менеджера пакетов DNF. Установка программы прерывается.

Решение

Установка программы невозможна, если в системном менеджере пакетов DNF недоступны (или неправильно настроены) репозитории с установочными пакетами операционной системы. Для установки программы требуется отключить недоступные репозитории.

Чтобы отключить недоступные репозитории и установить программу:

1. Загрузите список всех подключенных репозиториев менеджера пакетов DNF. Для этого откройте консоль операционной системы и в командной строке введите команду:

   ```
   dnf repolist
   ```

2. Найдите в списке недоступные репозитории и отключите их. Для отключения репозитория в командной строке введите команду:

   ```
   sudo dnf config-manager --set-disabled <имя репозитория>
   ```

3. Выполните переустановку программы с теми же параметрами установки.

Не выполняется установка компонента программы на выбранном узле

Проблема

При централизованной установке компонентов программы выводится сообщение о недоступности узла для установки компонента из-за невозможности подключения по протоколу SSH. Установка компонента на этом узле не выполняется.

Решение

Централизованная установка компонента программы невозможна, если после настройки доступа по протоколу SSH на узле для установки компонента изменилась адресная информация или сетевое имя компьютера. Для централизованной установки компонента программы требуется восстановить доступ по протоколу SSH к удаленному компьютеру.

Чтобы восстановить доступ по протоколу SSH и установить компонент программы:

1. На компьютере, с которого выполняется централизованная установка компонентов программы, обновите ключ для подключения к узлу по протоколу SSH. Для этого войдите в систему с учетными данными пользователя, от имени которого выполняется установка программы, и в консоли операционной системы введите команду:

   ```
   sudo ssh-keygen -R <IP-адрес узла>
   ```

2. Выполните переустановку программы с теми же параметрами установки. При переустановке убедитесь в отсутствии сообщения о недоступности узла для установки компонента.

Обнаружены проблемы в работе программы

Проблема

При подключении к Серверу через веб-интерфейс в верхней части меню веб-интерфейса программы отображается значок красного цвета рядом с кнопкой .

Решение

Такое состояние Kaspersky Industrial CyberSecurity for Networks означает, что работа одного из процессов программы нарушена.

Чтобы восстановить работу программы:

1. Подождите 20–30 секунд.

   Работоспособность программы может восстановиться автоматически. Если программа продолжит работать нормально, значок красного цвета перестанет отображаться.

2. Если неисправность сохраняется, обратитесь в Службу технической поддержки "Лаборатории Касперского". Будьте готовы предоставить журналы работы процессов Kaspersky Industrial CyberSecurity for Networks и другие данные системы по запросу специалистов Службы технической поддержки. Журналы работы процессов располагаются в директориях, перечисленных в статье Директории для хранения данных программы. Для доступа к журналам нужно иметь root-права в операционной системе.

Новое сообщение программы

Проблема

Появилось новое сообщение программы в разделе **Параметры** → **Сообщения программы**.

О сообщениях, на которые вам нужно обратить внимание, оповещает значок красного или желтого цвета рядом с кнопкой в меню веб-интерфейса. Если значок отображается, это может означать, что появилось сообщение о нарушении работы программы или о некритическом сбое и эта проблема не устранена. Для просмотра сведений вы можете перейти в раздел **Параметры** → **Сообщения программы** с помощью кнопки, пока рядом с этой кнопкой отображается значок красного или желтого цвета.

Решение

Сообщение программы означает, что в работе программы произошло какое-либо событие.

Просмотрите краткую информацию в сообщении в разделе **Параметры** → **Сообщения программы**. По этой информации вы можете принять решение о необходимых действиях.

Дальнейшие действия зависят от статуса сообщения. Для сообщений предусмотрены следующие статусы:

- *Нормальная работа* – в большинстве случаев сообщение не требует реакции. Однако возможны ситуации, требующие дополнительного выяснения обстоятельств. Например, по сообщению об успешном применении политики безопасности, если вам неизвестны причины, по которым было выполнено это действие.

- *Неизвестно*, *Сбой* – если сообщение появилось только что, подождите 20–30 секунд и проверьте текущее состояние программы.

- *Серьезный сбой*, *Критический сбой* или *Неустранимый сбой* – работа программы нарушена. Если проблему решить не удалось, обратитесь в Службу технической поддержки "Лаборатории Касперского". Будьте готовы предоставить журналы работы процессов Kaspersky Industrial CyberSecurity for Networks и другие данные системы по запросу специалистов Службы технической поддержки. Журналы работы процессов располагаются в директориях, перечисленных в статье Директории для хранения данных программы. Для доступа к журналам нужно иметь root-права в операционной системе.

Закончилось свободное пространство на жестком диске

Проблема

На жестком диске компьютера, на котором установлен Сервер или сенсор программы, закончилось свободное пространство.

Решение

Для работы компонентов программы компьютер должен удовлетворять аппаратным и программным требованиям.

Чтобы программа работала верно:

1. Освободите на жестком диске компьютера достаточный объем пространства, соответствующий минимальным требованиям к объему свободного пространства.

2. Перезапустите сервисы, обеспечивающие работу компонентов программы.

При включении точки мониторинга возникает ошибка

Проблема

После переключения точки мониторинга в режим *Включена* отображается статус *Ошибка*. Вследствие этого узел, к которому относится точка мониторинга, отображается со статусом *Нарушена работа*. Также в списке уведомлений о проблемах в работе программы появляется сообщение о нарушении работы из-за обнаруженных проблем на точке мониторинга.

Решение

Статус *Ошибка* на точке мониторинга может быть связан с неподдерживаемым операционным состоянием (operational state), в котором находится сетевой интерфейс. Для успешного завершения проверки при включении точки мониторинга сетевой интерфейс должен находиться в операционном состоянии *UP*. Если сетевой интерфейс находится в другом операционном состоянии (например, *UNKNOWN*), программа присваивает точке мониторинга статус *Ошибка* из-за возможных проблем при получении или обработке сетевых пакетов.

Вы можете проверить текущее операционное состояние сетевого интерфейса на компьютере узла с помощью команды `ip link`. Сведения о текущем операционном состоянии выводятся в строке с именем интерфейса в виде: `state <состояние>`. На проблемном сетевом интерфейсе наиболее вероятны следующие операционные состояния:

- *DOWN*. В этом случае вы можете перевести интерфейс в операционное состояние *UP* с помощью команды:

  ```
  sudo ip link set <имя интерфейса> up
  ```

- *UNKNOWN*. Такое операционное состояние может быть связано с неправильным добавлением интерфейса. Например, в состоянии *UNKNOWN* могут работать сетевые интерфейсы, добавляемые по умолчанию на виртуальной машине VMware™. В этом случае рекомендуется заново добавить (создать) сетевой интерфейс с правильными параметрами, используя соответствующие средства для работы с сетевыми интерфейсами.

После перевода сетевого интерфейса в операционное состояние *UP* проверьте статус точки мониторинга, которая добавлена на этот сетевой интерфейс. Если для точки мониторинга продолжает отображаться статус *Ошибка*, выключите и снова включите эту точку мониторинга.

Отсутствует трафик на точке мониторинга

Проблема

Программа зарегистрировала событие, описание которого содержит следующий текст: `Отсутствует трафик на точке мониторинга`. В описании события указана длительность отсутствия трафика, имя точки мониторинга и сетевой интерфейс, на который не поступает трафик.

Решение

Для того чтобы трафик поступал на точку мониторинга, должны выполняться следующие условия:

- точка мониторинга включена и ее текущий статус *OK*;
- на сетевом интерфейсе точки мониторинга к Ethernet-порту подключен сетевой кабель;
- на сетевом интерфейсе точки мониторинга скорость поступления входящего трафика больше чем 0 бит/с.

Вы можете просмотреть сведения о точках мониторинга и сетевых интерфейсах при подключении к Серверу через веб-интерфейс в разделе **Параметры** → **Развертывание**.

Если на сетевом интерфейсе точки мониторинга отображается скорость поступления входящего трафика 0 бит/с, проверьте выполнение следующих условий:

- сетевой интерфейс точки мониторинга правильно настроен в операционной системе;
- при подключении сетевого интерфейса к сетевому коммутатору промышленной сети – на сетевом коммутаторе правильно настроена передача зеркалированного трафика через порт подключения (SPAN).

Не загружается трафик для событий или инцидентов

Проблема

Невозможно загрузить трафик для выбранных событий и/или инцидентов. В таблице событий либо не отображаются инструменты для загрузки трафика (например, отсутствует кнопка **Скачать трафик** в области деталей, если выбрано одно событие), либо выводится сообщение `Для выбранных событий трафик отсутствует` (при попытке загрузки трафика).

Решение

Сохраненный трафик для выбранных событий и/или инцидентов может отсутствовать по одной из следующих причин:

- трафик не сохранялся;
- трафик удален из базы данных;
- файлы дампа трафика удалены.

Программа сохраняет трафик при регистрации события, если включено сохранение трафика для типа этого события. По умолчанию сохранение трафика выключено для всех типов событий. Вы можете включить и настроить сохранение трафика для нужных типов событий.

Программа удаляет сохраненный трафик для зарегистрированных событий при достижении одного из ограничений хранения трафика (например, если превышен максимальный объем сохраненного трафика в базе данных). Из базы данных удаляются пакеты трафика, которые были сохранены раньше других пакетов. Если сохраненный трафик удаляется слишком быстро и вы не успеваете его загрузить для нужных событий, вы можете увеличить максимальные значения параметров сохранения трафика.

Программа удаляет временные файлы дампа трафика, которые были сохранены раньше других файлов, при достижении ограничения по объему хранения файлов дампа трафика. Если файлы дампа трафика удаляются слишком быстро и вы не успеваете загрузить трафик из этих файлов, вы можете увеличить максимальные значения параметров сохранения файлов дампа трафика или подключить внешние хранилища на узлах.

Профилактические и пусконаладочные работы на АСУ ТП

Проблема

Проведение профилактических и пусконаладочных работ на АСУ ТП может стать причиной регистрации большого числа важных и критических событий в Kaspersky Industrial CyberSecurity for Networks.

Решение

На время проведения профилактических и пусконаладочных работ вы можете выбрать один из следующих вариантов решения проблемы:

- Оставить включенными все точки мониторинга и все технологии на Сервере и на сенсорах программы. В этом случае при просмотре сведений о событиях и взаимодействиях устройств учитывайте время и перечень проводимых профилактических и пусконаладочных работ.

- Выключить точки мониторинга или выключить использование технологий на точках мониторинга, на которые поступает трафик из сегментов промышленной сети, где проводятся профилактические и пусконаладочные работы. Например, если работы проводятся в одном цехе, вы можете выключить точку мониторинга, на которую поступает трафик из этого цеха, и оставить включенными все остальные точки мониторинга.

- Выключить все точки мониторинга на всех узлах с установленными компонентами программы. Вы можете выбрать этот вариант, если профилактические и пусконаладочные работы проводятся во всей промышленной сети.

Если вы выключили точки мониторинга или технологии, для возобновления контроля защищаемой АСУ ТП вам нужно снова включить точки мониторинга или технологии сразу после завершения профилактических и пусконаладочных работ.

Следует учитывать, что злоумышленники могут попытаться получить несанкционированный доступ к сети именно в период профилактических и пусконаладочных работ на АСУ ТП. Для принятия решения о выключении точек мониторинга или технологий руководствуйтесь регламентами и процедурами для обеспечения безопасности, принятыми на вашем предприятии.

Если при проведении профилактических и пусконаладочных работ изменился состав или параметры сетевого оборудования промышленной сети (например, MAC-адреса или IP-адреса), внесите соответствующие изменения для контроля процесса, контроля взаимодействий и контроля активов. Для этого, например, вы можете настроить режим обучения технологий для соответствующих точек мониторинга.

Непредвиденная перезагрузка системы

Проблема

Неожиданная перезагрузка компьютера с установленным компонентом Kaspersky Industrial CyberSecurity for Networks.

Решение

Дождитесь окончания загрузки компьютера. После загрузки возможны следующие варианты состояния Kaspersky Industrial CyberSecurity for Networks:

- Работоспособность Kaspersky Industrial CyberSecurity for Networks восстановилась полностью.

  Программа работает в нормальном режиме.

- Работоспособность Kaspersky Industrial CyberSecurity for Networks не восстановилась.

  Программа информирует об обнаруженных проблемах в работе.

Если неисправность сохраняется, перезапустите сервисы, обеспечивающие работу компонентов программы. Если после перезапуска проблема не устранена, обратитесь в Службу технической поддержки "Лаборатории Касперского". Будьте готовы предоставить журналы работы процессов Kaspersky Industrial CyberSecurity for Networks и другие данные системы по запросу специалистов Службы технической поддержки. Журналы работы процессов располагаются в директориях, перечисленных в статье Директории для хранения данных программы. Для доступа к журналам нужно иметь root-права в операционной системе.

Недоступна функциональность коннекторов и удаленных подключений после изменения или добавления IP-адреса Сервера

Проблема

Если на компьютере Сервера был изменен или добавлен IP-адрес для подключений через веб-сервер, коннекторы не могут подключиться к Серверу по новому IP-адресу из-за ошибок проверки сертификатов. Также недоступна возможность сканирований устройств через сенсоры программы при использовании способа опроса **Удаленное подключение**.

Решение

Для использования нового IP-адреса Сервера вам нужно заменить (выпустить новый) основной сертификат Сервера, используемый для защиты соединений с коннекторами и сервисами компонентов программы.

Замена основного сертификата Сервера выполняется как часть процедуры обновления сертификатов для соединений между узлами Kaspersky Industrial CyberSecurity for Networks. Вследствие этого при замене основного сертификата Сервера становятся недействительны старые сертификаты сенсоров программы, что приводит к разрыву соединений сенсоров с Сервером. Для возобновления соединений в рамках процедуры обновления сертификатов вам потребуется заново добавить и подключить все сенсоры. Также вам потребуется обновить сертификаты для подключения коннекторов.

Чтобы заменить основной сертификат Сервера и обеспечить его использование коннекторами и сервисами компонентов программы:

1. На компьютере Сервера перейдите в директорию /opt/kaspersky/kics4net/sbin/ и введите команду запуска скрипта локального обновления сертификатов:

   ```
   sudo bash kics4net-update-certs.sh
   ```

2. После завершения работы скрипта переведите все сенсоры в начальное состояние с помощью скрипта для локального перевода узла в начальное состояние kics4net-reset-to-defaults.sh. Скрипт находится на компьютере с установленным компонентом программы в директории /opt/kaspersky/kics4net/sbin/.

3. Заново добавьте и подключите сенсоры.

4. Обновите сертификаты для подключения коннекторов.

   Вы можете обновлять сертификаты для подключения неуправляемых коннекторов (или коннекторов с включенным режимом игнорирования функций управляемого коннектора) при создании новых файлов свертки для коннекторов. Для обновления сертификатов управляемых коннекторов вам нужно удалить и заново добавить эти коннекторы.

Не выполняется загрузка обновлений с Сервера администрирования Kaspersky Security Center

Проблема

При запуске обновления баз и программных модулей с выбранным источником обновлений **Сервер администрирования Kaspersky Security Center** программа выводит сообщение `Установка обновлений не завершена из-за ошибки, прервавшей процесс.`

Решение

Получение обновлений с Сервера администрирования Kaspersky Security Center возможно при выполнении условий для взаимодействия Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center. Если какое-то из условий не выполнено, обеспечьте выполнение этого условия. Например, если не установлен плагин управления Kaspersky Industrial CyberSecurity for Networks текущей версии для Kaspersky Security Center, то установите плагин.

В некоторых случаях ошибки установки обновлений могут быть связаны с невозможностью скачивания обновлений из хранилища Kaspersky Security Center. Если обновления для Kaspersky Industrial CyberSecurity for Networks были загружены в хранилище обновлений, но недоступны для скачивания, вы можете выполнить действия для очистки хранилища, описанные в Базе знаний Kaspersky Security Center.

После переустановки Сервера администрирования Kaspersky Security Center не выполняется синхронизация Агента администрирования

Проблема

Если после переустановки Сервера администрирования Kaspersky Security Center не выполнялось восстановление параметров из резервной копии, то в Консоли администрирования Kaspersky Security Center не отображается компьютер, на котором установлен Kaspersky Industrial CyberSecurity for Networks.

Решение

Для восстановления синхронизации Агента администрирования вы можете восстановить параметры Сервера администрирования Kaspersky Security Center с помощью утилиты резервного копирования klbackup. Утилита klbackup входит в состав дистрибутива Kaspersky Security Center. Подробную информацию о резервном копировании и восстановлении параметров Сервера администрирования Kaspersky Security Center см. в справочной системе для Kaspersky Security Center.

Если по каким-либо причинам невозможно восстановить параметры Сервера администрирования Kaspersky Security Center с помощью утилиты klbackup, вы можете восстановить синхронизацию Агента администрирования с помощью утилиты klmover, входящей в состав Агента администрирования.

Чтобы восстановить синхронизацию Агента администрирования с помощью утилиты klmover:

1. На компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks, откройте консоль операционной системы и перейдите в директорию /opt/kaspersky/klnagent64/bin/.

2. В командной строке введите команду:

   `sudo ./klmover -address <IP-адрес или имя компьютера>`

   где `<IP-адрес или имя компьютера>` – IP-адрес или имя компьютера с Kaspersky Security Center.

3. После завершения работы утилиты klmover проверьте подключение Агента администрирования к Серверу администрирования Kaspersky Security Center. Для этого в командной строке введите команду:

   `sudo ./klnagchk`

   На экране отобразится информация о подключении к Серверу администрирования.

После успешного восстановления синхронизации Агента администрирования в Консоли администрирования Kaspersky Security Center отобразится компьютер, на котором установлен Kaspersky Industrial CyberSecurity for Networks.

Не выполняется подключение к Серверу через веб-интерфейс

Проблема

При попытке подключения к Серверу не загружается страница веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Решение

Возможны следующие ситуации:

- Отсутствует доступ по сети к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks с установленным веб-сервером. Проверьте соединение с компьютером по указанному имени Сервера (например, с помощью команды `ping`).

- В адресной строке браузера введены неправильные данные. Введите IP-адрес или имя компьютера Сервера, которое было указано для веб-сервера в разделе **Параметры** → **Серверы подключений**. Номер порта можно не указывать, если задан порт по умолчанию 443. Если задан другой номер порта, введите полный адрес в формате `https://<имя Сервера>:<порт>` в адресной строке.

- В браузере выключено выполнение сценариев JavaScript. Сообщение об этом выводится на странице предупреждения о невозможности подключения. В параметрах браузера включите выполнение JavaScript и обновите страницу.

- Доступ к компьютеру Сервера заблокирован межсетевым экраном. Выполните настройку используемого межсетевого экрана.

При подключении к Серверу браузер выводит предупреждение о сертификате

Проблема

При попытке подключения к компьютеру с установленным компонентом Kaspersky Industrial CyberSecurity for Networks браузер выводит предупреждение о том, что сертификат безопасности или устанавливаемое соединение не является доверенным. Содержание предупреждения зависит от используемого браузера.

Решение

Предупреждение означает, что на веб-сервере используется самоподписанный сертификат. Для получения и использования доверенного сертификата вам нужно обратиться к администратору.

Вы можете временно использовать самоподписанный сертификат для подключения к Серверу (например, при тестовой эксплуатации Kaspersky Industrial CyberSecurity for Networks). Для использования самоподписанного сертификата в окне предупреждения браузера выберите вариант, позволяющий продолжить подключение. После подключения к Серверу в окне браузера будет отображаться предупреждающее сообщение о сертификате. Текст сообщения зависит от используемого браузера.

Для постоянного использования вы можете добавить для веб-сервера доверенный сертификат в разделе **Параметры → Серверы подключений**.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Industrial CyberSecurity for Networks, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Industrial CyberSecurity for Networks.

Kaspersky предоставляет поддержку Kaspersky Industrial CyberSecurity for Networks в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Получение информации для технической поддержки

Специалисты Службы технической поддержки "Лаборатории Касперского" могут запросить у вас журналы Kaspersky Industrial CyberSecurity for Networks и другие данные системы.

Журналы располагаются на компьютерах с установленными компонентами Kaspersky Industrial CyberSecurity for Networks. Сведения о директориях для хранения журналов представлены в статье Директории для хранения данных программы.

Для доступа к журналам нужно иметь root-права в операционной системе.

Также специалисты Службы технической поддержки "Лаборатории Касперского" могут запросить дополнительные данные о компонентах программы. Эти данные можно получить с помощью скрипта централизованной установки компонентов программы kics4net-deploy-<номер версии программы>.bundle.sh или с помощью скрипта для локального запуска kics4net-gather-artefacts.sh, который находится на компьютере с установленным компонентом программы в директории /opt/kaspersky/kics4net/sbin/.

Чтобы получить данные о компонентах программы с помощью скрипта kics4net-deploy-<номер версии программы>.bundle.sh:

1. На компьютере, с которого выполнялась централизованная установка, перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-centos.

2. Введите команду:

   `bash kics4net-deploy-<номер версии программы>.bundle.sh --gather-artefacts -<параметр> <имя директории>`

   где:

   - `<параметр>` – определяет режим получения данных.

     Предусмотрены следующие параметры:

     - `a` – для получения всех данных;
     - `c` – для получения данных о сертификатах;
     - `i` – для получения данных о конфигурации обнаружения вторжений;
     - `t` – для получения файлов дампа трафика.

   - `<имя директории>` – имя директории для копирования архивных файлов с данными.

     Пример:
     `bash kics4net-deploy-<номер версии программы>.bundle.sh --gather-artefacts -a /tmp/data_for_support`

3. В приглашениях `SSH password` и `BECOME password` введите пароль учетной записи пользователя, от имени которого выполнялась установка компонентов программы.

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh. При успешном завершении файлы будут созданы в указанной директории.

Чтобы получить данные об установленном на компьютере компоненте программы с помощью скрипта kics4net-gather-artefacts.sh:

1. Выполните вход в систему с учетными данными пользователя с root-правами.

2. Перейдите в директорию /opt/kaspersky/kics4net/sbin/ и введите команду запуска скрипта для получения данных о компоненте программы:

   `bash kics4net-gather-artefacts.sh -<параметр> <имя директории>`

   где:

   - `<параметр>` – определяет режим получения данных.

     Предусмотрены следующие параметры:

     - `a` – для получения всех данных;
     - `c` – для получения данных о сертификатах;
     - `i` – для получения данных о конфигурации обнаружения вторжений;
     - `t` – для получения файлов дампа трафика.

   - `<имя директории>` – имя директории для копирования архивных файлов с данными.

     Пример:
     `bash kics4net-gather-artefacts.sh -a /tmp/data_for_support`

Дождитесь завершения работы скрипта kics4net-gather-artefacts.sh. При успешном завершении файлы будут созданы в указанной директории.

Источники информации о программе

На странице Kaspersky Industrial CyberSecurity for Networks вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

В онлайн-справке содержится информация об администрировании Kaspersky Industrial CyberSecurity for Networks. Также в онлайн-справке представлены сведения о возможностях решения типовых задач пользователями программы.

В состав онлайн-справки входит документация для Kaspersky Industrial CyberSecurity for Networks API. Документация представляет собой руководство разработчика Kaspersky Industrial CyberSecurity for Networks API на английском языке. В руководстве разработчика Kaspersky Industrial CyberSecurity for Networks API вы можете найти информацию для выполнения следующих задач:

- подготовка к использованию Kaspersky Industrial CyberSecurity for Networks API;
- выполнение запросов для получения данных из Kaspersky Industrial CyberSecurity for Networks и отправки данных в программу.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа примерами, а также справочными и дополнительными сведениями.

Настройка синхронизации времени по протоколам NTP и PTP

Этот раздел содержит информацию о доступных действиях по настройке синхронизации времени по протоколам NTP и PTP.

Синхронизация времени узлов с установленными компонентами Kaspersky Industrial CyberSecurity for Networks должна выполняться с общим источником времени, который используют устройства промышленной сети. Для синхронизации вы можете использовать стандартные протоколы Network Time Protocol (NTP) и Precision Time Protocol (PTP).

На узле Сервера требуется настроить синхронизацию времени при любом способе установки этого компонента (как после централизованной установки, так и после локальной).

На узлах с установленными сенсорами настраивать синхронизацию времени требуется в следующих случаях:

- если при централизованной установке Kaspersky Industrial CyberSecurity for Networks не включена автоматическая синхронизация времени между Сервером и сенсорами;
- если установка сенсора выполнена локально с помощью скрипта kics4net-install.sh.

Действия по настройке синхронизации различаются в зависимости от версии операционной системы и протокола.

Настройка синхронизации времени по протоколу NTP в CentOS

Чтобы настроить синхронизацию времени по протоколу NTP в CentOS:

1. Откройте консоль операционной системы.
2. Проверьте статус стандартного сервиса синхронизации времени chrony. Для этого введите команду:

   ```
   systemctl status chronyd
   ```

3. Если сервис не найден, введите следующие команды для добавления пакета и работы сервиса:

   ```
   sudo dnf install chrony
   sudo systemctl enable chronyd
   sudo systemctl start chronyd
   ```

4. Откройте файл конфигурации сервиса. Для этого введите команду:

   ```
   sudo mcedit /etc/chrony.conf
   ```

5. Укажите NTP-серверы, которые будут использоваться для синхронизации времени. Для указания сервера достаточно добавить строку вида:

   ```
   server <имя или IP-адрес сервера> iburst
   ```

6. Сохраните и закройте файл конфигурации.

7. Перезапустите сервис. Для этого введите команду:

   ```
   sudo systemctl restart chronyd
   ```

8. Проверьте наличие указанных NTP-серверов в списке источников синхронизации. Для этого введите команду:

   ```
   chronyc sources
   ```

Настройка синхронизации времени по протоколу PTP в CentOS

Чтобы настроить синхронизацию времени по протоколу PTP в CentOS:

1. Откройте консоль операционной системы.

2. Проверьте наличие установленного пакета linuxptp. Для этого введите команду:

   ```
   dnf list installed
   ```

3. Если пакет linuxptp не установлен, введите следующие команды для добавления пакета и работы сервиса синхронизации времени ptp4l:

   ```
   sudo dnf install linuxptp
   sudo systemctl enable ptp4l
   sudo systemctl start ptp4l
   ```

4. Откройте файл конфигурации сервиса. Для этого введите команду:

   ```
   sudo mcedit /etc/ptp4l.conf
   ```

5. Для параметра `slaveOnly` укажите значение `1`.

6. Сохраните и закройте файл конфигурации.

7. Откройте файл общих параметров для сервиса. Для этого введите команду:

   ```
   sudo mcedit /etc/sysconfig/ptp4l
   ```

8. В строке `OPTIONS` укажите параметры в виде:

   ```
   OPTIONS="-f <файл конфигурации> -i <имя интерфейса> -S -s"
   ```

   где:

   - `-f <файл конфигурации>` – полный путь и имя файла конфигурации по умолчанию.
   - `-i <имя интерфейса>` – имя сетевого интерфейса, который используется для синхронизации времени.
   - `-S` – включает использование программных меток времени. Вы можете пропустить этот параметр, если хотите использовать аппаратные метки времени. При этом оборудование должно поддерживать такую возможность.
   - `-s` – включает подчиненный режим синхронизации времени.

   Пример строки `OPTIONS`:

   ```
   OPTIONS="-f /etc/ptp4l.conf -i eth0 -S -s"
   ```

9. Сохраните и закройте файл общих параметров.

10. В межсетевом экране разрешите использование портов 319 и 320 для протокола UDP. Для этого введите следующие команды:

    ```
    sudo firewall-cmd --permanent --add-port=319/udp
    sudo firewall-cmd --permanent --add-port=320/udp
    ```

11. Перезапустите сервис межсетевого экрана. Для этого введите команду:

    ```
    sudo systemctl restart firewalld
    ```

12. Перезапустите сервис синхронизации времени. Для этого введите команду:

    ```
    sudo systemctl restart ptp4l
    ```

Поддерживаемые типы кадров ASDU в протоколах стандартов IEC 60870-5-104 и IEC 60870-5-101

В этой статье приведено описание типов кадров ASDU, поддерживаемых в Kaspersky Industrial CyberSecurity for Networks (см. таблицу ниже). Перечисленные типы кадров обрабатываются при контроле технологического процесса на устройствах, которые взаимодействуют по протоколам стандартов IEC 60870-5-104 и IEC 60870-5-101.

Типы кадров в протоколах стандартов IEC 60870-5-104 и IEC 60870-5-101

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
1. Информация о процессе в направлении контроля			
<1>	M_SP_NA	Одноэлементная информация	bool (0 – ВЫКЛ, 1 – ВКЛ)
<2>	M_SP_TA	Одноэлементная информация (с меткой времени)	bool (0 – ВЫКЛ, 1 – ВКЛ)
<3>	M_DP_NA	Двухэлементная информация	unsigned int8 (0 – Неопределенное или промежуточное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное)

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
<4>	M_DP_TA	Двухэлементная информация (с меткой времени)	unsigned int8 (0 – Неопределенное или промежуточное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное)
<5>	M_ST_NA	Информация о положении отпаек	int8 (-64 … +64)
<6>	M_ST_TA	Информация о положении отпаек (с меткой времени)	int8 (-64 … +64)
<7>	M_BO_NA	Строка из 32 бит	unsigned int32
<8>	M_BO_TA	Строка из 32 бит (с меткой времени)	unsigned int32
<9>	M_ME_NA	Значение измеряемой величины, нормализованное значение	float
<10>	M_ME_TA	Значение измеряемой величины, нормализованное значение (с меткой времени)	float
<11>	M_ME_NB	Значение измеряемой величины, масштабированное значение	float
<12>	M_ME_TB	Значение измеряемой величины, масштабированное значение (с меткой времени)	float
<13>	M_ME_NC	Значение измеряемой величины, короткий формат с плавающей запятой	float
<14>	M_ME_TC	Значение измеряемой величины, короткий формат с плавающей запятой (с меткой времени)	float
<15>	M_IT_NA	Интегральная сумма	int32
<16>	M_IT_TA	Интегральная сумма (с меткой времени)	int32
<17>	M_EP_TA	Информация о работе релейной защиты (с меткой времени)	unsigned int8 (0 – Неопределенное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное)
<18>	M_EP_TB	Упакованная информация о срабатывании пусковых органов защиты (с меткой времени)	unsigned int8 (Набор битов в соответствии со стандартом)
<19>	M_EP_TC	Упакованная информация о срабатывании выходных цепей защиты (с меткой времени)	unsigned int8 (Набор битов в соответствии со стандартом)
<20>	M_PS_NA	Упакованная одноэлементная информация с определением изменения состояния	unsigned int16
<21>	M_ME_ND	Значение измеряемой величины, нормализованное значение без описателя качества	float
<30>	M_SP_TB	Одноэлементная информация (с меткой времени CP56Время2a)	bool (0 – ВЫКЛ, 1 – ВКЛ)
<31>	M_DP_TB	Двухэлементная информация (с меткой времени CP56Время2a)	unsigned int8 (0 – Неопределенное или промежуточное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное)
<32>	M_ST_TB	Информация о положении отпаек (с меткой времени CP56Время2a)	int8 (-64 … +64)
<33>	M_BO_TB	Строка из 32 бит (с меткой времени CP56Время2a)	unsigned int32
<34>	M_ME_TD	Значение измеряемой величины, нормализованное значение (с меткой времени CP56Время2a)	float
<35>	M_ME_TE	Значение измеряемой величины, масштабированное значение (с меткой времени CP56Время2a)	float
<36>	M_ME_TF	Значение измеряемой величины, короткий формат с плавающей запятой (с меткой времени CP56Время2a)	float
<37>	M_IT_TB	Интегральные суммы (с меткой времени CP56Время2a)	int32
<38>	M_EP_TD	Информация о работе релейной защиты (с меткой времени CP56Время2a)	unsigned int8 (0 – Неопределенное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное)
<39>	M_EP_TE	Упакованная информация о срабатывании пусковых органов защиты (с меткой времени CP56Время2a)	unsigned int8 (Набор битов в соответствии со стандартом)

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
<40>	M_EP_TF	Упакованная информация о срабатывании выходных цепей защиты (с меткой времени CP56Время2a)	unsigned int8 (Набор битов в соответствии со стандартом)
2. Информация о процессе в направлении управления			
<45>	C_SC_NA	Одноэлементная команда	bool (0 – ВЫКЛ, 1 – ВКЛ)
<46>	C_DC_NA	Двухэлементная команда	unsigned int8 (0 – Не разрешено, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Не разрешено)
<47>	C_RC_NA	Команда пошагового регулирования	unsigned int8 (0 – Не разрешено, 1 – Следующий шаг ВВЕРХ, 2 – Следующий шаг ВНИЗ, 3 – Не разрешено)
<48>	C_SE_NA	Команда уставки, нормализованное значение	float
<49>	C_SE_NB	Команда уставки, масштабированное значение	float
<50>	C_SE_NC	Команда уставки, короткое число с плавающей запятой	float
<51>	C_BO_NA	Строка из 32 битов	int32
<58>	C_SC_TA	Одноэлементная команда (с меткой времени CP56Время2a)	bool (0 – ВЫКЛ, 1 – ВКЛ)
<59>	C_DC_TA	Двухэлементная команда (с меткой времени CP56Время2a)	unsigned int8 (0 – Не разрешено, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Не разрешено)
<60>	C_RC_TA	Команда пошагового регулирования (с меткой времени CP56Время2a)	unsigned int8 (0 – Не разрешено, 1 – Следующий шаг ВВЕРХ, 2 – Следующий шаг ВНИЗ, 3 – Не разрешено)
<61>	C_SE_TA	Команда уставки, нормализованное значение (с меткой времени CP56Время2a)	float
<62>	C_SE_TB	Команда уставки, масштабированное значение (с меткой времени CP56Время2a)	float
<63>	C_SE_TC	Команда уставки, короткое число с плавающей запятой (с меткой времени CP56Время2a)	float
<64>	C_BO_TA	Строка из 32 битов (с меткой времени CP56Время2a)	int32
3. Информация о системе в направлении контроля			
<70>	M_EI_NA	Конец инициализации	Системная команда END OF INITIALIZATION
4. Информация о системе в направлении управления			
<100>	C_IC_NA	Команда опроса	Системная команда INTERROGATION
<101>	C_CI_NA	Команда опроса счетчика	Системная команда COUNTER INTERROGATION
<102>	C_RD_NA	Команда чтения	Системная команда READ
<103>	C_CS_NA	Команда синхронизации времени	Системная команда CLOCK SYNCHRONIZATION
<104>	C_TS_NA	Команда тестирования	Системная команда TEST
<105>	C_RP_NA	Команда установки процесса в исходное состояние	Системные команды RESET PROCESS ACTIVATION / RESET PROCESS CONFIRMATION
<106>	C_CD_NA	Команда задержки сбора данных	Системная команда DELAY ACQUISITION
<107>	C_TS_TA	Команда тестирования (с меткой времени CP56Время2a)	Системная команда TEST WITH TIME TAG
5. Параметры в направлении управления			
<110>	P_ME_NA	Параметр измеряемой величины, нормализованное значение	float
<111>	P_ME_NB	Параметр измеряемой величины, масштабированное значение	float
<112>	P_ME_NC	Параметр измеряемой величины, короткий формат с плавающей запятой	float
<113>	P_AC_NA	Активация параметра	Системная команда PARAMETER ACTIVATION
6. Пересылка файлов			

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
<120>	F_FR_NA	Файл готов	Не обрабатывается
<121>	F_SR_NA	Секция готова	Не обрабатывается
<122>	F_SC_NA	Вызов директории, выбор файла, вызов файла, вызов секции	Системная команда CALL DIRECTORY, SELECT FILE, CALL FILE, CALL SELECTION
<123>	F_LS_NA	Последняя секция, последний сегмент	Не обрабатывается
<124>	F_AF_NA	Подтверждение файла, подтверждение секции	Не обрабатывается
<125>	F_SG_NA	Сегмент	Не обрабатывается
<126>	F_DR_TA	Директория	Не обрабатывается

Загрузка, обработка и контроль конфигураций устройств и тегов с поддержкой протоколов стандарта IEC 61850

Технологии для анализа трафика промышленной сети, используемые в Kaspersky Industrial CyberSecurity for Networks, позволяют получать основные сведения о параметрах и взаимодействиях устройств с поддержкой протоколов стандарта IEC 61850: IEC 61850-8-1 (GOOSE, MMS). Однако для получения и сохранения в программе наиболее полных данных об этих устройствах, включая теги в их исходном структурном виде, рекомендуется загружать в программу содержимое файлов, подготовленных в соответствии со стандартом IEC 61850-6. Загрузка содержимого таких файлов выполняется путем импорта проектов для устройств IEC 61850.

При импорте проекта для устройств IEC 61850 Kaspersky Industrial CyberSecurity for Networks проверяет синтаксис и формат содержимого файлов проекта, а также анализирует конфигурации устройств в проекте на соответствие требованиям и рекомендациям стандарта IEC 61850. После успешного импорта проекта программа анализирует трафик на соответствие импортированной конфигурации. При обнаружении в трафике взаимодействий, которые являются отклонениями от сохраненной конфигурации (взаимодействия устройств или передаваемые параметры не соответствуют описаниям в конфигурации), программа регистрирует события.

Таким образом, за счет встроенных средств обработки и контроля конфигураций устройств IEC 61850, вы можете использовать Kaspersky Industrial CyberSecurity for Networks и как программу для защиты от угроз информационной безопасности, и как инструмент проверки файлов с описаниями конфигураций. По данным из файлов программа позволяет выявлять ошибки и недочеты проектирования комплексов устройств IEC 61850. Устранять выявленные ошибки и недочеты проектирования вы можете поэтапно.

Поддерживаемые типы проектов и модули обработки протоколов обновляются вместе с обновлениями баз и программных модулей. Для использования всех возможностей, поддерживаемых программой для анализа конфигураций устройств и анализа трафика по протоколам IEC 61850, вам нужно установить обновления.

Сценарий приведения проекта в соответствие со стандартом IEC 61850 состоит из следующих этапов:

1. **Импорт проекта для устройств IEC 61850 в Kaspersky Industrial CyberSecurity for Networks**

   На этом этапе вам нужно выполнить импорт проекта для устройств IEC 61850. Конфигурации устройств в импортируемом проекте должны быть описаны на языке SCL (System Configuration Language) и сохранены в одном или нескольких файлах, применяемых по стандарту IEC 61850. Для импорта этого типа проекта поддерживаются следующие типы файлов SCL: *.SCD, *.CID, *.ICD.

По окончании процесса импорта программа предоставляет возможность просмотра отчета о результатах. Для просмотра отчета вам нужно открыть список фоновых операций с помощью кнопки в меню веб-интерфейса программы и нажать на кнопку **Вывести отчет** после завершения процесса импорта.

Если в процессе проверки и анализа импортируемого файла обнаружены ошибки или недочеты (несоответствия), сведения о них отображаются в окне отчета в следующих разделах:

- **Ошибки синтаксиса и формата**.
- **Несоответствия стандарту** (выводится не более 100 обнаруженных несоответствий).

Если окно отчета не содержит ни одного из указанных разделов, вы можете перейти к выполнению этапа 3. Иначе внимательно ознакомьтесь со списками ошибок и несоответствий в окне отчета и перейдите к выполнению этапа 2.

2 Устранение ошибок и несоответствий по отчету об импорте

Ошибки и несоответствия, обнаруженные при импорте, различаются по своей значимости. Некоторые ошибки (например, ошибки синтаксиса разных ревизий) приводят к невозможности загрузки файла и блокируют импорт всего содержимого проекта. Другие ошибки и несоответствия могут быть обусловлены как логическими ошибками в импортируемом проекте, так и особенностями настройки используемого оборудования (если эксплуатационные возможности оборудования позволяют задавать для него параметры без соблюдения определенных рекомендаций по применению стандарта IEC 61850). Для таких ошибок и несоответствий программа выводит соответствующие предупреждения в отчете об импорте.

После ознакомления со списками ошибок и несоответствий, обнаруженных при импорте, вам нужно принять решение о необходимых доработках в проекте. Для устранения ошибок и несоответствий используйте соответствующие программные инструменты.

Если вы выполнили какие-либо доработки или дополнения в проекте, сохраните файлы проекта и повторно выполните этап 1 для импорта обновленных файлов. Если доработки проекта не требуются, перейдите к выполнению этапа 3.

3 Проверка объектов, созданных в Kaspersky Industrial CyberSecurity for Networks в результате импорта проекта

На этом этапе вам нужно проверить изменения в программе после импорта и при необходимости выполнить дополнительные действия с объектами в программе.

При наличии в импортированном проекте соответствующих данных программа выполняет следующие действия:

- добавляет новые устройства (или обновляет существующие устройства) с указанием адресной информации участников сетевых взаимодействий;
- добавляет параметры контроля процесса для устройств и сохраняет в этих параметрах:
  - отслеживаемые системные команды;
  - подписки и блоки данных для протоколов MMS и GOOSE;
- добавляет теги протоколов MMS и GOOSE в исходном структурном виде тегов;
- формирует правила контроля взаимодействий на основе информации об устройствах в импортируемой конфигурации.

Для тегов в структурном виде невозможно задать правила контроля процесса с заданными условиями для отслеживания значений. Если вы хотите проверять значения тегов с помощью программы, вы можете использовать для этого правила с Lua-скриптами.

4. **Отслеживание событий, регистрируемых при обнаружении в трафике отклонений от сохраненной конфигурации**

   С использованием сохраненной конфигурации программа анализирует трафик промышленной сети. При обнаружении в трафике взаимодействий, которые являются отклонениями от сохраненной конфигурации (взаимодействия устройств или передаваемые параметры не соответствуют описаниям в конфигурации), программа регистрирует события по технологиям Контроль целостности сети и Контроль системных команд.

   При анализе взаимодействий по протоколу IEC 61850: GOOSE программа регистрирует события в следующих случаях:

   - обнаружены несоответствия MAC-адресов источников и получателей сообщений;
   - обнаружены заводские конфигурации (одинаковый идентификатор goID в сообщениях GOOSE);
   - обнаружены несоответствия версий ConfRev;
   - обнаружены несоответствия статусов сообщений GOOSE;
   - обнаружены несоответствия основных параметров в пакетах сообщений GOOSE;
   - обнаружены несоответствия параметров качества сигнала;
   - обнаружены несоответствия в последовательности передачи сообщений;
   - обнаружено сообщение GOOSE от неописанного устройства;
   - обнаружено неописанное сообщение GOOSE от описанного устройства;
   - обнаружены изменения структуры пакета данных в сообщении GOOSE;
   - обнаружены несоответствия в использовании идентификатора VLAN в сообщениях GOOSE;
   - обнаружены несоответствия значений тегов созданным правилам контроля процесса.

   При анализе взаимодействий по протоколу IEC 61850: MMS программа регистрирует события в следующих случаях:

   - обнаружены несоответствия IP- или MAC-адресов (с учетом взаимодействий через маршуртизаторы);
   - обнаружены повторяющиеся имена/адреса;
   - обнаружены несоответствия версий ConfRev;
   - обнаружены несоответствия в последовательности выполнения системных команд;
   - обнаружены несоответствия значений тегов созданным правилам контроля процесса;
   - обнаружены несоответствия методов подключения клиента к серверу (чтение/запись или по подписке).

   Длительность этапа отслеживания событий зависит от частоты взаимодействий устройств и изменений режимов работы в рамках технологического процесса. Если, по вашим оценкам, все контролируемые устройства выполнили свои предусмотренные операции и при этом в программе не зарегистрированы события по вышеперечисленным причинам, сценарий приведения проекта в соответствие со стандартом IEC 61850 можно считать завершенным. Иначе, в случае регистрации событий, перейдите к выполнению этапа 5.

5. **Донастройка проекта для устранения отклонений от сохраненной конфигурации**

При расследовании причин регистрации событий в первую очередь проверяйте отсутствие угроз информационной безопасности и отсутствие нарушений технологического процесса.

После того, как вы убедитесь, что события были зарегистрированы из-за ошибок или несоответствий в сохраненной конфигурации, вам нужно принять решение о необходимых доработках в проекте. Для устранения ошибок и несоответствий используйте соответствующие программные инструменты.

Если вы выполнили какие-либо доработки в проекте, сохраните файлы проекта и повторно выполните этапы данного сценария, начиная с этапа 1.

После выполнения всех действий для приведения проекта в соответствие со стандартом IEC 61850 вы можете использовать все функции Kaspersky Industrial CyberSecurity for Networks в режиме наблюдения. При этом рекомендуется регулярно оценивать защищенность и работоспособность инфраструктуры промышленной сети с помощью следующих частей функциональности программы:

- Мониторинг сетевых сеансов и мониторинг в онлайн-режиме – для оценки текущей загруженности сети (в том числе с помощью виджетов **Трафик** и **Теги**).
- Контроль активов, контроль взаимодействий и обнаружение вторжений – для контроля появления в сети устройств с новыми адресами.
- Мониторинг событий – для контроля неописанных сообщений, регистрируемых в событиях по технологии Контроль системных команд, и для контроля неисправностей и сетевых ошибок, регистрируемых в событиях по технологии Обнаружение вторжений (коды системных типов событий 4000005100, 4000005101, 4000005102, 4000005103 и 4000002701) и в событиях по технологии Контроль активов (код системного типа события 4000005005).

Отправка событий Kaspersky Industrial CyberSecurity for Networks в SIEM-системы

Этот раздел содержит информацию о событиях, отправляемых в SIEM-системы.

В Kaspersky Industrial CyberSecurity for Networks вы можете использовать коннектор для отправки данных на сервер SIEM-системы. После добавления коннектора вам нужно настроить передачу событий через этот коннектор.

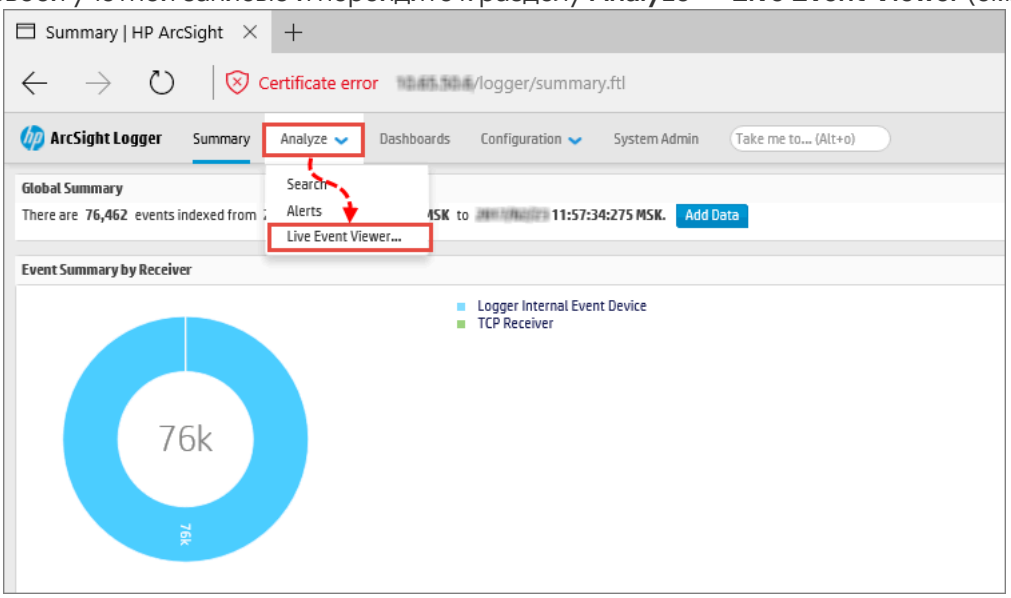
Содержание и порядок отображения сведений о событиях, передаваемых в SIEM-систему, могут отличаться от отображаемых данных на вкладке **События и инциденты** раздела **События** веб-интерфейса Сервера Kaspersky Industrial CyberSecurity for Networks.

Проверка передачи событий на примере системы HP ArcSight

Чтобы проверить передачу событий на примере системы HP ArcSight:

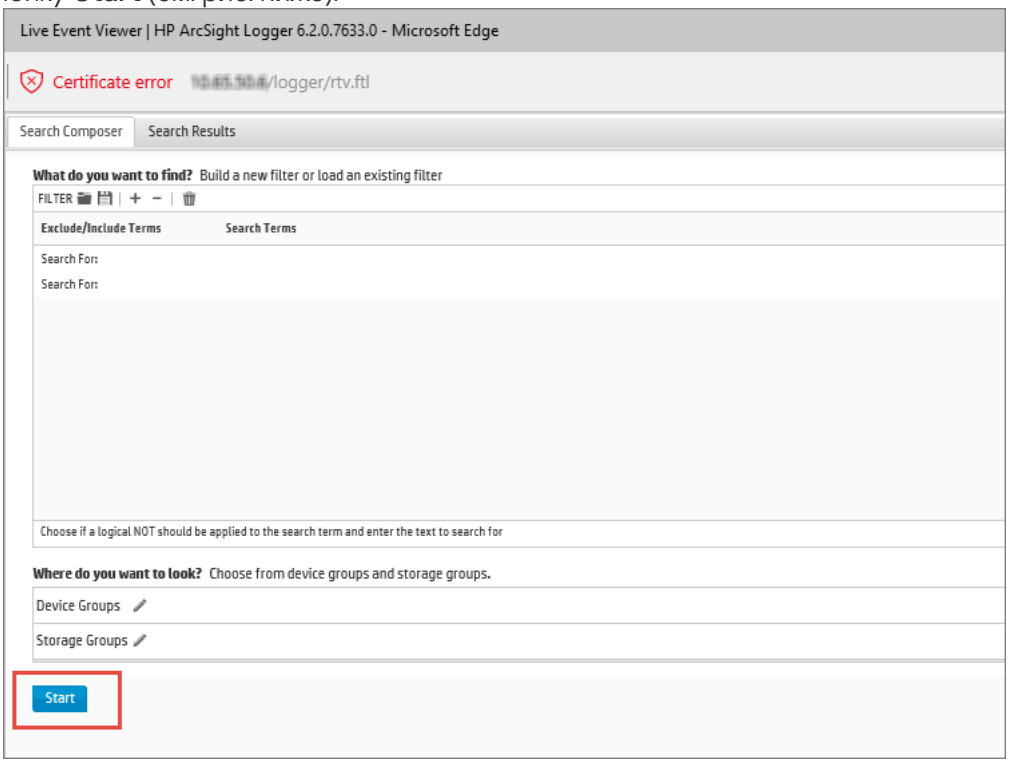
1. Убедитесь, что настроен канал приема сообщений от Kaspersky Industrial CyberSecurity for Networks штатными средствами системы HP ArcSight.
2. Откройте браузер и перейдите по адресу вашей системы HP ArcSight.

3. Войдите под своей учетной записью и перейдите к разделу **Analyze** → **Live Event Viewer** (см. рис. ниже).



Открытие раздела **Live Event Viewer** в системе HP ArcSight

4. Нажмите на кнопку **Start** (см. рис. ниже).



Запуск **Live Event Viewer** в системе HP ArcSight

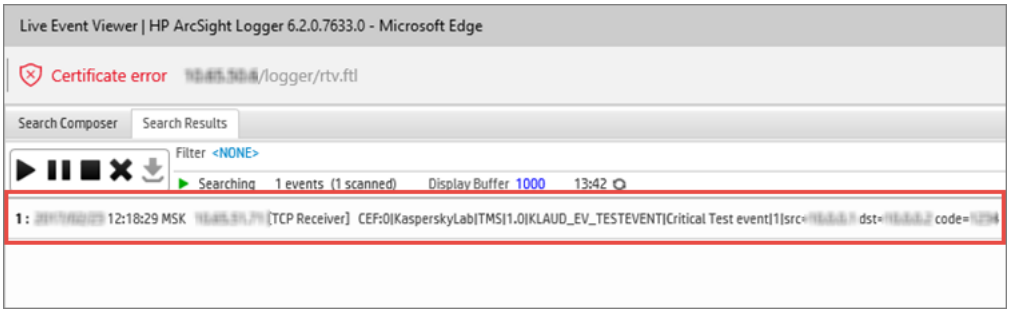
5. Откройте интерфейс командной строки и введите команду, чтобы соединиться с сервером по протоколу Telnet:

```
telnet <адрес сервера ArcSight> <порт>
```

6. Отправьте тестовое сообщение в формате CEF:

```
CEF:0|KasperskyLab|TMS|1.0|KLAUD_EV_TESTEVENT|Critical Test event|1|src=10.0.0.1
dst=10.0.0.2 code=1234
```

Если есть соединение с системой HP ArcSight, в разделе **Live Event Viewer** появится событие, содержимое которого совпадает с отправленным сообщением (см. рис. ниже).



Проверка результатов работы

Формат сообщений, посылаемых в SIEM-систему

Программа передает данные в SIEM-систему в формате CEF 20. При передаче данных используются следующие внутренние структуры:

- `EventMessage` – для событий.
- `ApplicationMessage` – для сообщений программы.
- `AuditMessage` – для записей аудита.

Получаемые сообщения не преобразуются в формат протокола системного журнала.

Формат структуры EventMessage

В таблице ниже данные представлены в следующих столбцах:

- EventMessage — имя поля в сообщении.
- Event — соответствующее поле события в Kaspersky Industrial CyberSecurity for Networks или конкретное значение.
- Описание — описание поля.

EventMessage	Event	Описание
dateTime	Начало	Дата и время (с точностью до миллисекунды) перехвата сетевого пакета, который привел к возникновению события.
hostname	Адрес Сервера Kaspersky Industrial CyberSecurity for Networks	Адрес Сервера Kaspersky Industrial CyberSecurity for Networks.
cefVersion	0	Номер версии CEF.
deviceVendor	Kaspersky Lab	Производитель.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Название продукта.
deviceVersion	Пример: 4.2.0.335	Версия Kaspersky Industrial CyberSecurity for Networks.
messageType	Event	Тип отправляемого сообщения.
signatureId	Тип события	Идентификатор типа события.
name	Заголовок	Описание события.
severity	Уровень критичности события: • 9 – для оценок 8.0–10.0; • 6 – для оценок 4.0–7.9; • 3 – для оценок 0.0–3.9.	Уровень критичности события. Значения от 3 до 9, где 9 – наиболее критичное событие.
score	Оценка события	Значение оценки события.
extension	Указано в таблице Extension Fields	Определяется отдельно для каждого типа сообщения.

Дата и время отправляются в формате: `ГГГГ-ММ-ДД Т чч:мм:сс.мс Z`. Пример: 2024-09-30T22:14:15.030Z — время события, которое возникло 30 сентября 2024 года в 22 часа, 14 минут, 15 секунд, 030 миллисекунд.

Содержимое Extension Fields

В таблице ниже данные представлены в следующих столбцах:

- Extension — имя поля в сообщении.
- Связанные события — события, в которых отправляется конкретное поле.
- Описание — описание поля.

Extension	Связанные события	Описание
cnt	Общие поля событий	Счетчик количества повторов после регистрации события.
dmac	Общие поля событий	MAC-адрес получателя.
dmacas	Общие поля событий	Адресное пространство для MAC-адреса получателя.
dpt	Общие поля событий	Порт получателя.
dst	Общие поля событий	IP-адрес получателя.
das	Общие поля событий	Адресное пространство для IP-адреса получателя (если в программу добавлены дополнительные адресные пространства).
end	Общие поля событий	Время завершения события.
smac	Общие поля событий	MAC-адрес отправителя.
smacas	Общие поля событий	Адресное пространство для MAC-адреса отправителя.
spt	Общие поля событий	Порт отправителя.
src	Общие поля событий	IP-адрес отправителя.
srcas	Общие поля событий	Адресное пространство для IP-адреса отправителя (если в программу добавлены дополнительные адресные пространства).
start	Общие поля событий	Время регистрации события.
technology	Общие поля событий	Технология, которая использовалась для регистрации события.
triggeredRule	Общие поля событий	Сработавшее правило.
protocol	Общие поля событий	Протокол.
vlanId	Общие поля событий	VLAN ID.
monitoringPoint	Общие поля событий	Точка мониторинга, трафик с которой вызвал регистрацию события.
sourceIndustrialAddress	Общие поля событий	Адрес прикладного уровня для отправителя.
destinationIndustrialAddress	Общие поля событий	Адрес прикладного уровня для получателя.
eventIdentifier	Общие поля событий	Идентификатор события.
noTrafficDuration	Отсутствует трафик на точке мониторинга	Длительность отсутствия трафика.
tagId	Неверный тип тега	ID тега.
expectedTagType	Неверный тип тега	Ожидаемый тип данных тега.
actualTagType	Неверный тип тега	Фактический тип данных тега.
ruleName	• Нарушение правила контроля процесса • Сработало правило обнаружения вторжений из системного набора правил	Имя правила.
tags	Нарушение правила контроля процесса	Теги.

msg	Сработало правило обнаружения вторжений из системного набора правил	Сообщение.
substitutedIpAddress	• Обнаружены признаки ARP-подмены в ARP-ответах • Обнаружены признаки ARP-подмены в ARP-запросах	IP-адрес отправителя сетевых пакетов.
targetIpAddress	• Обнаружены признаки ARP-подмены в ARP-ответах • Обнаружены признаки ARP-подмены в ARP-запросах	IP-адрес получателя сетевых пакетов.
attackStartTimestamp	• Обнаружены признаки ARP-подмены в ARP-ответах • Обнаружены признаки ARP-подмены в ARP-запросах	Время начала действий, имеющих признаки атаки.
ownerMac	• Обнаружен конфликт IP-адреса • Обнаружен новый IP-адрес • Обнаружено новое устройство • Получена новая информация • Обнаружен трафик с MAC-адреса • Добавлен MAC-адрес к устройству • Добавлен IP-адрес к устройству	MAC-адрес владельца.
ownerIp	• Обнаружено новое устройство • Добавлен MAC-адрес к устройству • Добавлен IP-адрес к устройству • Обнаружен конфликт IP-адреса • Обнаружен новый MAC-адрес	IP-адрес владельца.
challengerMac	Обнаружен конфликт IP-адреса	MAC-адрес претендента.
newIpAddress	Обнаружен новый IP-адрес	Новый IP-адрес.
newMacAddress	Обнаружен новый MAC-адрес	Новый MAC-адрес.
oldIpAddress	Обнаружен новый IP-адрес	Старый IP-адрес.
assetName	Обнаружено новое устройство	Имя устройства.

Параметры устройств

В таблице ниже представлены данные о параметрах устройств.

Если для обнаруженного взаимодействия определены одно или два устройства, Kaspersky Industrial CyberSecurity for Networks дополнительно отправляет в SIEM-систему известную информацию об одном или двух устройствах.

Если для обнаруженного взаимодействия определены несколько устройств, сообщение дублируется с другой адресной информацией и другими параметрами устройств (если устройства различны).

Extension	Параметр устройства
srcAssetName	Имя устройства-отправителя.

srcVendor	Производитель устройства-отправителя.
srcOS	Операционная система устройства-отправителя.
srcNetworkName	Сетевое имя устройства-отправителя.
srcModel	Модель устройства-отправителя.
dstAssetName	Имя устройства-получателя.
dstVendor	Производитель устройства-получателя.
dstOS	Операционная система устройства-получателя.
dstNetworkName	Сетевое имя устройства-получателя.
dstModel	Модель устройства-получателя.

Формат структуры ApplicationMessage

В таблице ниже данные представлены в следующих столбцах:

- EventMessage — имя поля в сообщении.
- Application message — соответствующее поле сообщения программы в Kaspersky Industrial CyberSecurity for Networks или конкретное значение.
- Описание — описание поля.

EventMessage	Application message	Описание
dateTime	Дата и время возникновения	Дата и время (с точностью до миллисекунды) обнаружения ситуации, которая привела к регистрации сообщения.
hostname	Адрес Сервера или сенсора Kaspersky Industrial CyberSecurity for Networks	Адрес узла Сервера или сенсора Kaspersky Industrial CyberSecurity for Networks.
cefVersion	0	Номер версии CEF.
deviceVendor	Kaspersky Lab	Производитель.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Название продукта.
deviceVersion	Пример: 4.2.0.335	Версия Kaspersky Industrial CyberSecurity for Networks.
messageType	Application message	Тип отправляемого сообщения.
severity	Уровень критичности сообщения программы: • 10 – для статусов *Серьезный сбой*, *Критический сбой*, *Неустранимый сбой*, • 5 – для статусов *Неизвестно*, *Сбой*, • 0 – для статуса *Нормальная работа*.	Уровень критичности сообщения программы. Значения от 0 до 10, где 10 – наиболее критичное сообщение.
address	Адрес узла	Адрес узла, от которого поступило сообщение.
systemProcess	Имя процесса	Процесс программы, который вызвал регистрацию сообщения.
msg	Сообщение	Числовой идентификатор и текст сообщения.

Формат структуры AuditMessage

В таблице ниже данные представлены в следующих столбцах:

- EventMessage — имя поля в сообщении.
- Audit message — соответствующее поле записи аудита в Kaspersky Industrial CyberSecurity for Networks или конкретное значение.
- Описание — описание поля.

EventMessage	Audit message	Описание
dateTime	Дата и время возникновения	Дата и время (с точностью до миллисекунды) обнаружения ситуации, которая привела к регистрации записи аудита.
hostname	Адрес Сервера Kaspersky Industrial CyberSecurity for Networks	Адрес узла Сервера Kaspersky Industrial CyberSecurity for Networks.
cefVersion	0	Номер версии CEF.
deviceVendor	Kaspersky Lab	Производитель.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Название продукта.
deviceVersion	Пример: 4.2.0.335	Версия Kaspersky Industrial CyberSecurity for Networks.
messageType	Audit message	Тип отправляемого сообщения.
address	Узел пользователя	Адрес узла, на котором совершено зарегистрированное действие.
user	Пользователь	Имя пользователя, который совершил зарегистрированное действие.
action	Действие	Зарегистрированное действие, которое совершил пользователь.
result	Результат	Результат выполнения зарегистрированного действия (успешно или неуспешно).
msg	Описание	Дополнительные сведения о зарегистрированном действии.

Особенности подключения узлов Kaspersky Industrial CyberSecurity for Networks в качестве шлюзов соединений в Kaspersky Security Center

Вы можете использовать узлы с установленными компонентами программы (Сервер и сенсоры) в качестве шлюзов соединений в Kaspersky Security Center. Роль шлюзов соединений с Сервером администрирования Kaspersky Security Center выполняют точки распространения. Схема взаимодействий с управляемыми устройствами с использованием точек распространения позволяет оптимизировать в сети передаваемый трафик обновлений баз, программных модулей и программ "Лаборатории Касперского" и настроить ограничения трафика для IP-диапазонов в Kaspersky Security Center. Если узел Сервера или сенсора Kaspersky Industrial CyberSecurity for Networks представляет единственную возможность соединения Сервера администрирования и управляемых устройств, находящихся в изолированной сети, роль шлюза соединения на этом узле позволяет обеспечить сетевую связанность Сервера администрирования с этими устройствами.

В этой статье описан сценарий настройки и проверки узла Kaspersky Industrial CyberSecurity for Networks для работы в качестве шлюза соединения в Kaspersky Security Center. Сценарий состоит из следующих этапов:

1. **Установка Агента администрирования на узле**

На узле Сервера Kaspersky Industrial CyberSecurity for Networks Агент администрирования устанавливается автоматически, если при установке Сервера добавлена функциональность взаимодействия программы с Kaspersky Security Center. После добавления функциональности взаимодействия вам нужно включить и настроить эту функциональность в Kaspersky Industrial CyberSecurity for Networks.

Включение и настройку функциональности взаимодействия в Kaspersky Industrial CyberSecurity for Networks нужно выполнить до настройки конфигурации Агента администрирования на Сервере для работы в качестве шлюза соединения. Если включение функциональности взаимодействия выполнено после настройки конфигурации Агента администрирования на Сервере, это приводит к сбросу заданных параметров конфигурации и к выключению роли шлюза соединения на этом узле. В этом случае для возобновления работы узла в качестве шлюза соединения вам потребуется заново выполнить этапы данного сценария, начиная с этапа настройки конфигурации Агента администрирования.

На узле сенсора Агент администрирования по умолчанию не устанавливается при централизованной или локальной установке компонентов Kaspersky Industrial CyberSecurity for Networks. Если на узле сенсора не установлен Агент администрирования, установите его с помощью пакета для установки klnagent64-<номер версии Агента администрирования>.x86_64.rpm, который сохраняется в директории kics4net-release_<номер версии программы>/linux-centos при подготовке к установке программы.

Для установки Агента администрирования вам нужно выполнить следующие действия на компьютере с установленным сенсором:

1. Скопируйте в произвольную директорию файл пакета для установки Агента администрирования klnagent64-<номер версии Агента администрирования>.x86_64.rpm.

2. В консоли операционной системы перейдите в директорию, в которой находится файл пакета, и введите команду:

   ```
   sudo rpm -i klnagent64-<номер версии Агента администрирования>.x86_64.rpm
   ```

Дождитесь завершения установки Агента администрирования.

2 Разрешение использования портов

На этом этапе вам нужно разрешить использование портов в межсетевом экране на компьютере узла с установленным Агентом администрирования. Для разрешения использования портов вы можете использовать следующие команды:

```
sudo firewall-cmd --permanent --add-port=13000/tcp
sudo firewall-cmd --permanent --add-port=13295/tcp
sudo systemctl restart firewalld
```

3 Настройка конфигурации Агента администрирования

В результате выполнения этого этапа на Агенте администрирования будет активирован режим шлюза соединения. При активации этого режима с последующим добавлением узла в качестве точки распространения в Kaspersky Security Center изменяется идентификационная и аутентификационная информация для использования этого устройства в качестве шлюза соединения.

Изменение идентификационной и аутентификационной информации приводит к тому, что для использования новой точки распространения в качестве шлюза соединения в ранее настроенной сети вам потребуется переустановить Агент администрирования на всех устройствах, которые вы хотите подключить к вновь добавленному шлюзу соединения. В том числе на тех устройствах, которые ранее использовали этот узел в качестве шлюза соединения. До переустановки Агента администрирования на этих устройствах возможность их подключения к вновь добавленному шлюзу соединения будет недоступна.

Для активирования режима шлюза соединения на Агенте администрирования вам нужно выполнить следующие действия на компьютере узла:

1. Запустите послеустановочный скрипт для настройки конфигурации локальной среды Агента администрирования. Для этого введите команду:

   ```
   sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

2. Внимательно прочитайте Лицензионное соглашение. Для переходов к следующим экранам с текстом Лицензионного соглашения нажимайте на клавишу **Пробел**.

3. По окончании просмотра, если вы полностью согласны с условиями Лицензионного соглашения, примите его условия. Для этого введите символ `y`.

4. Введите имя или IP-адрес Сервера администрирования.

5. При необходимости измените заданные по умолчанию порты для незашифрованных и зашифрованных подключений к Серверу администрирования.

6. Выберите режим для подключений к Серверу администрирования. Для этого введите соответствующий символ:

   `y` – подключения по защищенному SSL-протоколу;

   `n` – незашифрованные подключения.

7. На шаге с запросом режима работы Агента администрирования выберите параметр **Использовать как шлюз соединения** (**Use as connection gateway**).

8. Дождитесь завершения работы скрипта. Через 2–3 минуты после завершения работы скрипта проверьте подключение Агента администрирования к Серверу администрирования. Для этого введите команду:

   ```
   sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

На экране отобразится информация о подключении к Серверу администрирования. При успешном применении заданной конфигурации на экране отображаются следующие сообщения:

```
HostId: < ID в виде буквенно-цифровой последовательности >

This host was installed as a connection gateway, but not yet registered on server

Connecting to server...OK

Connecting to the Administration Agent...OK
```

4 Добавление узла в качестве точки распространения в Kaspersky Security Center

Узел Kaspersky Industrial CyberSecurity for Networks начнет выполнять функции шлюза соединения после его добавления в качестве точки распространения в Kaspersky Security Center. Для этого вам нужно выполнить следующие действия:

1. Подключитесь к Серверу администрирования Kaspersky Security Center.

2. В дереве консоли откройте контекстное меню узла **Сервер администрирования** и выберите пункт **Свойства**.

3. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.

4. В правой части окна выберите параметр **Вручную назначать точки распространения** и нажмите на кнопку **Добавить**.

   Откроется окно **Добавление точки распространения**.

5. Для указания устройства, которое будет выполнять роль точки распространения, выберите вариант добавления шлюза соединения и введите IP-адрес или имя компьютера узла Kaspersky Industrial CyberSecurity for Networks.

6. Для указания области действия точки распространения выберите вариант **Группа администрирования** и укажите группу администрирования, устройства из которой будут использовать шлюз соединений.

7. После добавления узла в список точек распространения убедитесь, что для этого узла включено постоянное соединение с Сервером администрирования. Для этого откройте окно свойств узла и проверьте наличие флажка **Не разрывать соединение с Сервером администрирования** в разделе **Общие**. Флажок должен быть установлен автоматически, его не следует снимать или устанавливать вручную.

5 **Проверка успешного соединения Агента администрирования с Kaspersky Security Center**

Вы можете проверить успешность выполненных действий по добавлению шлюза соединения и точки распространения на компьютере узла. Для этого введите команду:

```
sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

На экране отобразится информация о подключении к Серверу администрирования. При успешном выполнении действий на экране отображаются следующие сообщения:

```
Host is a connection gateway

Host is a distribution point

Connection with server: active

CG connection with server: active
```

Файлы для импорта проекта универсального формата

Вы можете использовать проект универсального формата для импорта в Kaspersky Industrial CyberSecurity for Networks конфигураций параметров контроля процесса для устройств и тегов. Импорт из проекта универсального формата выполняется с помощью текстовых файлов с разделителями (csv-файлов). Формат CSV – это текстовый формат для представления табличных данных.

Вы можете создавать файлы данных любым удобным для вас способом (например, из систем SCADA). Для импорта в программу созданные файлы нужно упаковать в ZIP-архив.

Набор файлов для импорта проекта универсального формата может состоять из следующих CSV-файлов:

- devices.csv. Содержит описания устройств.
- connections.csv. Содержит описания соединений.

  Соединение – это именованная связь между устройством, набором протоколов устройства и набором тегов устройства, передаваемых через эти протоколы.

- variables.csv. Содержит описания переменных и тегов для соединений.
- enums.csv. Содержит описания перечислений для стандарта IEC 61850.
- datasets.csv. Содержит описания наборов данных для стандарта IEC 61850.
- iec61850_mms_reports.csv. Содержит описания отчетов для протокола IEC 61850: MMS.

С помощью проекта универсального формата невозможно импортировать теги протоколов MMS и GOOSE стандарта IEC 61850 в исходном структурном виде тегов. Если тег содержит структуру полей, каждое поле этой структуры требуется описать как отдельный тег для программы. Для добавления в программу тегов в структурном виде используйте специально предназначенный тип проекта: **проект для устройств IEC 61850**.

При использовании файлов данных учитывайте следующие особенности:

- Файлы данных должны быть в кодировке UTF-8.
- Список тегов в файле variables.csv имеет группирующий признак "соединение".
- Для одного соединения в файле connections.csv можно указать несколько разных протоколов и адресов.
- Протокол может иметь один или несколько адресов.
- Одно устройство может иметь несколько соединений с разными наборами тегов.
- При импорте файлов данных учитываются только значения указанных параметров. Параметры, значения которых не указаны, пропускаются. Если в файле данных отсутствуют строки, на которые ссылается другой файл из набора файлов данных, то при импорте отсутствующие строки пропускаются.
- Строки, содержащие значения параметров, в файлах enums.csv и datasets.csv заполняются только при описании перечислений и наборов данных для протоколов MMS и GOOSE стандарта IEC 61850. Для других протоколов файлы enums.csv и datasets.csv могут содержать только заголовочные строки. При этом файлы enums.csv и datasets.csv должны присутствовать в наборе файлов для импорта.

Файл описания устройств: devices.csv

Файл описания устройств содержит перечисление устройств, их типов и идентификаторов соединений. Идентификатор соединения, указанный в файле описания устройств, задается в файле описания соединений и используется для связи протоколов с устройствами.

Если вы используете разные протоколы с разными наборами тегов, то нужно использовать несколько соединений для одного устройства. Идентификаторы соединений в каждой строке файла devices.csv должны быть уникальными.

В начале файла должны быть указаны заголовочные строки, которые содержат необходимые данные для обработки файла. Пример заголовочных строк файла devices.csv приведен ниже.

Пример:

```
'Devices
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Device;Type;Connection
```

Заголовочные строки файла devices.csv содержат следующие значения:

- `Devices`

  В этой строке указано имя csv-файла. `Devices` – это имя файла описания устройств. Имя файла данных соответствует назначению файла и определено для каждого файла в наборе.

- `Format Version;KICS Importer Version`

  В этой строке указаны версия формата файла и версия инструмента, с помощью которого файл был создан. Для параметра `Format version` задайте значение V1.0.0.0. Далее рекомендуется указать имя и версию инструмента, с помощью которой был создан csv-файл.

- `Field separator: ; Decimal separator: . Text quotes: " Var name separator: .`

  В этой строке указаны разделители, которые используются в файле данных:

  - разделитель полей: `Field separator: ;`
  - разделитель целой и дробной части: `Decimal separator: .`
  - ограничитель строк: `Text quotes: "`
  - разделитель полей в имени тега: `Var name separator: .`

- `Device;Type;Connection`

  В этой строке указаны наименования столбцов с данными. Данные в файле должны следовать согласно указанному порядку следования столбцов:

  - `Device` – имя устройства.
  - `Type` – код типа устройства. Используются следующие коды:
    - 0 – SIEMENS SIMATIC S7-300;
    - 1 – SIEMENS SIMATIC S7-400;
    - 2 – SCHNEIDER ELECTRIC MOMENTUM;
    - 3 – SCHNEIDER ELECTRIC M340;
    - 4 – MITSUBISHI SYSTEM Q;
    - 5 – ALLEN-BRADLEY CONTROL LOGIX 5000;
    - 6 – SIEMENS SIPROTEC;
    - 7 – IEC 61850 GOOSE, MMS device;
    - 8 – IEC 60870-5-104 device;
    - 9 – ABB RELION 670;
    - 10 – GENERAL ELECTRIC RX3I;
    - 11 – SIEMENS SIMATIC S7-1500;
    - 12 – IEC 61850 SAMPLED VALUES device;
    - 13 – SIEMENS SIPROTEC 6MD66;
    - 14 – SIEMENS SIPROTEC 7SS52;
    - 15 – SIEMENS SIPROTEC 7UM62;
    - 16 – SIEMENS SIPROTEC 7SA52;
    - 17 – SIEMENS SIPROTEC 7SJ64;

- 18 – SIEMENS SIPROTEC 7UT63;
- 19 – GENERAL ELECTRIC MULTILIN B30;
- 20 – GENERAL ELECTRIC MULTILIN C60;
- 21 – EMERSON DELTAV;
- 22 – SCHNEIDER ELECTRIC M580;
- 23 – RELEMATIKA TOR 300;
- 24 – EKRA 200 series;
- 25 – EKRA BE2704 / BE2502;
- 26 – OMRON CJ2M;
- 27 – ABB AC 800M;
- 28 – YOKOGAWA CENTUM;
- 29 – CODESYS V3 based device;
- 30 – DNP3 device;
- 31 – OPC UA server;
- 32 – ABB AC 700F;
- 33 – SIEMENS SIMATIC S7-1200;
- 34 – OPC DA server;
- 35 – BECKHOFF CX series;
- 36 – PROSOFT-SYSTEMS REGUL R500;
- 37 – EMERSON CONTROLWAVE;
- 38 – IEC 60870-5-101 device;
- 39 – MOXA NPORT IA 5000 series;
- 40 – I/O device;
- 41 – ABB RELION REF615;
- 42 – SIEMENS SIMATIC S7-200;
- 43 – MODBUS TCP device;
- 44 – SCHNEIDER ELECTRIC SEPAM 80 NPP;
- 45 – YOKOGAWA PROSAFE-RS;

- 46 – SCHNEIDER ELECTRIC FOXBORO FCP280 / FCP270;
- 47 – HONEYWELL CONTROLEDGE 900 series;
- 48 – HONEYWELL EXPERION C300;
- 49 – SCHNEIDER ELECTRIC MICOM C264;
- 50 – UMAS device;
- 51 – TASE.2 server;
- 52 – PROFINET device;
- 53 – DIRECTLOGIC;
- 54 – Server with encryption support;
- 55 – BACNET device;
- 56 – SCHNEIDER ELECTRIC P545;
- 57 – YCU/ELC;
- 58 – FEU device;
- 59 – Generic IED;
- 60 – Generic Gateway;
- 61 – Generic PLC;
- 62 – VALMET DNA device;
- 63 – IPU device;
- 64 – OWEN PLC100 series;
- 65 – CODESYS V2 based device;
- 66 – PNU20 device;
- 67 – KNX device;
- 68 – DTS device;
- 69 – B&R;
- 70 – SIEMENS SICAM PAS server.

- `Connection` – идентификатор соединения из файла описания соединений connections.csv.

После заголовочных строк следует тело файла, содержащее значения параметров (имя устройства, код типа устройства, идентификатор соединения). Пример файла devices.csv приведен ниже.

Пример:

```
'Devices
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Device;Type;Connection
"ms_plc";4;"ms_plc"
"mc_SysQ";8;"mc_SysQ"
```

Файл описания соединений: connections.csv

Файл описания соединений содержит идентификаторы соединений, коды протоколов прикладного уровня и полные сетевые адреса устройств.

В начале файла должны быть указаны заголовочные строки, которые содержат необходимые данные для обработки файла. Пример заголовочных строк файла connections.csv приведен ниже.

Пример:

```
'Connections

'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0

'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .

'Connection;Protocol;Address
```

Первые три заголовочные строки аналогичны заголовочным строкам в файле devices.csv.

Строка `Connection;Protocol;Address` содержит наименования столбцов с данными:

- `Connection` – идентификатор соединения для файлов описаний.

  Идентификатор соединения используется для связи протоколов с устройствами и тегами.

- `Protocol` – код протокола прикладного уровня. Используются следующие коды протоколов:
  - 0 – MODBUS TCP;
  - 1 – SIEMENS S7COMM over TCP;
  - 2 – SIEMENS S7COMM over INDUSTRIAL ETHERNET;
  - 3 – MITSUBISHI MELSEC SYSTEM Q;
  - 4 – ALLEN-BRADLEY ETHERNET/IP;
  - 5 – IEC 61850 MMS;
  - 6 – IEC 61850 GOOSE;
  - 7 – IEC 60870-5-104;
  - 8 – GENERAL ELECTRIC SRTP;
  - 9 – IEC 61850 SAMPLED VALUES;
  - 10 – SIEMENS S7COMMPLUS over TCP;
  - 11 – EMERSON DELTAV;
  - 12 – OMRON FINS over UDP;
  - 13 – MMS for ABB AC 800M;
  - 14 – YOKOGAWA VNET/IP;
  - 15 – CODESYS V3 GATEWAY over TCP;
  - 16 – DNP3;
  - 17 – OMRON FINS over TCP;
  - 18 – OPC UA BINARY;
  - 19 – DMS for ABB AC 700F;
  - 20 – OPC DA;
  - 21 – OMRON FINS over ETHERNET/IP;
  - 22 – CODESYS V3 GATEWAY over UDP;
  - 23 – BECKHOFF ADS/AMS;

- 24 – IEC 60870-5-101;
- 25 – FOXBORO FCP280 / FCP270 INTERACTION;
- 26 – BSAP;
- 27 – HONEYWELL CONTROLEDGE 900 INTERACTION;
- 28 – WMI INTERACTION;
- 29 – HONEYWELL EXPERION INTERACTION;
- 30 – MiCOM C264 INTERACTION;
- 31 – SCHNEIDER ELECTRIC UMAS;
- 32 – TASE.2;
- 33 – PROFINET IO;
- 34 – DIRECTLOGIC INTERACTION;
- 35 – BACNET;
- 36 – YARD;
- 37 – COS;
- 38 – IPU-FEU INTERACTION;
- 39 – VALMET DNA INTERACTION;
- 40 – CODESYS V2;
- 41 – PNU20;
- 42 – GENERAL ELECTRIC EGD;
- 43 – KNXnet/IP;
- 44 – DTS;
- 45 – INA2000;
- 46 – SIEMENS SICAM SCC - INTERACTION with SICAM PAS.

- `Address` – строка, содержащая полный сетевой адрес устройства, специфичный для указанного протокола.

  Пример:
  Соединение с контроллером Schneider Momentum (один IP-адрес):
  `"Barline1";0;"IP-Address=192.168.0.7;Port=502"`

  Соединение с контроллером Mitsubishi System Q (один IP-адрес, два порта):
  `"Station1";3;"IP-Address=192.168.0.8;Port=5001 Network=0;Station=0;PC=255"`
  `"Station1";3;"IP-Address=192.168.0.8;Port=5002 Network=0;Station=0;PC=255"`

Соединение с резервируемым контроллером Siemens S7-400, два контроллера (два IP-адреса, один набор тегов):

```
"S7$Program";1;"IP-Address=192.168.0.21;Port=102;Rack=0;Slot=2"
"S7$Program";1;"IP-Address=192.168.0.22;Port=102;Rack=0;Slot=2"
```

Соединение с контроллером Siemens S7-400, используется два протокола: S7Comm поверх стека TCP/IP и S7Comm поверх сети Industrial Ethernet (один набор тегов):

```
"S7$Program";1;"IP-Address=192.168.0.21;Port=102;Rack=0;Slot=2"
"S7$Program";2;"MAC=00:01:02:03:04:05;Rack=0;Slot=2"
```

После заголовочных строк следует тело файла, содержащее значения параметров (идентификатор соединения, код протокола прикладного уровня, полный сетевой адрес устройства). Пример файла connections.csv приведен ниже.

Пример:

```
'Connections
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;Protocol;Address
"ms_plc";3;"IP-Address=192.168.0.77;Port=1025"
"mc_SysQ";7;"IP-Address=192.168.0.77;Port=2404;Asdu=555"
```

Формат сетевого адреса устройства в файле connections.csv зависит от типа используемого протокола.

Пример:

Для поддерживаемых в Kaspersky Industrial CyberSecurity for Networks протоколов могут использоваться следующие форматы адреса:

- MODBUS TCP:

  `"IP-Address=192.168.0.7;Port=502"`

- SIEMENS S7COMM over TCP:

  `"IP-Address=192.168.0.7;Port=502;Rack=0;Slot=2"`

- SIEMENS S7COMM over INDUSTRIAL ETHERNET:

  `"MAC=00:01:02:03:04:05;Rack=0;Slot=2"`

- MITSUBISHI MELSEC SYSTEM Q:

  `"IP-Address=192.168.0.7;Port=502;Network=0;Station=0;PC=255"`

- ALLEN-BRADLEY ETHERNET/IP:

  `"IP-Address=192.168.0.7;Port=44818"`

- IEC 61850 MMS:

  `"IP-Address=192.168.0.7;Port=502;Domains=IED_0009CTRL,IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"`

- IEC 61850 GOOSE:

  `"Domains=IED_0009CTRL,IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"`

- IEC 60870-5-104:

  `"IP-Address=192.168.0.7;Port=104;Asdu=2"`

- GENERAL ELECTRIC SRTP:

  `"IP-Address=192.168.0.50;Port=18245"`

- IEC 61850 SAMPLED VALUES:

  `"MAC=00:01:02:03:04:05;Domains=IED_TRANSFORMER1;Vendor=TMW;Model=IED"`

- SIEMENS S7COMMPLUS over TCP:

  `"IP-Address=192.168.0.22;Port=102"`

- EMERSON DELTAV:

  `"IP-Address=192.168.0.38;Port=18507"`

- OMRON FINS over UDP:

  `"IP-Address=192.168.0.1;Port=9600"`

- MMS for ABB AC 800M:

  `"IP-Address=192.168.0.60;Port=102"`

- YOKOGAWA VNET/IP:

  `"IP-Address=192.168.0.4;Port=5313"`

- CODESYS V3 GATEWAY over TCP:
  `"IP-Address=192.168.0.4;Port=11740"`
- DNP3:
  `"IP-Address=192.168.1.10;Port=20000"`
- OMRON FINS over TCP:
  `"IP-Address=192.168.0.1;Port=9600"`
- OPC UA BINARY:
  `"IP-Address=192.168.0.213;Port=49320"`
- DMS for ABB AC 700F:
  `"IP-Address=192.168.0.7;Port=9991"`
- OMRON FINS over ETHERNET/IP:
  `"IP-Address=192.168.0.1;Port=44818"`
- OPC DA:
  `"IP-Address=192.168.0.7;Port=135"`
- WMI INTERACTION:
  `"IP-Address=192.168.0.7;Port=135"`
- CODESYS V3 GATEWAY over UDP:
  `"IP-Address=192.168.0.7;Port=1740"`
- BECKHOFF ADS/AMS:
  `"IP-Address=192.168.0.7;Port=48898"`
- IEC 60870-5-101:
  `"IP-Address=192.168.0.7;Port=950"`
- FOXBORO FCP270, FCP280 INTERACTION:
  `"MAC=00:00:6C:C0:00:0A"`
- BSAP:
  `"IP-Address=192.168.0.7;Port=1234"`
- HONEYWELL CONTROLEDGE 900 INTERACTION:
  `"IP-Address=192.168.1.99;Port=41103"`
- HONEYWELL EXPERION INTERACTION:
  `"IP-Address=192.168.1.10;Port=55553"`
- SCHNEIDER ELECTRIC UMAS:
  `"IP-Address=192.168.0.7;Port=502"`

- TASE.2:
  `"IP-Address=192.168.0.20;Port=102"`
- PROFINET IO:
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.0.20\;Frame=IDS_TEL352"`
- DIRECTLOGIC INTERACTION:
  `"IP-Address=192.168.0.70;Port=28784"`
- BACNET:
  `"IP-Address=192.168.5.200;Port=47808"`
- YARD:
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.12.1\;Port=2002"`
- COS:
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.1.131\;Port=3077"`
- IPU-FEU INTERACTION:
  `"IP-Address=192.168.5.200;Port=57005"`
- VALMET DNA INTERACTION:
  `"IP-Address=192.168.10.11;Port=2519"`
- CODESYS V2:
  `"IP-Address=192.168.7.200;Port=1210"`
- PNU20:
  `"IP-Address=192.168.7.200;Port=43962"`
- GENERAL ELECTRIC EGD:
  `"IP-Address=192.168.0.51;Port=18246"`
- KNXnet/IP:
  `"IP-Address=192.168.10.76;Port=3671"`
- DTS:
  `"IP-Address=192.168.50.11;Port=30000"`
- INA2000:
  `"IP-Address=192.168.1.1;Port=11159"`
- SIEMENS SICAM SCC - INTERACTION with SICAM PAS:
  `"IP-Address=192.168.50.01;Port=10501"`

Файл описания переменных и тегов: variables.csv

Файл описания переменных и тегов содержит перечисления тегов, их параметров и соединений, с которыми связаны теги.

В начале файла должны быть указаны заголовочные строки, которые содержат данные для обработки файла. Пример заголовочных строк файла variables.csv приведен ниже.

Пример

```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
```

Первые три заголовочные строки аналогичны заголовочным строкам в файле devices.csv.

Строка `ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;E` содержит наименования столбцов с данными:

- `ID` – уникальный числовой идентификатор тега.

  Идентификатор тега нужен для создания ссылок на тег в файле datasets.csv.

- `Varname` – полное имя тега (например, `Drain.8450PT00058.value20`).

- `Connection` – идентификатор соединения, с которым связан тег.

  Идентификатор соединения задается в файле описания соединений и используется для связи протоколов с тегами.

- `Address` – адрес тега в строковом виде.

  Адрес зависит от типа протокола, с которым связан тег (например, для протокола S7comm значение адреса – `M2.7`, `DB575:82.0`, для протокола Modbus TCP значение адреса – `400537`, `123`, `300001`).

- `Datatype` – числовой код типа данных тега. Используются следующие коды:
  - 0 – BOOL;
  - 1 – INT8;
  - 2 – UINT8;
  - 3 – INT16;
  - 4 – UINT16;
  - 5 – INT32;
  - 6 – UINT32;
  - 7 – INT64;
  - 8 – UINT64;
  - 9 – FLOAT;
  - 10 – DOUBLE;
  - 11 – STRING;
  - 12 – ENUM;
  - 13 – BOOL ARRAY;
  - 14 – UNSPECIFIED.
- `Length` – длина строки в байтах для тега строкового типа (string).
- `InLo;InHi;OutLo;OutHi` – параметры для масштабирования значения тега.

  Если значения всех параметров для масштабирования равны нулю, то масштабирование значения тега не используется. Если заданы числовые значения параметров, то для расчета значения тега применяется следующая формула: TagValue = OutLo + (TagValue – InLo) * (OutHi – OutLo) / (InHi – InLo), где TagValue – это значение тега.
- `Description` – описание тега (например, "Давление пара на выходе котла №1").
- `EngUnits` – единицы измерения физической величины, которая соответствует тегу (например, м/с, Дж).
- `EnumName` – имя перечисления из файла enums.csv, которое определяет значение тега.

  Поле `EnumName` может быть заполнено для тегов с типами данных ENUM, INT* или UINT*. Поле `EnumName` содержит ссылку на перечисление из файла enums.csv.

  Пример:
  Поле `EnumName` в файле variables.csv:
  `EnumName = "OnOffSwitch"`
  Описание перечисления в файле enums.csv:
  `"OnOffSwitch"; 0; " Включено "`
  `"OnOffSwitch"; 1; " Отключено "`

После заголовочных строк следует тело файла, содержащее значения параметров (например, идентификатор тега, имя тега, идентификатор соединения). Пример файла variables.csv приведен ниже.

Пример:

```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
5;"System.mitsub_n.ms_plc.Bit01";"ms_plc";"W0";4;0;0;0;0;0;"System.mitsub_n.ms_plc.Bit01";"";""
6;"System.mitsub_n.ms_plc.Register01";"ms_plc";"W20";9;0;0;0;0;0;"System.mitsub_n.ms_plc.Register01";"";""
1;"systemQ.Bit01";"mc_SysQ";"10";0;0;0;0;0;0;"systemQ.Bit01";"";""
```

Структура адреса тега в поле `Address` зависит от используемого протокола.

Для поддерживаемых протоколов используются следующие структуры адреса:

- MODBUS TCP: целое число (например, адреса дискретных входов (Discrete inputs): от 100001).
- SIEMENS S7COMM over TCP и S7COMM over INDUSTRIAL ETHERNET: строка вида `[Area][ByteAddress].[BitAddress]`.

  Если выполняется условие `MemArea=DataBlocks`, то к адресу добавляется номер блока данных. Строка принимает вид `[DB17]:[ByteAddress].[BitAddress]`, где:

  - `Area` – перечисление кодов области памяти в соответствии со стандартом протокола: M, I, O, DB, C, T.
  - `ByteAddress` – адрес регистра, представленный целым числом.
  - `BitAddress` – адрес бита внутри регистра, представленный целым числом.
- MITSUBISHI MELSEC SYSTEM Q: строка вида `[Area][Address]`, где:
  - `Area` – перечисление кодов области памяти в соответствии со спецификацией протокола: SM, SD, M, L, F, V, D, TS, TC, TN, SS, SC, SN, CS, CC, CN, S, Z, R, X, Y, B, W, SB, SW, DX, DY, ZR.
  - `Address` – значение адреса. Адрес представляет собой целое число в диапазоне, который зависит от области данных.
- ALLEN-BRADLEY ETHERNET/IP: строка с именем тега.
- IEC 61850 MMS и GOOSE: согласно стандарту IEC 61850 – строка вида `DOMAIN=Domain;LN=LnName;CO=CoName;DA=FullTagName;CDC=CdcName;LNCDC=LNClassName`, где:
  - `DOMAIN` – параметр, который включает в себя имя устройства и имя логического устройства (logical device name).
  - `LN` – имя логического узла (logical node name).
  - `CO` – имя функциональной ссылки (functional constraint name).
  - `DA` – имя тега (tag name).
  - `CDC` – имя класса общих данных атрибута (attribute common data class name).
  - `LNCDC` – имя класса общих данных логического узла (logical node common data class name).

- IEC 60870-5-104 и IEC 60870-5-101: строка вида `[ASDU]:[Address]`, где:
  - `ASDU` – номер ASDU, представленный целым числом.
  - `Address` – номер объекта InformationObject, представленный целым числом.
- GENERAL ELECTRIC SRTP: строка вида `[Area][ByteAddress].[BitAddress]`, где:
  - `Area` – перечисление кодов области памяти в соответствии со стандартом протокола: I, Q, T, M, G, AI, AQ, R, P, L, W.
  - `ByteAddress` – адрес регистра, представленный целым числом.
  - `BitAddress` – адрес бита внутри регистра, представленный целым числом.
- SIEMENS S7COMMPLUS over TCP: строка вида `LID=LidValue;RID=RidValue`, где `LidValue` и `RidValue` – внутренние идентификаторы тега в проекте TiaPortal.
- EMERSON DELTAV: строка с именем тега.
- OMRON FINS over UDP, OMRON FINS over TCP и OMRON FINS over ETHERNET/IP: строка вида `[Area][ByteAddress].[BitAddress]`, где:
  - `Area` – перечисление кодов области памяти в соответствии со стандартом протокола: A, CIO, C, CS, D, DR, E, H, IR, TK, T, TS, W.
  - `ByteAddress` – адрес регистра, представленный целым числом.
  - `BitAddress` – адрес бита внутри регистра, представленный целым числом.
- YOKOGAWA VNET/IP: строка с именем тега.
- DNP3: строка вида `[GROUP]:[INDEX]`, где:
  - `GROUP` – группа.
  - `INDEX` – индекс.
- DMS for ABB AC 700F: целое число.
- MMS for ABB AC 800M: строка вида `[Application]:[POUInstance].[VarOffset]`, где:
  - `Application` – название приложения.
  - `POUInstance` – экземпляр POU.
  - `VarOffset` – смещение переменной.
- CODESYS V3 GATEWAY over TCP и CODESYS V3 GATEWAY over UDP: строка с именем тега.
- OPC UA BINARY: строка с именем тега.
- OPC DA: строка с именем тега.

- BSAP: строка вида `[MSD_VERSION]:[MSD]`, где:
  - `MSD_VERSION` – целое число в диапазоне 0–65535, используемое для сравнения версий проектов/тегов в ПЛК и SCADA-системе.
  - `MSD` – идентификатор тега, представленный целым числом в диапазоне 0–65535.
- FOXBORO FCP280 / FCP270 INTERACTION: строка с именем тега.
- HONEYWELL EXPERION INTERACTION: строка вида `[BLOCK_ID]:[SUBBLOCK_ID]:[PROPERTY_ID]`, где:
  - `BLOCK_ID` – порядковый номер блока в программе ПЛК, представленный целым числом в диапазоне 0–65535.
  - `SUBBLOCK_ID` – порядковый номер вложенного блока в программе ПЛК, представленный целым числом в диапазоне 0–65535.
  - `PROPERTY_ID` – порядковый номер параметра блока в программе ПЛК, представленный целым числом в диапазоне 0–65535.
- DIRECTLOGIC INTERACTION: строка вида `[Area][ByteAddress].[BitAddress]`, где:
  - `Area` – перечисление кодов области памяти в соответствии со спецификацией протокола: X, Y, C, S, T, CT, GX, GY, V, P, SP, B, PB.
  - `ByteAddress` – адрес регистра, представленный целым числом.
  - `BitAddress` – адрес бита внутри регистра, представленный целым числом.
- BACNET: строка вида `[OBJECT_TYPE]:[OBJECT_ID]`, где:
  - `OBJECT_TYPE` – тип объекта в соответствии со спецификацией протокола.
  - `OBJECT_ID` – порядковый номер объекта, представленный целым числом в диапазоне 0–4194303.
- PROFINET IO: строка вида `[IO]:[SubSlot]:[Index]:[Offset].[BitAddress]`, где:
  - `IO` – направление переменной (input, output).
  - `SubSlot` – номер подслота, представленный целым числом.
  - `Index` – индекс тега, представленный целым числом.
  - `Offset` – адрес байта тега, представленный целым числом.
  - `BitAddress` – адрес бита внутри регистра, представленный целым числом (используется только для тегов с типом данных bool).

  Кроме того, для правильной загрузки параметров протокола требуется указать файл GSDML, специфичный для устройства.

- YARD: строка вида `[Controller Address]:[Index]:[Size]:[Config]:[MessageType]`, где:
  - `Controller Address` – адрес объектного контроллера, представленный целым шестнадцатеричным числом.
  - `Index` – битовый индекс тега, представленный целым числом.
  - `Size` – битовый размер, представленный целым числом.
  - `Config` – положение перемычек на объектном контроллере, представленное целым шестнадцатеричным числом.
  - `MessageType` – тип сообщения (`Order` или `Status`).

  Кроме того, для правильной загрузки параметров протокола может потребоваться указать файлы конфигурации, специфичные для устройства.
- COS: строка вида `[Object ID]:[Variable ID]`, где:
  - `Object ID` – идентификатор объекта, представленный целым числом.
  - `Variable ID` – идентификатор переменной, представленный целым числом.

  Кроме того, для правильной загрузки параметров протокола требуется указать файл конфигурации станции. Для файла должно быть указано имя specific.zip.
- VALMET DNA INTERACTION: строка с именем тега.

  Кроме того, для правильной загрузки параметров протокола требуется указать файл, содержащий журнал загрузки ПЛК. Для файла должно быть указано имя specific.zip.
- PNU20: целое число в диапазоне 0–65535.
- GENERAL ELECTRIC EGD: строка вида `[ExchangeId]:[RefAddress]`, где:
  - `ExchangeId` – идентификатор подписки, представленный целым числом в диапазоне 0–4294967295.
  - `RefAddress` – смещение адреса тега (в байтах), представленное целым числом в диапазоне 0–65535.
- KNXnet/IP: целое число в диапазоне 0–65535.
- SIEMENS SICAM SCC - INTERACTION with SICAM PAS: целое число в диапазоне 0–65535.

Файл описания перечислений: enums.csv

Файл описания перечислений содержит все элементы всех перечислений, используемых в текущем наборе файлов данных для стандарта IEC 61850.

В начале файла должны быть указаны заголовочные строки, которые содержат данные для обработки файла. Пример заголовочных строк файла enums.csv приведен ниже.

Пример:

```
'Enums
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;EnumName;IntValue;TextValue
```

Первые три заголовочные строки аналогичны заголовочным строкам в файле devices.csv.

Строка `Connection;EnumName;IntValue;TextValue` содержит наименования столбцов с данными:

- `Connection` – идентификатор соединения, к которому относится этот элемент.
- `EnumName` – имя перечисления.
- `IntValue` – числовое значение перечисления.
- `TextValue` – текстовое описание, которое соответствует числовому значению перечисления.

После заголовочных строк следует тело файла, содержащее значения параметров (идентификатор соединения, имя перечисления, числовое значение перечисления, текстовое описание). Пример файла enums.csv приведен ниже.

Пример:

```
'Enums
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;EnumName;IntValue;TextValue
"AA1J1Q01A2";"Beh";1;"on"
"AA1J1Q01A2";"Beh";2;"blocked"
"AA1J1Q01A2";"Beh";3;"test"
"AA1J1Q01A2";"Beh";4;"test/blocked"
"AA1J1Q01A2";"Beh";5;"off"
```

Файл описания наборов данных (группы тегов): datasets.csv

Файл описания наборов данных (группы тегов) содержит параметры наборов данных (dataset) для протоколов стандарта IEC 61850.

В начале файла должны быть указаны заголовочные строки, которые содержат данные для обработки файла. Пример заголовочных строк файла datasets.csv приведен ниже.

Пример:

```
'Datasets
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;DatasetName;Deprecated;ItemName
```

Первые три заголовочные строки аналогичны заголовочным строкам в файле devices.csv.

Строка `Connection;DatasetName;Deprecated;ItemName` содержит наименования столбцов с данными:

- `Connection` – идентификатор соединения, к которому относится файл datasets.csv.
- `DatasetName` – имя набора данных.

- `Deprecated` – неиспользуемые данные (нулевое значение).
- `ItemName` – полное имя элемента модели устройства. Это может быть конечное имя тега или имя верхней ветки дерева структуры.

После заголовочных строк следует тело файла, содержащее значения параметров (идентификатор соединения, имя набора данных, неиспользуемое значение, имя элемента модели устройства). Пример файла datasets.csv приведен ниже.

Пример:

```
'Datasets
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;DatasetName;Deprecated;ItemName
"S7UTDZD";"S7UTDZDPROT/LLN0$DataSet";0;"S7UTDZDPROT/PTRC1$ST$Tr"
"S7UTDZD";"S7UTDZDPROT/LLN0$DataSet";0;"S7UTDZDMEAS/M1_MMXU1$MX$A$phsA"
```

Файл описания отчетов протокола MMS: iec61850_mms_reports.csv

Файл описания отчетов протокола MMS содержит параметры для сервиса Reports протокола IEC 61850: MMS.

В начале файла должны быть указаны заголовочные строки, которые содержат данные для обработки файла. Пример заголовочных строк файла iec61850_mms_reports.csv приведен ниже.

Пример:

```
'Reports
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;ReportName;ReportId;DataSetName;IsBuffered
```

Первые три заголовочные строки аналогичны заголовочным строкам в файле devices.csv.

Строка `Connection;ReportName;ReportId;DataSetName;IsBuffered` содержит наименования столбцов с данными:

- `Connection` – идентификатор соединения, к которому относится строка настроек в файле iec61850_mms_reports.csv.
- `ReportName` – имя отчета.
- `ReportId` – идентификатор отчета.
- `DataSetName` – имя набора данных, связанного с этим отчетом.
- `IsBuffered` – признак, является отчет буферизированным или нет. Принимает значения `Buffered` или `Unbuffered`.

После заголовочных строк следует тело файла, содержащее значения параметров (идентификатор соединения, имя отчета, идентификатор отчета, имя набора данных для отчета, признак буферизации). Пример файла iec61850_mms_reports.csv приведен ниже.

Пример:

```
'Reports
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;ReportName;ReportId;DataSetName;IsBuffered
"IED24151LD";"IED24151LD/LLN0$BR$brcbST01";"brcbST01";"IED24151LD/LLN0$DSList";"Buffered"
"IED24151LD";"IED24151LD/LLN0$RP$urcbMX01";"urcbMX01";"IED24151LD/LLN0$MXList";"Unbuffered"
```

Системные типы событий в Kaspersky Industrial CyberSecurity for Networks

Для регистрации событий в Kaspersky Industrial CyberSecurity for Networks используются системные типы событий, автоматически созданные при установке программы.

Каждый тип события относится к определенной технологии регистрации событий.

Системные типы событий по технологии Контроль технологического процесса

В этой статье приведено описание системных типов событий, относящихся к технологии Контроль технологического процесса (см. таблицу ниже).

Системные типы событий по технологии Контроль технологического процесса (DPI)

Код	Заголовок типа события	Условия для регистрации
4000002900	$technology_rule	Сработало правило контроля процесса. В заголовке и в описании системного типа события используются следующие переменные: • $technology_rule – название правила; • $tags – полученные значения тегов, для которых заданы условия в правиле. В зарегистрированном событии для заголовка, описания и оценки события используются пользовательские параметры, заданные в сработавшем правиле контроля процесса.
4000000001	Тестовое событие (DPI)	Обнаружен тестовый сетевой пакет.

Системные типы событий по технологии Контроль системных команд

В этой статье приведено описание системного типа события, относящегося к технологии Контроль системных команд (см. таблицу ниже).

Системный тип события по технологии Контроль системных команд (CC)

Код	Заголовок типа события	Условия для регистрации
4000002602	$systemCommandShort	Обнаружена системная команда, выбранная для отслеживания (при этом для системной команды нет включенного правила контроля взаимодействий). В заголовке и в описании типа события используются следующие переменные: • $systemCommandShort – краткое описание обнаруженной системной команды; • $systemCommandFull – подробное описание обнаруженной системной команды; • $attackTechniques – список возможных техник из базы знаний MITRE ATT&CK, которые могут применять злоумышленники для атак с использованием этой системной команды.

Системные типы событий по технологии Контроль целостности сети

В этой статье приведено описание системных типов событий, относящихся к технологии Контроль целостности сети (см. таблицу ниже).

Системные типы событий по технологии Контроль целостности сети (NIC)

Код	Заголовок типа события	Условия для регистрации
4000002601	Обнаружено неразрешенное сетевое взаимодействие ($top_level_protocol)	Обнаружено сетевое взаимодействие, не указанное во включенном правиле контроля взаимодействий. В заголовке и в описании типа события используются следующие переменные: • $top_level_protocol – название протокола верхнего уровня; • $protocol – название протокола прикладного уровня.
4000002700	Отсутствует трафик на точке мониторинга $monitoringPoint	На сетевой интерфейс, связанный с точкой мониторинга, не поступает трафик более 15 секунд. В заголовке и в описании типа события используются следующие переменные: • $monitoringPoint – название точки мониторинга; • $interface – имя сетевого интерфейса, который связан с точкой мониторинга; • $duration – длительность отсутствия трафика (в секундах).
4000000002	Тестовое событие (NIC)	Обнаружен тестовый сетевой пакет (при включенной технологии Контроль целостности сети).

Системные типы событий по технологии Обнаружение вторжений

В этой статье приведено описание системных типов событий, относящихся к технологии Обнаружение вторжений (см. таблицу ниже).

Системные типы событий по технологии Обнаружение вторжений (IDS)

Код	Заголовок типа события	Условия для регистрации
4000003000	Сработало правило из набора $fileName (системный набор правил)	Сработало правило обнаружения вторжений, входящее в системный набор правил. В заголовке и в описании типа события используются следующие переменные: • $fileName – название набора правил; • $category – класс правила; • $ruleName – название правила; • $signature_id – идентификатор правила (sid).
4000003001	Сработало правило из набора $fileName (пользовательский набор правил)	Сработало правило обнаружения вторжений, входящее в пользовательский набор правил. В заголовке и в описании типа события используются следующие переменные: • $fileName – название набора правил; • $category – класс правила; • $ruleName – название правила; • $signature_id – идентификатор правила (sid); • $action – тип действия с сетевыми пакетами, заданный в правиле (действия типов `drop` или `reject` не выполняются в Kaspersky Industrial CyberSecurity for Networks).
4000003002	Обнаружены признаки подбора или сканирования	Сработало правило обнаружения атак с использованием методов подбора или сканирования. В описании типа события используется переменная $ruleName для названия правила.
4000004001	Обнаружены признаки ARP-спуфинга в ARP-ответах	Обнаружены признаки подмены адресов в ARP-пакетах: несколько ARP-ответов, которые не связаны с ARP-запросами. В описании типа события используются следующие переменные: • $senderIp – подменяемый IP-адрес; • $targetIp – IP-адрес целевого узла; • $attackStartTimestamp – время обнаружения первого ARP-ответа.
4000004002	Обнаружены признаки ARP-спуфинга в ARP-запросах	Обнаружены признаки подмены адресов в ARP-пакетах: несколько ARP-запросов с одного MAC-адреса разным получателям. В описании типа события используются следующие переменные: • $senderIp – подменяемый IP-адрес; • $targetIp – IP-адрес целевого узла; • $attackStartTimestamp – время обнаружения первого ARP-ответа.
4000005100	Обнаружена аномалия в протоколе IP: конфликт данных при сборке IP-пакета	Обнаружена аномалия в протоколе IP: при наложении фрагментов IP-пакета данные не совпадают.
4000005101	Обнаружена аномалия в протоколе IP: превышение размера фрагментированного IP-пакета	Обнаружена аномалия в протоколе IP: фактический суммарный размер фрагментированного IP-пакета после сборки превышает допустимый предел.
4000005102	Обнаружена аномалия в протоколе IP: размер начального фрагмента IP-пакета меньше ожидаемого	Обнаружена аномалия в протоколе IP: размер начального фрагмента IP-пакета меньше минимально допустимого значения.
4000005103	Обнаружена аномалия в протоколе IP: несоответствие фрагментов IP-пакета (mis-associated fragments)	Обнаружена аномалия в протоколе IP: фрагменты собираемого IP-пакета содержат различные данные о длине фрагментированного пакета.
4000002701	Обнаружена аномалия в протоколе TCP: подмена содержимого в перекрывающихся TCP-сегментах	Обнаружена аномалия в протоколе TCP: пакеты содержат перекрывающиеся TCP-сегменты с различающимся содержимым.
4000000003	Тестовое событие (IDS)	Обнаружен тестовый сетевой пакет (при включенном методе обнаружения вторжений по правилам).

Системные типы событий по технологии Контроль активов

В этой статье приведено описание системных типов событий, относящихся к технологии Контроль активов (см. таблицу ниже).

Системные типы событий по технологии Контроль активов (AM)

Код	Заголовок типа события	Условия для регистрации
4000005003	Обнаружено новое устройство с адресом $owner_ip_or_mac	В режиме наблюдения контроля активов автоматически добавлено новое устройство по обнаруженному IP- или MAC-адресу, который не указан для других устройств в таблице. Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Неразрешенное устройство**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – присвоенное имя устройства; • $assigned_mac – присвоенный MAC-адрес (если определен); • $owner_ip – присвоенный IP-адрес (если определен); • $asset_id – идентификатор устройства.
4000005004	Получена новая информация об устройстве с адресом $owner_ip_or_mac	В режиме наблюдения контроля активов автоматически обновлены сведения об устройстве на основе полученных данных из трафика. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $updated_params – список обновленных сведений; • $asset_id – идентификатор устройства.
4000005005	Обнаружен конфликт IP-адреса $owner_ip	В режиме наблюдения контроля активов обнаружено использование IP-адреса не тем устройством, для которого был указан этот IP-адрес. В заголовке и в описании типа события используются следующие переменные: • $owner_ip – IP-адрес; • $challenger_asset_name – имя устройства, которое использовало IP-адрес; • $challenger_mac – MAC-адрес устройства, которое использовало IP-адрес; • $asset_name – имя устройства, в параметрах которого был указан IP-адрес; • $owner_mac – MAC-адрес устройства, в параметрах которого был указан IP-адрес; • $challenger_ips_list – список других IP-адресов устройства, которое использовало IP-адрес; • $asset_id – идентификатор устройства, в параметрах которого был указан IP-адрес; • $challenger_id – идентификатор устройства, которое использовало IP-адрес.
4000005006	Обнаружен трафик с адреса $owner_ip_or_mac, который закреплен за устройством со статусом Неиспользуемое	В режиме наблюдения контроля активов или по полученным данным от EPP-приложения обнаружена активность устройства, которому был присвоен статус *Неиспользуемое*. Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Неразрешенное устройство**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $last_seen_timestamp – дата и время последнего появления устройства в сети; • $asset_id – идентификатор устройства.

Код	Заголовок типа события	Условия для регистрации
4000005007	Обнаружен новый IP-адрес $new_ip_addr у устройства с MAC-адресом $owner_mac	В режиме наблюдения контроля активов обнаружен новый IP-адрес, использованный устройством. В заголовке и в описании типа события используются следующие переменные: • $new_ip_addr – обнаруженный IP-адрес; • $owner_mac – MAC-адрес устройства; • $asset_name – имя устройства; • $owner_ips_list – список других IP-адресов устройства; • $asset_id – идентификатор устройства.
4000005008	Добавлен MAC-адрес $owner_mac устройству с IP-адресом $owner_ip	В режиме наблюдения контроля активов автоматически добавлен MAC-адрес для сетевого интерфейса, у которого был указан только IP-адрес (при этом устройство было со статусом *Неразрешенное* или *Неиспользуемое*). В заголовке и в описании типа события используются следующие переменные: • $owner_mac – обнаруженный MAC-адрес устройства; • $owner_ip – IP-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства.
4000005009	Добавлен IP-адрес $owner_ip устройству с MAC-адресом $owner_mac	В режиме наблюдения контроля активов автоматически добавлен IP-адрес для сетевого интерфейса, у которого был указан только MAC-адрес (при этом устройство было со статусом *Неразрешенное* или *Неиспользуемое*). В заголовке и в описании типа события используются следующие переменные: • $owner_ip – обнаруженный IP-адрес устройства; • $owner_mac – MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства.
4000005010	Обнаружен новый MAC-адрес $new_mac_addr у устройства с IP-адресом $owner_ip	В режиме наблюдения контроля активов обнаружен новый MAC-адрес, использованный устройством (при этом для устройства выключено автоматическое обновление адресной информации). В заголовке и в описании типа события используются следующие переменные: • $new_mac_addr – обнаруженный MAC-адрес; • $owner_ip – IP-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства.
4000005011	Обнаружено изменение MAC-адреса $owner_mac на адрес $challenger_mac в полученных данных об устройстве от EPP-приложения	По полученным данным от EPP-приложения обновлен MAC-адрес устройства. В заголовке и в описании типа события используются следующие переменные: • $owner_mac – старый MAC-адрес устройства; • $challenger_mac – новый MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства.
4000005012	Обнаружена новая адресная информация устройства $asset_name в полученных данных от EPP-приложения	В полученных данных от EPP-приложения обнаружена новая адресная информация устройства. Событие этого типа регистрируется, если изменение адресной информации устройства не было обработано программой как событие с кодом 4000005009 или 4000005010. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $detected_epp_addresses – адресная информация; • $asset_id – идентификатор устройства.

Код	Заголовок типа события	Условия для регистрации
4000005013	Обнаружен конфликт в адресах устройств $conflicted_epp_assets после получения данных от EPP-приложения	По полученным данным от EPP-приложения обнаружен конфликт с адресами нескольких устройств в Kaspersky Industrial CyberSecurity for Networks. По данным от EPP-приложения, адреса принадлежат одному устройству. В заголовке и в описании типа события используются следующие переменные: • $conflicted_epp_assets – устройства, у которых обнаружен конфликт адресов; • $unaccepted_epp_addresses – адреса, для которых установлена принадлежность одному устройству.
4000005014	Добавлена подсеть $subnet_mask по данным от EPP-приложения	После получения данных от EPP-приложения в список известных подсетей автоматически добавлена новая подсеть. Подсеть добавляется в то адресное пространство, в котором источником данных может являться сервер интеграции, получающий данные от EPP-приложения. При наличии нескольких таких адресных пространств выбирается то АП, которое содержит наиболее подходящую подсеть для автоматического добавления новой вложенной подсети. В заголовке и в описании типа события используются следующие переменные: • $subnet_mask – адрес подсети; • $subnet_type – тип подсети.
4000005015	Обнаружено изменение оборудования устройства с адресом $owner_ip_or_mac	По полученным данным от EPP-приложения обновлены сведения об оборудовании устройства с помощью функциональности контроля оборудования. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства; • $added_asset_hardware – список добавленного оборудования; • $modified_asset_hardware – список измененного оборудования; • $removed_asset_hardware – список удаленного оборудования.
4000005200	Контроль проектов ПЛК: обнаружено чтение неизвестного блока из ПЛК $asset_name	При контроле чтения и записи проектов ПЛК обнаружена операция чтения неизвестного блока проекта из ПЛК (если отсутствует сохраненная информация об этом блоке). Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Чтение неизвестного блока проекта из ПЛК**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $block_name – имя блока; • $saved_date_time – дата и время обнаружения операции.
4000005201	Контроль проектов ПЛК: обнаружено чтение известного блока из ПЛК $asset_name	При контроле чтения и записи проектов ПЛК обнаружена операция чтения известного блока проекта из ПЛК (если есть сохраненная информация об этом блоке, но полученная информация не совпадает с последней сохраненной информацией об этом блоке). Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Чтение известного блока проекта из ПЛК**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $block_name – имя блока; • $saved_date_time – дата и время сохранения блока в программе.

Код	Заголовок типа события	Условия для регистрации
4000005202	Контроль проектов ПЛК: обнаружена запись нового блока в ПЛК $asset_name	При контроле чтения и записи проектов ПЛК обнаружена операция записи неизвестного блока проекта из ПЛК (если отсутствует сохраненная информация об этом блоке). Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Запись нового блока проекта в ПЛК**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $block_name – имя блока; • $saved_date_time – дата и время обнаружения операции.
4000005203	Контроль проектов ПЛК: обнаружена запись известного блока в ПЛК $asset_name	При контроле чтения и записи проектов ПЛК обнаружена операция записи известного блока проекта из ПЛК (если есть сохраненная информация об этом блоке, но полученная информация не совпадает с последней сохраненной информацией об этом блоке). Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Запись известного блока проекта в ПЛК**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $block_name – имя блока; • $saved_date_time – дата и время сохранения блока в программе.
4000005204	Контроль проектов ПЛК: обнаружено чтение неизвестного проекта из ПЛК $asset_name	При контроле чтения и записи проектов ПЛК обнаружена операция чтения неизвестного проекта из ПЛК (если отсутствует сохраненная информация об этом проекте). Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Чтение неизвестного проекта из ПЛК**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $saved_date_time – дата и время обнаружения операции.
4000005205	Контроль проектов ПЛК: обнаружено чтение известного проекта из ПЛК $asset_name	При контроле чтения и записи проектов ПЛК обнаружена операция чтения известного проекта из ПЛК (если есть сохраненная информация об этом проекте, но полученная информация не совпадает с последней сохраненной информацией об этом проекте). Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Чтение известного проекта из ПЛК**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $saved_date_time – дата и время сохранения проекта в программе.
4000005206	Контроль проектов ПЛК: обнаружена запись нового проекта в ПЛК $asset_name	При контроле чтения и записи проектов ПЛК обнаружена операция записи нового проекта в ПЛК (если отсутствует сохраненная информация об этом проекте). Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Запись нового проекта в ПЛК**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $saved_date_time – дата и время обнаружения операции.
4000005207	Контроль проектов ПЛК: обнаружена запись известного проекта в ПЛК $asset_name	При контроле чтения и записи проектов ПЛК обнаружена операция записи известного проекта в ПЛК (если есть сохраненная информация об этом проекте, но полученная информация не совпадает с последней сохраненной информацией об этом проекте). Одновременно с регистрацией события программа может зарегистрировать для этого устройства и риск **Запись известного проекта в ПЛК**. В этом случае устанавливается связь риска и события. В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $saved_date_time – дата и время сохранения проекта в программе.

Код	Заголовок типа события	Условия для регистрации
4000005600	Обнаружены изменения в списке пользователей устройства с адресом $owner_ip_or_mac	При контроле пользователей на устройствах обнаружены изменения сведений о пользователях. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства; • $added_asset_users – список добавленных пользователей; • $modified_asset_users – список измененных пользователей; • $removed_asset_users – список удаленных пользователей.
4000005601	Обнаружены изменения в списке приложений устройства с адресом $owner_ip_or_mac	При контроле приложений и патчей на устройствах обнаружены изменения сведений о приложениях устройства. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства; • $added_asset_apps – список добавленных приложений; • $removed_asset_apps – список удаленных приложений.
4000005602	Обнаружены изменения в списке патчей устройства с адресом $owner_ip_or_mac	При контроле приложений и патчей на устройствах обнаружены изменения сведений о патчей устройства. В заголовке и в описании типа события используются следующие переменные: • $owner_ip_or_mac – IP- или MAC-адрес устройства; • $asset_name – имя устройства; • $asset_id – идентификатор устройства; • $added_asset_patches – список добавленных патчей; • $removed_asset_patches – список удаленных патчей.
4000005603	Обнаружены изменения в компоненте конфигурации $inventory_loc_key на устройстве	При контроле конфигураций устройств обнаружены изменения в компоненте конфигурации при сравнении с предыдущей конфигурацией по результатам сканирования устройства (для заданий в режимах обработки конфигураций **Только обновление** и/или **Архивирование версий**). В заголовке и в описании типа события используются следующие переменные: • $inventory_loc_key – название компонента конфигурации; • $device_config_inventory_changed_format – обнаруженные изменения в компоненте конфигурации.
4000005604	Обнаружены отличия от эталонного компонента конфигурации $inventory_loc_key на устройстве	При контроле конфигураций устройств обнаружены отличия от эталонного компонента конфигурации по результатам сканирования устройства (для заданий в режиме обработки конфигураций **Сравнение с эталоном**). В заголовке и в описании типа события используются следующие переменные: • $inventory_loc_key – название компонента конфигурации; • $device_config_diverged_format – обнаруженные отличия от эталонного компонента конфигурации.
4000005700	Обнаружено несовпадение открытого ключа при удаленном подключении к устройству	При удаленном подключении к устройству обнаружено несовпадение полученного открытого ключа устройства со значением, сохраненным в программе. Сканирование устройства отменено. В описании типа события используются следующие переменные: • $asset_name – имя устройства; • $new_asset_sshpublickey – полученный открытый ключ; • $old_asset_sshpublickey – сохраненный открытый ключ.

Код	Заголовок типа события	Условия для регистрации
4000005701	Обнаружено несовпадение открытого ключа при активном опросе устройства	При активном опросе устройства обнаружено несовпадение полученного открытого ключа устройства со значением, сохраненным в программе. Активный опрос устройства отменен. В описании типа события используются следующие переменные: • $asset_name – имя устройства; • $new_asset_sshpublickey – полученный открытый ключ; • $old_asset_sshpublickey – сохраненный открытый ключ. Этот тип события используется в версии Kaspersky Industrial CyberSecurity for Networks 4.2. В версии Kaspersky Industrial CyberSecurity for Networks 4.2.1 вместо этого типа события используется тип события с кодом 4000005700.
4000000004	Тестовое событие (AM)	Обнаружен тестовый сетевой пакет (при включенном методе обнаружения активности устройств).

Системные типы событий по технологии Внешние системы

В этой статье приведено описание системных типов событий, относящихся к технологии Внешние системы (см. таблицу ниже).

Системные типы событий по технологии Внешние системы (EXT)

Код	Заголовок типа события	Условия для регистрации
8000000001	Инцидент	Обнаружена последовательность событий, удовлетворяющих условиям правила корреляции. При регистрации события в качестве заголовка и описания инцидента указываются заголовок и описание из правила корреляции.
4000005400	Событие от внешней системы	Поступило событие от внешней системы с использованием Kaspersky Industrial CyberSecurity for Networks API. При регистрации события содержимое заголовка и описания определяются внешней системой.

Системные типы событий по технологии Защита конечных устройств

В этой статье приведено описание системных типов событий, относящихся к технологии Защита конечных устройств (см. таблицу ниже).

Системный тип события по технологии Защита конечных устройств (EPP)

Код	Заголовок типа события	Условия для регистрации
4000005500	Активность, характерная для сетевых атак	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Защита от сетевых угроз. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005501	Подключение недоверенного внешнего устройства	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Контроль устройств. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005502	Попытка запуска неразрешенной или недоверенной программы	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Контроль запуска программ. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.

Код	Заголовок типа события	Условия для регистрации
4000005503	Неразрешенная файловая операция в заданной области мониторинга	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Мониторинг файловых операций. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005504	Изменены файлы в заданной области мониторинга	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Мониторинг целостности файлов на основе эталона. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005505	Сетевое подключение, не разрешенное правилами сетевого экрана	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Управление сетевым экраном. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005506	Изменения системного реестра в заданной области мониторинга	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Мониторинг реестра. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005507	Сработало правило анализа журналов	На сервер интеграции поступили данные о срабатывании правила компонента EPP-приложения Анализ журналов. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005508	Попытка эксплуатации уязвимости в защищаемом процессе	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Защита от эксплойтов. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005509	Попытка вредоносного шифрования сетевых файловых ресурсов	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Защита от шифрования. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005510	Попытка подключения к сети Wi-Fi	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Контроль Wi-Fi. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005511	Изменение проекта ПЛК в сравнении с эталонным проектом	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Контроль проектов ПЛК. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005512	Обнаружен зараженный или возможно зараженный объект	На сервер интеграции поступили данные о срабатывании компонента EPP-приложения Постоянная защита файлов. В описании типа события используется переменная $epp_event_description для данных от EPP-приложения.
4000005513	Сработало Sigma-правило $sigmaAlertTitle	На сервер интеграции поступили данные о срабатывании Sigma-правила компонента Endpoint Agent. В заголовке и в описании типа события используются следующие переменные: • $sigmaAlertTitle – название Sigma-правила; • $sigma_detection_type – технология обнаружения; • $sigma_object_type – тип объекта, вызвавшего срабатывание Sigma-правила; • $sigma_object_name – имя объекта, для которого сработало Sigma-правило, или название первого сработавшего Sigma-правила; • $sigma_status – статус обнаружения.

Категории системных команд в Kaspersky Industrial CyberSecurity for Networks

В этой статье перечислены категории системных команд, поддерживаемых в Kaspersky Industrial CyberSecurity for Networks при анализе трафика промышленной сети (см. таблицу ниже).

Категории системных команд

Категория системных команд	Описание
Подключение	Команды управления соединением.
Аутентификация	Команды аутентификации.
Изменения режима работы	Команды изменения режима работы устройств.
Загрузка программы	Команды загрузки программы устройств.
Выгрузка программы	Команды выгрузки программы устройств.
Команды управления	Стандартизированные команды протоколов для интеллектуальных электронных устройств (IED).
Изменение программы	Команды изменения управляющей программы устройства.
Управление сигналами тревоги	Команды управления сигналами тревоги.
Онлайн-режим	Команды работы с программой устройств в онлайн-режиме или режиме отладки.
Изменение значений тегов	Команды принудительного изменения значений тегов.
Чтение тегов и данных	Команды получения значений тегов, подписки на теги, запросы данных о программах устройств.
Обновление прошивки	Команды изменения прошивки устройств.
Чтение конфигурации устройства	Команды чтения или запроса информации об устройствах.
Изменение конфигурации устройства	Команды изменения параметров устройств.
Файловая операция	Команды управления файлами и директориями устройств.
Сервисная команда	Команды по обслуживанию устройств.
Управление датой и временем	Команды управления датой и временем на устройствах.
Диагностическое сообщение	Диагностические сообщения об ошибках или о несоответствии данных в трафике.
Взаимодействие по DCOM	Команды протоколов, использующих технологию DCOM (например, OPC DA).
Ошибка разбора сообщений	Ошибки разбора сообщений.
Другое	Команды, не относящиеся к остальным категориям.

Примеры использования адресных пространств в Kaspersky Industrial CyberSecurity for Networks

Адресные пространства позволяют обеспечить работу Kaspersky Industrial CyberSecurity for Networks в тех случаях, когда используются устройства с одинаковыми адресами в разных сегментах сети. В этой статье приведены примеры использования адресных пространств для следующих вариантов дублирования адресов устройств в разных сегментах сети:

- дублирование IP-адресов;
- дублирование MAC-адресов;
- дублирование MAC-адресов и использование одинаковых диапазонов IP-адресов.

Адресные пространства для варианта дублирования IP-адресов устройств

В этом примере рассматривается предприятие, в состав которого входят 16 технологических площадок с группами ПЛК на этих площадках. На каждой технологической площадке используются одинаковые диапазоны IP-адресов: 10.4.0.0/16, 10.5.0.0/16, 10.8.0.0/16, 10.9.0.0/16. Как следствие, устройства на разных площадках могут иметь одинаковые IP-адреса.

Сегменты технологических площадок полностью изолированы от общей сети предприятия. В каждом сегменте функционируют ПЛК, инженерные и рабочие станции, а также компьютеры, выполняющие функции станций приложений (далее "компьютер Application Station"). Интеграция сегмента с общей сетью предприятия обеспечивается через компьютер Application Station. Этот компьютер имеет выделенный сетевой интерфейс с уникальным IP-адресом общей сети предприятия.

Для работы в такой конфигурации в Kaspersky Industrial CyberSecurity for Networks требуется добавить следующие объекты для каждого сегмента технологической площадки:

- точка мониторинга для получения трафика внутри сегмента;
- точка мониторинга для получения трафика с компьютера Application Station;
- адресное пространство, содержащее одно правило.

Например, для первого сегмента вы можете добавить объекты со следующими именами:

- **MPoint_1-1**
- **MPoint_1-2**
- **Site_1**

Параметры адресных пространств для каждого сегмента описаны в таблице ниже.

АП для сегментов с одинаковой IP-адресацией

Имя АП	Источник данных	Уровни модели OSI	VLAN ID	IP-адреса
Site_1	**Точки мониторинга**: MPoint_1-1 MPoint_1-2	**Сетевой (L3)**	**Любые или не используются**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
Site_2	**Точки мониторинга**: MPoint_2-1 MPoint_2-2	**Сетевой (L3)**	**Любые или не используются**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
Site_3	**Точки мониторинга**: MPoint_3-1 MPoint_3-2	**Сетевой (L3)**	**Любые или не используются**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
…				
Site_16	**Точки мониторинга**: MPoint_16-1 MPoint_16-2	**Сетевой (L3)**	**Любые или не используются**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16

Адресные пространства для варианта дублирования MAC-адресов устройств

В этом примере рассматривается промышленная сеть, в которой используется технология VLAN. В сети выделены два сегмента технологических площадок, отличающиеся идентификаторами VLAN 3910 и 3915. В сегментах сети есть устройства с принудительно назначенными MAC-адресами (устройства и программное обеспечение для них поддерживают такую возможность). Как следствие, устройства в разных сегментах могут иметь одинаковые MAC-адреса.

Для работы в такой конфигурации в Kaspersky Industrial CyberSecurity for Networks требуется добавить по одному адресному пространству для каждого сегмента. Например, для адресных пространств можно задать имена **Site_1** и **Site_2**. Адресные пространства могут содержать по одному правилу.

Параметры адресных пространств для каждого сегмента описаны в таблице ниже.

АП для сегментов с одинаковой MAC-адресацией

Имя АП	Источник данных	Уровни модели OSI	VLAN ID	IP-адреса
Site_1	**Точки мониторинга**: **любые**	**Канальный (L2)**	3910	**Любые**
Site_2	**Точки мониторинга**: **любые**	**Канальный (L2)**	3915	**Любые**

Адресные пространства для варианта дублирования MAC-адресов устройств и с одинаковым диапазоном IP-адресов

В этом примере рассматривается промышленная сеть, в которой используется технология VLAN. В сети выделены два сегмента технологических площадок, отличающиеся идентификаторами VLAN 3910 и 3915. В сегментах сети есть устройства с принудительно назначенными MAC-адресами (устройства и программное обеспечение для них поддерживают такую возможность). При этом для IP-адресов в каждом сегменте используется одинаковый диапазон адресов: 140.80.0.0/16. Как следствие, устройства в разных сегментах могут иметь как одинаковые MAC-адреса, так и одинаковые IP-адреса.

Для работы в такой конфигурации в Kaspersky Industrial CyberSecurity for Networks требуется добавить по одному адресному пространству для каждого сегмента. Например, для адресных пространств можно задать имена **Site_1** и **Site_2**. Адресные пространства могут содержать по одному правилу.

Параметры адресных пространств для каждого сегмента описаны в таблице ниже.

АП для сегментов с одинаковой MAC-адресацией и одинаковым диапазоном IP-адресов

Имя АП	Источник данных	Уровни модели OSI	VLAN ID	IP-адреса
Site_1	**Точки мониторинга**: **любые**	**Канальный и сетевой (L2 и L3)**	3910	140.80.0.0/16
Site_2	**Точки мониторинга**: **любые**	**Канальный и сетевой (L2 и L3)**	3915	140.80.0.0/16

Поддерживаемые протоколы общего применения

Kaspersky Industrial CyberSecurity for Networks поддерживает отслеживание следующих протоколов общего применения в трафике:

- Bitcoin.
- Bittorrent.
- BOOTP / DHCP.
- DNS.
- FTP.
- GLBP.
- HTTP.
- HTTPS.
- ICMP.
- IMAP.
- IRC.
- Jabber®.
- Litecoin.
- MQTT.
- NBNS.
- NetBIOS.
- NTP.
- POP3.
- Radius.

- Radmin.
- RDP.
- RLOGIN.
- SIP.
- SMB.
- SMTP.
- SNMP.
- SSDP.
- SSH.
- SSL / TLS.
- Syslog.
- Telegram.
- Telnet.
- TFTP.
- TNS.
- Tor®.
- VNC.
- VRRP.

Особенности получения типов конфигураций устройств с помощью заданий контроля конфигураций

При добавлении заданий контроля конфигураций вы можете выбирать типы конфигураций, в соответствии с которыми программа будет получать данные при сканированиях устройств.

Этот раздел содержит информацию об особенностях получения конфигураций устройств для разных типов конфигураций.

Конфигурации устройств под управлением операционных систем семейства Windows

Программа текущей версии поддерживает получение типа конфигурации **Операционная система Windows** для устройств под управлением операционных систем, поддерживаемых программой Kaspersky Endpoint Agent для сценариев интеграции с Kaspersky Industrial CyberSecurity for Networks.

Для типа конфигурации **Операционная система Windows** вы можете указывать следующие компоненты конфигураций для получения данных:

- **Пользователи**.
- **Группы**.
- **Приложения**.
- **Патчи**.
- **Службы**.
- **Драйверы**.
- **Задачи по расписанию**.
- **Общие сетевые ресурсы**.
- **Соответствие IP - сетевое имя**.
- **Соответствие IP - NetBIOS-имя**.
- **Элементы автозапуска**.

Получаемые данные о пользователях

Если для задания контроля конфигураций указан компонент конфигурации **Пользователи**, при сканировании устройства выполняется чтение данных об учетных записях пользователей на устройстве. Программа позволяет получать следующие данные о каждой учетной записи пользователя:

- Имя пользователя в формате `домен\имя пользователя`.
- Уникальный идентификатор пользователя.
- Полное имя пользователя (например, `Иванов Иван`).
- Является ли учетная запись активной.
- Является ли учетная запись заблокированной.
- Может ли истечь пароль учетной записи.

- Истек ли пароль.
- Может ли пользователь изменить свой пароль.
- Список групп, в которые входит пользователь.

Получаемые данные о группах

Если для задания контроля конфигураций указан компонент конфигурации **Группы**, при сканировании устройства выполняется чтение данных об учетных записях групп на устройстве. Программа позволяет получать следующие данные о каждой учетной записи группы:

- Имя группы в формате `домен\имя группы`.
- Уникальный идентификатор группы.
- Список пользователей, входящих в группу. В каждом элементе списка представлены следующие данные:
  - Уникальный идентификатор члена группы.
  - Имя члена группы.

Получаемые данные о приложениях

Если для задания контроля конфигураций указан компонент конфигурации **Приложения**, при сканировании устройства выполняется чтение данных об установленных приложениях на устройстве. Программа позволяет получать следующие данные о каждом приложении:

- Название приложения.
- Производитель приложения.
- Размер приложения в байтах.
- Версия приложения.
- Дата и время установки приложения.

Получаемые данные о патчах

Если для задания контроля конфигураций указан компонент конфигурации **Патчи**, при сканировании устройства выполняется чтение данных об установленных патчах для приложений на устройстве. Программа позволяет получать следующие данные о каждом патче:

- Название патча.
- Производитель приложения.
- Приложение, для которого установлен патч.
- Версия патча.

Получаемые данные о службах

Если для задания контроля конфигураций указан компонент конфигурации **Службы**, при сканировании устройства выполняется чтение данных о зарегистрированных службах на устройстве. Программа позволяет получать следующие данные о каждой службе:

- Имя службы.
- Полное имя службы.
- Тип запуска.
- Команда запуска.
- Имена зависимых служб.

Получаемые данные о драйверах

Если для задания контроля конфигураций указан компонент конфигурации **Драйверы**, при сканировании устройства выполняется чтение данных об установленных драйверах на устройстве. Программа позволяет получать следующие данные о каждом драйвере:

- Имя драйвера.
- Полное имя драйвера.
- Тип запуска.
- Путь к файлу драйвера.
- Имена зависимых драйверов.

Получаемые данные о задачах по расписанию

Если для задания контроля конфигураций указан компонент конфигурации **Задачи по расписанию**, при сканировании устройства выполняется чтение данных о зарегистрированных задачах в Планировщике заданий на устройстве. Программа позволяет получать следующие данные о каждой задаче:

- Название задачи.
- Статус задачи.
- Описание.
- Автор.
- Команды выполняемые при запуске задачи (действия, связанные с запуском исполняемого кода).

Получаемые данные об общих сетевых ресурсах

Если для задания контроля конфигураций указан компонент конфигурации **Общие сетевые ресурсы**, при сканировании устройства выполняется чтение данных о созданных общих сетевых ресурсах на устройстве. Программа позволяет получать следующие данные о каждом общем сетевом ресурсе:

- Сетевое имя общего ресурса.
- Локальный путь к сетевому ресурсу.
- Описание.
- Тип сетевого ресурса.
- Максимальное количество подключений.

Получаемые данные из таблицы соответствий IP – сетевое имя

Если для задания контроля конфигураций указан компонент конфигурации **Соответствие IP - сетевое имя**, при сканировании устройства выполняется чтение данных об элементах таблицы соответствия IP - сетевое имя (\etc\hosts) на устройстве. Программа позволяет получать следующие данные о каждом элементе таблицы:

- IP-адрес.
- Сетевое имя.

Получаемые данные из таблицы соответствий IP – NetBIOS-имя

Если для задания контроля конфигураций указан компонент конфигурации **Соответствие IP - NetBIOS-имя**, при сканировании устройства выполняется чтение данных об элементах таблицы соответствия IP – NetBIOS-имя (\etc\lmhosts) на устройстве. Программа позволяет получать следующие данные о каждом элементе таблицы:

- IP-адрес.
- Сетевое имя.
- Загружается ли запись в кеш имен.
- Какому домену соответствует запись.
- Подключаемые файлы lmhosts.

Получаемые данные об элементах автозапуска

Если для задания контроля конфигураций указан компонент конфигурации **Элементы автозапуска**, при сканировании устройства выполняется чтение данных об элементах автозапуска при старте операционной системы на устройстве. Программа позволяет получать следующие данные о каждом элементе автозапуска:

- Информация о точке автозапуска (например, путь в системном реестре).
- Исполняемая команда или файл (COM-объект).

Конфигурации устройств под управлением операционных систем семейства Linux

Получение типа конфигурации **Операционная система Linux** выполняется на устройствах с использованием команд для запуска стандартных утилит диагностики Linux-устройств.

Для типа конфигурации **Операционная система Linux** вы можете указывать следующие компоненты конфигураций для получения данных:

- **Пользователи**.
- **Приложения**.

Получаемые данные о пользователях

Если для задания контроля конфигураций указан компонент конфигурации **Пользователи**, при сканировании устройства выполняется чтение данных об учетных записях пользователей на устройстве. Программа позволяет получать следующие данные о каждой учетной записи пользователя:

- Имя пользователя в формате `домен\имя пользователя`.
- Уникальный идентификатор пользователя.
- Полное имя пользователя (например, `Иванов Иван`).
- Является ли учетная запись активной.
- Является ли учетная запись заблокированной.
- Может ли истечь пароль учетной записи.
- Истек ли пароль.
- Может ли пользователь изменить свой пароль.
- Список групп, в которые входит пользователь.

Получаемые данные о приложениях

Если для задания контроля конфигураций указан компонент конфигурации **Приложения**, при сканировании устройства выполняется чтение данных об установленных приложениях на устройстве. Программа позволяет получать следующие данные о каждом приложении:

- Название приложения.
- Размер приложения в байтах.
- Версия приложения.
- Дата и время установки приложения.

Конфигурации устройств, относящихся к сетевому оборудованию

Программа текущей версии поддерживает получение типа конфигурации **Сетевые устройства** для следующих устройств:

- Cisco IOS™-устройства.
- Siemens серии SCALANCE с поддержкой протокола SSH.
- Moxa серии PT.

  > Возможности получения конфигураций для устройств Moxa серии PT не поддерживаются, если устройство находится в режиме настройки по умолчанию (режим MENU).

- Eltex серии MES.

Для типа конфигурации **Сетевые устройства** вы можете указывать следующие компоненты конфигураций для получения данных:

- **Пользователи**.
- **Элементы ARP-таблицы**.
- **Версия платформы**.
- **Выполняемые процессы**.
- **Начальная конфигурация**.
- **Текущая конфигурация**.
- **Таблица маршрутизации**.
- **Таблица MAC-адресов**.
- **Сетевые интерфейсы**.

Получаемые данные о пользователях

Если для задания контроля конфигураций указан компонент конфигурации **Пользователи**, при сканировании устройства выполняется чтение данных об учетных записях пользователей на устройстве (для тех сетевых устройств, на которых поддерживается получение данных о пользователях). Программа позволяет получать следующие данные о каждой учетной записи пользователя:

- Для Cisco IOS™-устройств:
  - Имя пользователя в формате `домен\имя пользователя`.
  - Уникальный идентификатор пользователя.
  - Настроен ли ключ для SSH.
  - Настроен ли пароль.
  - Настроен ли секрет для пользователя.
  - Уровень привилегий пользователя.
- Для устройств Siemens серии SCALANCE не поддерживается получение данных о пользователях.
- Для устройств Moxa серии PT не поддерживается получение данных о пользователях.
- Для устройств Eltex серии MES не поддерживается получение данных о пользователях.

Получаемые данные об элементах ARP-таблицы

Если для задания контроля конфигураций указан компонент конфигурации **Элементы ARP-таблицы**, при сканировании устройства выполняется чтение данных об элементах ARP-таблицы на устройстве (для тех сетевых устройств, на которых поддерживается получение данных об элементах ARP-таблицы). Программа позволяет получать следующие данные о каждом элементе таблицы:

- Для Cisco IOS™-устройств:
  - IP-адрес.
  - Физический адрес.
  - Имя сетевого интерфейса или адаптера.
  - Тип физического адреса.
  - Тип записи.
- Для устройств Siemens серии SCALANCE:
  - IP-адрес.
  - Физический адрес.
  - Имя сетевого интерфейса или адаптера.

    - Тип физического адреса.
    - Тип записи.
- Для устройств Moxa серии PT не поддерживается получение данных об элементах ARP-таблицы.
- Для устройств Eltex серии MES:
    - IP-адрес.
    - Физический адрес.
    - Имя сетевого интерфейса или адаптера.
    - Тип физического адреса.
    - Тип записи.

Получаемые данные о версии платформы

Если для задания контроля конфигураций указан компонент конфигурации **Версия платформы**, при сканировании устройства выполняется чтение данных о версии аппаратной платформы устройства. Программа позволяет получать версию операционной системы в составе данных о версии аппаратной платформы устройства.

Получаемые данные о выполняемых процессах

Если для задания контроля конфигураций указан компонент конфигурации **Выполняемые процессы**, при сканировании устройства выполняется чтение данных о текущих выполняемых процессах на устройстве (для тех сетевых устройств, на которых поддерживается получение данных о выполняемых процессах). Программа позволяет получать следующие данные о каждом процессе:

- Для Cisco IOS™-устройств:
    - Уникальный идентификатор процесса.
    - Имя процесса.
- Для устройств Siemens серии SCALANCE не поддерживается получение данных о текущих выполняемых процессах.
- Для устройств Moxa серии PT не поддерживается получение данных о текущих выполняемых процессах.
- Для устройств Eltex серии MES не поддерживается получение данных о текущих выполняемых процессах.

Получаемые данные о начальной конфигурации

Если для задания контроля конфигураций указан компонент конфигурации **Начальная конфигурация**, при сканировании устройства выполняется чтение данных о секциях параметров начальной конфигурации устройства. Программа позволяет получать следующие данные о каждой секции параметров:

- Для Cisco IOS™-устройств:
  - Название секции параметров.
  - Текстовое представление параметров секции.
- Для устройств Siemens серии SCALANCE:
  - Название секции параметров.
  - Текстовое представление параметров секции (вывод команды `info` на разных уровнях вложенности).
- Для устройств Moxa серии PT:
  - Название секции параметров.
  - Текстовое представление параметров секции (вывод команды `show startup-config`).
- Для устройств Eltex серии MES:
  - Название секции параметров.
  - Текстовое представление параметров секции (вывод команды `show startup-config`).

Получаемые данные о текущей конфигурации

Если для задания контроля конфигураций указан компонент конфигурации **Текущая конфигурация**, при сканировании устройства выполняется чтение данных о секциях параметров текущей конфигурации устройства (для тех сетевых устройств, на которых поддерживается получение данных о текущей конфигурации). Программа позволяет получать следующие данные о каждой секции параметров:

- Для Cisco IOS™-устройств:
  - Название секции параметров.
  - Текстовое представление параметров секции.
- Для устройств Siemens серии SCALANCE не поддерживается получение данных о секциях параметров текущей конфигурации.

- Для устройств Moxa серии PT:
  - Название секции параметров.
  - Текстовое представление параметров секции.
- Для устройств Eltex серии MES:
  - Название секции параметров.
  - Текстовое представление параметров секции.

Получаемые данные о таблице маршрутизации

Если для задания контроля конфигураций указан компонент конфигурации **Таблица маршрутизации**, при сканировании устройства выполняется чтение данных об элементах таблицы маршрутизациии на устройстве (для тех сетевых устройств, на которых поддерживается получение данных об элементах таблицы маршрутизации). Программа позволяет получать следующие данные о каждом элементе таблицы:

- Для Cisco IOS™-устройств:
  - Имя или IP-адрес интерфейса.
  - Подсеть назначения.
  - Маска подсети назначения.
  - Шлюз (адрес следующего маршрутизатора в удаленной сети).
  - Протокол.
- Для устройств Siemens серии SCALANCE не поддерживается получение данных об элементах таблицы маршрутизации.
- Для устройств Moxa серии PT не поддерживается получение данных об элементах таблицы маршрутизации.
- Для устройств Eltex серии MES:
  - Имя или IP-адрес интерфейса.
  - Подсеть назначения.
  - Маска подсети назначения.

Получаемые данные о таблице MAC-адресов

Если для задания контроля конфигураций указан компонент конфигурации **Таблица MAC-адресов**, при сканировании устройства выполняется чтение данных об элементах таблицы MAC-адресов на устройстве (для тех сетевых устройств, на которых поддерживается получение данных об элементах таблицы MAC-адресов). Программа позволяет получать следующие данные о каждом элементе таблицы:

- Для Cisco IOS™-устройств:

    - Номер VLAN.
    - MAC-адрес.
    - Тип MAC-адреса.
    - Порт, которому назначен MAC-адрес.
- Для устройств Siemens серии SCALANCE не поддерживается получение данных об элементах таблицы MAC-адресов.
- Для устройств Moxa серии PT не поддерживается получение данных об элементах таблицы MAC-адресов.
- Для устройств Eltex серии MES:
    - Номер VLAN.
    - MAC-адрес.
    - Тип MAC-адреса.
    - Порт MAC-адреса.

Получаемые данные о сетевых интерфейсах

Если для задания контроля конфигураций указан компонент конфигурации **Сетевые интерфейсы**, при сканировании устройства выполняется чтение данных о сетевых интерфейсах на устройстве (для тех сетевых устройств, на которых поддерживается получение данных о сетевых интерфейсах). Программа позволяет получать следующие данные о каждом сетевом интерфейсе:

- Для Cisco IOS™-устройств:
    - Описание.
    - Включен ли сетевой интерфейс.
    - MAC-адрес.
    - Имя.
    - Является ли сетевой интерфейс физическим.
    - Назначенный IP-адрес.
- Для устройств Siemens серии SCALANCE не поддерживается получение данных о сетевых интерфейсах.

- Для устройств Moxa серии PT не поддерживается получение данных о сетевых интерфейсах.
- Для устройств Eltex серии MES:
  - Описание.
  - Включен ли сетевой интерфейс.
  - MAC-адрес.
  - Имя.
  - Является ли сетевой интерфейс физическим.

Конфигурации ПЛК и других устройств, получаемые с использованием коннекторов типа Active poll

Встроенный в программу тип коннектора **Active poll** поддерживает получение типа конфигурации **ПЛК** для следующих устройств:

- Siemens SIMATIC серий S7-300, S7-400.
- Schneider Electric серии Modicon: M580, M340.
- Emerson DeltaV (поддерживается только в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1).
- Rockwell Automation Allen-Bradley (поддерживается только в версии Kaspersky Industrial CyberSecurity for Networks 4.2.1).

Получаемые данные об устройствах Siemens SIMATIC серий S7-300, S7-400

При сканировании устройств Siemens SIMATIC с использованием коннекторов типа **Active poll** программа позволяет получать следующие данные:

- Общие параметры:
  - Модель или семейство ПЛК.
  - Программное обеспечение для разработки систем автоматизации, использованное при конфигурировании устройства.
  - Количество шасси в составе установки ПЛК.
  - Состояние памяти.
  - Параметры безопасности.
- Параметры для каждого полученного модуля:
  - Номер шасси, в котором находится модуль.
  - Номер слота в шасси, в котором находится модуль.
  - Производитель CPU-модуля.
  - Тип модуля.
  - Информация о модели модуля.
  - Идентификатор модуля по каталогу Siemens.
  - Уникальный буквенно-цифровой код модуля Siemens (MLFB).
  - Версия аппаратного обеспечения модуля.
  - Версия прошивки модуля.
  - Версия начального загрузчика.
  - Серийный номер CPU-модуля.
  - Запрошенный режим работы CPU-модуля (тот режим, на который должен быть выполнен переход).
  - Текущий режим работы CPU-модуля.

- Хеш-сумма проекта ПЛК.
- Параметры для каждого полученного блока проекта ПЛК:
  - Тип.
  - Идентификатор.
  - Язык мнемосхем, на котором написан блок.
  - Контрольная сумма.
  - Дата компиляции.
  - Сведения об авторе или среде разработки.

Получаемые данные об устройствах Schneider Electric серии Modicon

При сканировании устройств Schneider Electric серии Modicon с использованием коннекторов типа **Active poll** программа позволяет получать следующие данные:

- Общие параметры:
  - Модель или семейство ПЛК.
  - Программное обеспечение для разработки систем автоматизации, использованное при конфигурировании устройства.
  - Количество шасси в составе установки ПЛК.
- Параметры для каждого полученного модуля:
  - Номер шасси, в котором находится модуль.
  - Номер слота в шасси, в котором находится модуль.
  - Производитель CPU-модуля.
  - Тип модуля.
  - Информация о модели модуля.
  - Версия прошивки модуля.
  - Уникальный идентификатор модуля.
  - Режим работы или статус CPU-модуля.

- Общие параметры проекта ПЛК:
  - Имя, заданное пользователем.
  - Хеш-сумма.
  - Название и версия среды разработки (IDE), в которой выполнена последняя полная сборка проекта.
  - Дата и время последней полной сборки проекта.
  - Название и версия среды разработки (IDE), в которой выполнена последняя частичная сборка проекта (для отдельных блоков проекта).
  - Дата и время последней частичной сборки проекта.
  - Версия проекта, заданная пользователем.
- Параметры для каждого полученного блока проекта ПЛК:
  - Тип параметра Task, к которому относится блок.
  - Имя, заданное пользователем.
  - Тип блока и язык мнемосхем, на котором написан блок.
  - Контрольная сумма.

Получаемые данные об устройствах Emerson DeltaV

При сканировании устройств Emerson DeltaV с использованием коннекторов типа **Active poll** программа позволяет получать следующие данные:

- Общие параметры:
  - Модель или семейство устройств.
  - Серия устройств ПЛК.
  - Признак резервированности ПЛК.
- Параметры для CPU-модулей и каждой полученной карты:
  - Номер слота, в котором находится карта (в рамках всех панелей).
  - Производитель CPU-модуля.
  - Тип модуля или карты.
  - Модель модуля (модель CPU-модуля или карты ввода/вывода).
  - Краткое описание карты ввода/вывода.
  - Уникальный буквенно-цифровой код детали, номер по каталогу.
  - Версия аппаратной платформы.
  - Версия IDE-среды и прошивок контроллеров и карт.
  - Уникальное имя контроллера, заданное пользователем в IDE-среде разработки.
  - Уникальный идентификатор контроллера, присвоенный в IDE-среде разработки.
  - Серийный номер CPU-модуля ПЛК.
- Параметры для каждого полученного файла проекта ПЛК:
  - Имя модуля (файла) проекта.
  - Дата загрузки в ПЛК каждого из конфигурационных файлов.
  - Контрольная сумма модуля проекта.

Получаемые данные об устройствах Rockwell Automation Allen-Bradley

При сканировании устройств Rockwell Automation Allen-Bradley с использованием коннекторов типа **Active poll** программа позволяет получать следующие данные:

- Параметры для каждого полученного модуля:
  - Номер слота в шасси, в котором находится модуль.
  - Производитель модуля.
  - Тип модуля.
  - Код продукта (модуля).
  - Информация о модели модуля.
  - Версия прошивки.
  - Уникальное имя контроллера, заданное пользователем в IDE-среде разработки.
  - Серийный номер модуля.
  - Составной статус модуля.
- Общие параметры проекта ПЛК:
  - Номер слота модуля, которому принадлежит проект.
  - Имя, заданное пользователем.
  - Описание, заданное пользователем.
- Параметры для каждой программы и подпрограммы проекта ПЛК:
  - Имя задачи проекта.
  - Тип задачи проекта.
  - Приоритет задачи проекта.
  - Имя программы проекта.
  - Имя подпрограммы (routine) в программе проекта.
  - Контрольная сумма подпрограммы.

Используемые команды для сканирований Linux-устройств в заданиях аудита безопасности

При сканированиях устройств под управлением операционных систем семейства Linux в заданиях аудита настроек и уязвимостей или в заданиях контроля конфигураций получение нужных данных на каждом устройстве происходит с использованием команд запуска следующих утилит:

- blkid;
- cat;
- df;
- dmidecode;
- ethtool;
- free;
- hwinfo;
- ip;
- ls;
- lsblk;
- lshw;
- lsusb.

Все перечисленные утилиты должны быть установлены и доступны в операционной системе устройства. Если какая-либо утилита не установлена, это приводит к невозможности получить данные, которые могут быть предоставлены только этой утилитой.

В большинстве операционных систем, поддерживаемых Kaspersky Industrial CyberSecurity for Linux Nodes, все перечисленные утилиты установлены по умолчанию. Вы можете проверить наличие утилит с помощью соответствующих команд в консоли операционной системы устройства.

Пример:

Чтобы проверить наличие утилит в операционной системе CentOS:

1. В консоли операционной системы компьютера введите команду:

   ```
   which blkid cat df dmidecode ethtool free hwinfo ip ls lsblk lshw lsusb
   ```

   На экране появится список путей к файлам установленных утилит.

2. Убедитесь, что список содержит пути для всех нужных утилит.

Если какая-либо утилита не установлена, вам нужно установить пакет, содержащий эту утилиту.

Пример:

Чтобы установить пакет с утилитой dmidecode в операционной системе CentOS,

в консоли операционной системы компьютера введите команду:

```
sudo dnf install dmidecode
```

Операционные системы устройств, поддерживаемые для проведения активных опросов устройств

В этой статье перечислены операционные системы устройств, которые поддерживаются программой для проведения активных опросов устройств.

Операционные системы Windows

Kaspersky Industrial CyberSecurity for Networks поддерживает проведение активных опросов для устройств под управлением следующих версий операционной системы семейства Windows:

- Операционные системы для настольных компьютеров:
  - Windows XP Professional SP2 x86/x64.
  - Windows XP Professional SP3 x86.
  - Windows Vista® SP2 x86/x64.
  - Windows 7 Enterprise SP1 x86/x64.
  - Windows 7 Professional SP1 x86/x64.
  - Windows 7 Ultimate SP1 x86/x64.
  - Windows 8 Enterprise x86/x64.
  - Windows 8 Pro x86/x64.
  - Windows 8.1 Enterprise x86/x64.
  - Windows 8.1 Pro x86/x64.
  - Windows 10 LTSC 2015 версии 1507 x86/x64.
  - Windows 10 LTSC 2016 версии 1607 x86/x64.
  - Windows 10 Education RS4 версии 1803 x86/x64.
  - Windows 10 Enterprise RS4 версии 1803 x86/x64.
  - Windows 10 Home RS4 версии 1803 x86/x64.
  - Windows 10 Pro RS4 версии 1803 x86/x64.
  - Windows 10 Education RS5 версии 1809 x86/x64.
  - Windows 10 Enterprise RS5 версии 1809 x86/x64.
  - Windows 10 Home RS5 версии 1809 x86/x64.
  - Windows 10 Pro RS5 версии 1809 x86/x64.
  - Windows 10 LTSC 2019 версии 1809 x86/x64.
  - Windows 10 Education 19H1 версии 1903 x86/x64.
  - Windows 10 Enterprise 19H1 версии 1903 x86/x64.
  - Windows 10 Home 19H1 версии 1903 x86/x64.

- Windows 10 Pro 19H1 версии 1903 x86/x64.
- Windows 10 Education 20H1 версии 2004 x86/x64.
- Windows 10 Enterprise 20H1 версии 2004 x86/x64.
- Windows 10 Home 20H1 версии 2004 x86/x64.
- Windows 10 Pro 20H1 версии 2004 x86/x64.
- Windows 10 Education 20H2 версии 2009 x86/x64.
- Windows 10 Enterprise 20H2 версии 2009 x86/x64.
- Windows 10 Home 20H2 версии 2009 x86/x64.
- Windows 10 Pro 20H2 версии 2009 x86/x64.
- Windows 10 Education 21H1 версии 21H1 x86/x64.
- Windows 10 Enterprise 21H1 версии 21H1 x86/x64.
- Windows 10 Home 21H1 версии 21H1 x86/x64.
- Windows 10 Pro 21H1 версии 21H1 x86/x64.
- Windows 10 Education 21H2 версии 21H2 x86/x64.
- Windows 10 Enterprise 21H2 версии 21H2 x86/x64.
- Windows 10 Home 21H2 версии 21H2 x86/x64.
- Windows 10 Pro 21H2 версии 21H2 x86/x64.
- Windows 10 Education 22H2 версии 22H2 x86/x64.
- Windows 10 Enterprise 22H2 версии 22H2 x86/x64.
- Windows 10 Home 22H2 версии 22H2 x86/x64.
- Windows 10 Pro 22H2 версии 22H2 x86/x64.
- Windows 10 LTSC 2021 версии 21H2 x86/x64.
- Windows 11 Education 21H2 версии 21H2 x64.
- Windows 11 Enterprise 21H2 версии 21H2 x64.
- Windows 11 Home 21H2 версии 21H2 x64.
- Windows 11 Pro 21H2 версии 21H2 x64.
- Windows 11 Education 22H2 версии 22H2 x64.
- Windows 11 Enterprise 22H2 версии 22H2 x64.

- Windows 11 Home 22H2 версии 22H2 x64.
- Windows 11 Pro 22H2 версии 22H2 x64.

- Серверные операционные системы:
  - Windows Server® 2003 Enterprise SP1 x86/x64.
  - Windows Server 2003 Standard SP1 x86/x64.
  - Windows Server 2003 Enterprise SP2 x86/x64.
  - Windows Server 2003 Standard SP2 x86/x64.
  - Windows Server 2003 Enterprise R2 x86/x64.
  - Windows Server 2003 Standard R2 x86/x64.
  - Windows Server 2008 Enterprise SP2 x86/x64.
  - Windows Server 2008 Standard SP2 x86/x64.
  - Windows Server 2008 R2 Enterprise SP1 x86/x64.
  - Windows Server 2008 R2 Standard SP1 x86/x64.
  - Windows Server 2012 Datacenter x64.
  - Windows Server 2012 Essentials x64.
  - Windows Server 2012 Foundation x64.
  - Windows Server 2012 Standard x64.
  - Windows Server 2012 R2 Datacenter x64.
  - Windows Server 2012 R2 Essentials x64.
  - Windows Server 2012 R2 Foundation x64.
  - Windows Server 2012 R2 Standard x64.
  - Windows Server 2016 Datacenter версии 1709 x64.
  - Windows Server 2016 Essentials версии 1709 x64.
  - Windows Server 2016 Standard версии 1709 x64.
  - Windows Server 2016 Datacenter версии 1803 x64.
  - Windows Server 2016 Essentials версии 1803 x64.
  - Windows Server 2016 Standard версии 1803 x64.
  - Windows Server 2019 Datacenter версии 1809 x64.

- Windows Server 2019 Essentials версии 1809 x64.
- Windows Server 2019 Standard версии 1809 x64.
- Windows Server 2019 Datacenter версии 1903 x64.
- Windows Server 2019 Essentials версии 1903 x64.
- Windows Server 2019 Standard версии 1903 x64.
- Windows Server 2019 Datacenter версии 1909 x64.
- Windows Server 2019 Essentials версии 1909 x64.
- Windows Server 2019 Standard версии 1909 x64.
- Windows Server 2019 Datacenter Core версии 2004 x64.
- Windows Server 2019 Standard Core версии 2004 x64.
- Windows Server 2019 Datacenter Core версии 20H2 x64.
- Windows Server 2019 Standard Core версии 20H2 x64.
- Windows Server 2022 Datacenter Core версии 21H2 x64.
- Windows Server 2022 Standard Core версии 21H2 x64.

- Встраиваемые операционные системы:
  - Windows XP Embedded SP2 WEPOS x86/x64.
  - Windows XP Embedded SP3 x86 (POS Ready 2009).
  - Windows Embedded 7 SP1 x86/x64 (POS Ready 7).
  - Windows Embedded 8.0 Industry Pro x86/x64.
  - Windows Embedded 8.1 Industry Pro x86/x64.
  - Windows 10 IoT Enterprise 21H1 x86/x64.
  - Windows 10 IoT Enterprise 21H2 x86/x64.
  - Windows 10 IoT Enterprise 22H2 x86/x64.
  - Windows 10 IoT Enterprise версии 1803 x86/x64.
  - Windows 10 IoT Enterprise версии 1809 x86/x64.
  - Windows 10 IoT Enterprise версии 1903 x86/x64.
  - Windows 11 IoT Enterprise версии 21H2 x64.
  - Windows 11 IoT Enterprise версии 22H2 x64.

Операционные системы Linux

Kaspersky Industrial CyberSecurity for Networks поддерживает проведение активных устройств под управлением следующих версий операционной системы семейства Linux:

- 32-битные операционные системы:
  - Debian GNU / Linux 10.1 и выше.
  - Debian GNU / Linux 11.
- 64-битные операционные системы:
  - AlmaLinux OS 8 и выше.
  - AlmaLinux OS 9 и выше.
  - Astra Linux Common Edition (очередное обновление 2.12).
  - Astra Linux 1.4.
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
  - Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
  - Astra Orel 2.12.
  - CentOS 5.2.
  - CentOS 5.4.
  - CentOS 6.5 (kernel version 2.6.32-432).
  - CentOS 6.6.
  - CentOS 6.7 и выше.
  - CentOS 7.2 и выше.
  - CentOS 8.0 и выше.
  - CentOS Stream 9.
  - Debian 4.
  - Debian GNU / Linux 10.1 и выше.
  - Debian GNU / Linux 11.
  - EulerOS 2.0 SPS.

- Linux Mint 19.2 и выше.
- Linux Mint 20.3 и выше.
- openSUSE Leap 15.0 и выше.
- Oracle® Linux 7.3 и выше.
- Oracle Linux 8.0 и выше.
- Oracle Sun Solaris 5.10.
- Red Hat® 7.0 Guinness.
- Red Hat® Enterprise Linux® 6.3.
- Red Hat Enterprise Linux 6.5.
- Red Hat Enterprise Linux 7.2 и выше.
- Red Hat Enterprise Linux 8.0 и выше.
- Red Hat Enterprise Linux 9.
- Red Hat Enterprise Linux Server 5.7.
- Red Hat Enterprise Linux Server 6.9.
- Red Hat Enterprise Linux Workstation 6.7.
- Rocky Linux 8.5 и выше.
- Ruby duck 5.6 (kernel version 2.6.32.-504).
- SUSE Linux Enterprise Server 12.5.
- SUSE Linux Enterprise Server 15.
- Tenis WS (семейство Gentoo).
- Ubuntu 10.04.
- Ubuntu 16.04.
- Ubuntu 16.04 LTS.
- Ubuntu 18.04 LTS.
- Ubuntu 20.04.
- Ubuntu 20.04 LTS.
- Ubuntu 22.04.
- Ubuntu 22.04 LTS.

- Ubuntu Core.
- ALT Linux 8 SP Рабочая Станция.
- ALT Linux 8 SP Сервер.
- ALT Linux Рабочая Станция 10.
- ALT Linux Сервер 10.
- ALT erOS 7.5.
- Гослинукс 7.17.
- Гослинукс 7.2.
- RedOS 7.3.

Обнаружение атрибутов и типовых взаимодействий устройств в Kaspersky Industrial CyberSecurity for Networks

Программа Kaspersky Industrial CyberSecurity for Networks может обнаруживать в сетевом трафике важные сведения об инфраструктуре путем пассивного анализа активности устройств в промышленной сети и сохранять информацию об обнаруженных сетевых устройствах, их атрибутах и взаимодействиях.

Чтобы программа Kaspersky Industrial CyberSecurity for Networks могла получить наиболее точную и полную информацию о компонентах системы управления технологическими процессами, их атрибутах и типичных сетевых взаимодействиях, рекомендуется выполнять различные действия по обслуживанию и другие повседневные операции в системе управления. Это могут быть любые операции, которые вы сочтете приемлемыми. Операции должны быть безопасными, не нарушать нормальный технологический процесс и не оказывать на него негативного влияния.

К таким операциям могут, помимо прочего, относиться следующие действия:

- опрос сетевых устройств;
- инициирование операций между серверами SCADA, Historian, HMI и ПЛК;
- подключение к ПЛК и IED с помощью соответствующего инженерного программного обеспечения;
- загрузка и выгрузка проектов ПЛК;
- запрос информации о конфигурациях ПЛК и версиях прошивок;
- перезагрузка серверов SCADA, Historian, рабочих станций операторов и инженеров;
- перезапуск ПЛК и/или IED.

Для получения сведений о выполнении операций см. документацию к программному обеспечению и оборудованию вашей системы управления технологическим процессом.

Настройка зеркалирования портов для Kaspersky Industrial CyberSecurity for Networks

Для правильной работы программа Kaspersky Industrial CyberSecurity for Networks должна получать копию сетевого трафика, отправляемого с промышленного сетевого коммутатора, настроенного на дублирование сетевых пакетов в назначенный сетевой порт. Эта технология зеркалирования сетевого трафика называется Switched Port Analyzer (SPAN) или Port Mirroring.

Этот раздел содержит примеры настройки зеркалирования портов для нескольких моделей Ethernet-коммутаторов, которые могут использоваться в инфраструктуре промышленной сети. Аналогичные сведения о настройке других моделей коммутаторов вы можете получить в соответствующей документации для вашего сетевого оборудования.

Настройка зеркалирования портов для коммутаторов серий Cisco Access и Distribution

Настройка сеанса SPAN для коммутаторов Cisco Access и Distribution (например, Cisco Catalyst™ 2960 и Cisco Catalyst 3850) выполняется с помощью интерфейса командной строки коммутатора. Для этого необходимо получить доступ к целевому коммутатору через Ethernet или консольный порт и открыть функции управления коммутатором. В режиме настройки создайте новый сеанс мониторинга, выберите диапазон интерфейсов-источников для зеркалирования и анализа трафика, установите интерфейс-адресат и сохраните конфигурацию.

Подробнее о настройке зеркалирования портов для коммутаторов серий Cisco Access и Distribution см. в документации на устройства Cisco.

Чтобы настроить зеркалирование портов для коммутаторов серий Cisco Access и Distribution:

1. Из привилегированного режима EXEC войдите в режим глобальной конфигурации с помощью следующей команды:

   ```
   conf t /
   ```

2. Для просмотра существующих сеансов мониторинга введите команду:

   ```
   show monitor session all /
   ```

3. Если требуется, удалите существующий сеанс мониторинга:

   ```
   no monitor session <номер сеанса> /
   ```

   где `<номер сеанса>` соответствует номеру сеанса мониторинга, который требуется удалить. Вы можете указать значение от 1 до 66. Вместо номера сеанса вы можете использовать следующие ключевые слова:

   - `all` – для удаления всех сеансов мониторинга;
   - `local` – для удаления локальных сеансов мониторинга;
   - `remote` – для удаления удаленных сеансов мониторинга.

4. Укажите номера исходных портов:

   `monitor session <номер сеанса> source interface <исходный порт>/<VLAN-идентификатор> - <исходный порт>/<VLAN-идентификатор> /`

   где:

   - `<номер сеанса>` – номер сеанса мониторинга;
   - `<исходный порт>` – номер исходного порта;
   - `<VLAN-идентификатор>` – VLAN-идентификатор.

5. Укажите номера портов назначения:

   monitor session `<номер сеанса>` destination interface `<порт назначения>/<порт назначения>` `encapsulation replicate /`

   где:

   - `<номер сеанса>` – номер сеанса мониторинга;
   - `<порт назначения>` – номер порта назначения.

6. Вернитесь в привилегированный режим EXEC с помощью следующей команды:

   `end /`

7. Для проверки конфигурации сеанса мониторинга введите команду:

   `show monitor /`

8. Если требуется активировать параметры SPAN после перезагрузки коммутатора, сохраните конфигурацию сеанса мониторинга в файле конфигурации:

   `copy running-config startup-config /`

Настройка зеркалирования портов для коммутаторов серии Cisco Small Business™

Подробнее о настройке коммутаторов серии Cisco Small Business см. в документации на устройства Cisco.

Чтобы настроить зеркалирование портов для коммутаторов Cisco Small Business:

1. Подключитесь к коммутатору и откройте параметры зеркалирования портов в веб-интерфейсе коммутатора.
2. Выберите раздел **Administration** → **Diagnostics** → **Port and VLAN mirroring**.
3. Добавьте интерфейсы-источники и выберите интерфейс-адресат.
4. Примените изменения.

Настройка зеркалирования портов для промышленных Ethernet-коммутаторов Hirschmann

Подробнее о настройке зеркалирования портов для промышленных Ethernet-коммутаторов Hirschmann см. в документации на устройства Hirschmann.

Чтобы настроить зеркалирование портов для промышленных Ethernet-коммутаторов Hirschmann:

1. Подключитесь к коммутатору.
2. В веб-интерфейсе коммутатора выберите раздел **Diagnostics** → **Port Mirroring**.
3. В качестве источника выберите все необходимые порты RX и TX для входящего и исходящего мониторинга.
4. Выберите порт назначения с подключением к Kaspersky Industrial CyberSecurity for Networks.
5. Для включения зеркалирования выберите **On** в разделе **Operation**, а затем выберите **Set**.

   Будут применены изменения к энергозависимой памяти (RAM) устройства.
6. Для сохранения изменений для постоянного использования откройте диалоговое окно и нажмите на кнопку **Save**.

Настройка зеркалирования портов для коммутаторов Siemens серии SCALANCE

Подробнее о настройке зеркалирования портов для коммутаторов Siemens серии SCALANCE см. в документации на устройства Siemens.

Чтобы настроить зеркалирование портов для коммутаторов Siemens серии SCALANCE:

1. Подключитесь к веб-интерфейсу коммутатора и выберите раздел **Layer 2** → **Mirroring**.
2. Для создания сеанса зеркалирования выполните следующие действия:
   a. Выберите вкладку **General**.
   b. Включите зеркалирование.
   c. Для создания записи в таблице нажмите на кнопку **Create**.
      Идентификатор сеанса присваивается автоматически.
   d. В раскрывающемся списке **Session Type** выберите значение **Port Based**.
   e. Нажмите на кнопку **Set Values**.
   f. В столбце **Destination Port** выберите порт назначения.
      Например, **P0.8**.
   g. Нажмите на кнопку **Set Values**.
3. Выберите вкладку **Port**.
4. На вкладке **Port** выполните следующие действия:
   a. В раскрывающемся списке **Session ID** выберите идентификатор сеанса, который вы создали ранее на вкладке **General**.
   b. Для осуществления мониторинга всего трафика данных порта, выберите все порты в таблице в столбцах **Ingress** и **Egress**.
   c. Нажмите на кнопку **Set Values**.

Настройка зеркалирования портов для коммутаторов Siemens серии RUGGEDCOM i800, i801, i802, i803

Подробнее о настройке зеркалирования портов для коммутаторов Siemens серии RUGGEDCOM см. в документации на устройства Siemens.

Чтобы настроить зеркалирование портов для коммутаторов Siemens серии RUGGEDCOM i800, i801, i802, i803:

1. Подключитесь к веб-интерфейсу коммутатора.
   По умолчанию подключение к устройству осуществляется по IP-адресу 192.168.0.1/24.
2. Выберите раздел **Ethernet Ports** → **Configure Port Mirroring**.
3. В параметре **Port Mirroring** выберите **Enabled**.
4. В параметре **Source Port** укажите номер исходного порта.
5. В параметре **Source Direction** выберите **Egress and Ingress**.

6. В параметре **Target Port** укажите номер порта назначения.

7. Нажмите на кнопку **Apply**.

Настройка узла Kaspersky Industrial CyberSecurity for Networks для получения трафика по технологии ERSPAN

Если для передачи зеркалированного трафика на сетевом коммутаторе применяется технология ERSPAN, для приема и обработки этого трафика требуется выполнить дополнительную настройку операционной системы на узле с установленным компонентом Kaspersky Industrial CyberSecurity for Networks (Сервер или сенсор). В результате настройки в операционной системе создается виртуальный сетевой интерфейс, который позволяет узлу с установленным компонентом программы выступать в роли конечной точки назначения для создаваемых туннелей по протоколу GRE (Generic Routing Encapsulation).

Чтобы настроить узел Сервера или сенсора для получения трафика по технологии ERSPAN:

1. На компьютере, на котором установлен компонент программы, откройте консоль операционной системы.

2. Введите команду:

   `sudo ip link add <имя виртуального интерфейса> type erspan local <IP-адрес интерфейса> remote <IP-адрес коммутатора> erspan_ver <версия ERSPAN> seq key <ключ ERSPAN-сессий> erspan <индекс трафика ERSPAN> dev <имя физического интерфейса>`

   где:

   - `<имя виртуального интерфейса>` – имя создаваемого виртуального сетевого интерфейса;
   - `<IP-адрес интерфейса>` – IP-адрес сетевого интерфейса;
   - `<IP-адрес коммутатора>` – IP-адрес сетевого коммутатора, отправляющего зеркалированный трафик;
   - `<версия ERSPAN>` – номер используемой версии ERSPAN (`1` для type II или `2` для type III);
   - `<ключ ERSPAN-сессий>` – уникальный идентификатор, позволяющий группировать зеркалируемый трафик и маршрутизировать его;
   - `<индекс трафика ERSPAN>` – значение поля индекса, представляющее исходящий порт и направление зеркалированного трафика в 20-битном виде;
   - `<имя физического интерфейса>` – имя физического сетевого интерфейса, на который поступает зеркалированный трафик.

     Пример:
     ```
     sudo ip link add erspan1 type erspan local 192.168.2.2 remote 192.168.2.1 erspan_ver 1 seq key 1000 erspan 30 dev enp0s1f5
     ```

3. На созданный виртуальный сетевой интерфейс добавьте точку мониторинга.

Глоссарий

ARP-спуфинг

Прием, который злоумышленники могут применять для проведения сетевой атаки типа "человек посередине" (Man in the middle) в сетях с использованием протокола ARP (Address Resolution Protocol).

CVE

Аббревиатура от Common Vulnerabilities and Exposures. База данных общеизвестных уязвимостей и рисков информационной безопасности. Уязвимостям, описанным в этой базе данных, присваиваются идентификационные номера в формате CVE-<год>-<номер>.

Endpoint Protection Platform (EPP)

Интегрированная система комплексной защиты конечных устройств (например, мобильных устройств, компьютеров или ноутбуков) с помощью различных технологий безопасности. Пример Endpoint Protection Platform – решение Kaspersky Endpoint Security для бизнеса.

EPP-приложение

Приложение, входящее в состав системы защиты конечных устройств (англ. Endpoint Protection Platform, EPP). EPP-приложения устанавливаются на конечные устройства внутри IT-инфраструктуры организации (например, мобильные устройства, компьютеры или ноутбуки). Примером EPP-приложения является Kaspersky Endpoint Security for Windows в составе EPP-решения Kaspersky Endpoint Security for Business.

IOC

Indicator of Compromise (индикатор компрометации). Набор данных о вредоносном объекте или действии.

IOC-файл

Файл, содержащий набор индикаторов IOC, при совпадении с которыми приложение считает событие обнаружением. Вероятность обнаружения может повыситься, если в результате проверки были найдены точные совпадения данных об объекте с несколькими IOC-файлами.

SCADA

Аббревиатура от Supervisory Control And Data Acquisition. Программный пакет, который обеспечивает контроль технологических процессов оператором в реальном времени.

SIEM

Аббревиатура от Security Information and Event Management. Решение для управления информацией и событиями в системе безопасности организации.

Адресное пространство (АП)

Сегмент сети, определяемый по каким-либо правилам, которые задают множества адресов, VLAN-идентификаторов или точек мониторинга.

АСУ ТП

Аббревиатура от "автоматизированная система управления технологическим процессом". Группа технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Внешние системы

Технология регистрации инцидентов, а также событий, которые поступают в Kaspersky Industrial CyberSecurity for Networks от сторонних систем с использованием методов Kaspersky Industrial CyberSecurity for Networks API.

Выделенная сеть Kaspersky Industrial CyberSecurity

Вычислительная сеть, которая состоит из компьютеров, предназначенных для работы программ из состава решения Kaspersky Industrial CyberSecurity, и сетевого оборудования для обеспечения взаимодействия компьютеров. Выделенная сеть должна быть недоступна из других сетей.

Защита конечных устройств

Технология регистрации событий об угрозах, обнаруженных приложениями "Лаборатории Касперского", которые выполняют функции защиты рабочих станций и серверов (например, событие при обнаружении вредоносной программы).

Интеллектуальное электронное устройство (IED)

Комплекс устройств, обеспечивающих своевременное отключение аварийных энергообъектов от энергосистемы и выполняющих необходимые для обеспечения нормальной работы энергосистемы действия в автоматическом или полуавтоматическом режимах.

Инцидент

В Kaspersky Industrial CyberSecurity for Networks инцидентом является событие, которое регистрируется при получении определенной последовательности событий. Инциденты группируют события, имеющие некоторые общие признаки или относящиеся к одному процессу. Kaspersky Industrial CyberSecurity for Networks регистрирует инциденты по правилам корреляции событий.

Карта сетевых взаимодействий

Модель для визуального отображения обнаруженных взаимодействий между устройствами. Карта сетевых взаимодействий содержит следующие объекты: узлы, представляющие устройства, группы устройств и соединения между узлами/группами устройств.

Контроль активов

Технология регистрации событий, связанных с обнаружением информации об устройствах в трафике или в полученных данных от EPP-приложений (например, событие при обнаружении активности ранее неизвестного устройства).

Контроль системных команд

Технология регистрации событий, связанных с обнаружением в трафике системных команд для устройств (например, обнаружение неразрешенной системной команды).

Контроль технологического процесса

Технология регистрации событий, связанных с нарушениями технологического процесса (например, обнаружено превышение заданного значения температуры).

Контроль целостности сети

Технология регистрации событий, связанных с целостностью промышленной сети или с безопасностью взаимодействий (например, обнаружено взаимодействие устройств по неразрешенному протоколу).

Неуправляемый коммутатор

Устройство с отсутствующей адресной информацией, для которого обнаружены или потенциально возможны соединения на топологической карте.

Неуправляемый коннектор

Управляемый вручную программный модуль для обмена данными с программой.

Обнаружение вторжений

Технология регистрации событий, связанных с обнаружением в трафике аномалий, которые являются признаками атак (например, обнаружены признаки ARP-спуфинга).

Политика безопасности

Набор данных, которые определяют параметры работы Kaspersky Industrial CyberSecurity for Networks.

Правило контроля взаимодействий

Описание разрешенного взаимодействия для устройств промышленной сети. При обнаружении сетевого взаимодействия, которое удовлетворяет включенному правилу контроля взаимодействий, Kaspersky Industrial CyberSecurity for Networks не регистрирует событие.

Правило контроля процесса

Набор условий для значений тегов. При выполнении условий правила контроля процесса Kaspersky Industrial CyberSecurity for Networks регистрирует событие.

Правило корреляции событий

Набор условий для проверки последовательностей событий в Kaspersky Industrial CyberSecurity for Networks. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции событий, Kaspersky Industrial CyberSecurity for Networks регистрирует инцидент.

Правило обнаружения вторжений

Набор условий, по которым система обнаружения вторжений анализирует трафик. Правило описывает аномалию трафика, которая может быть признаком атаки в промышленной сети.

Программируемый логический контроллер (ПЛК)

Промышленный контроллер, используемый для автоматизации технологических процессов на предприятии.

Проект ПЛК

Микропрограмма, написанная для ПЛК. Хранится в памяти ПЛК и выполняется в рамках технологического процесса, использующего ПЛК. Проект ПЛК может состоять из блоков, которые по отдельности передаются и принимаются по сети при чтении или записи проекта.

Промышленная сеть

Вычислительная сеть, соединяющая узлы автоматизированной системы управления технологическим процессом промышленного предприятия.

Риск

Потенциальная угроза для ресурсов информационной системы, обнаруженная при анализе трафика и сведений об устройствах.

Роль учетной записи

Совокупность прав доступа, определяющая набор доступных пользователю действий при подключении к Серверу через веб-интерфейс. В Kaspersky Industrial CyberSecurity for Networks предусмотрены роли Администратор и Оператор.

Сенсор Kaspersky Industrial CyberSecurity for Networks

Компонент Kaspersky Industrial CyberSecurity for Networks. Сенсор устанавливается на отдельном компьютере (не на компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks). Сенсор получает и анализирует данные из вычислительных сетей, к которым подключены сетевые интерфейсы компьютера. Для получения и анализа трафика промышленной сети на сетевые интерфейсы должны быть добавлены точки мониторинга. Результаты анализа данных сенсор передает на Сервер.

Сервер Kaspersky Industrial CyberSecurity for Networks

Компонент Kaspersky Industrial CyberSecurity for Networks. Сервер принимает данные, обрабатывает и предоставляет их пользователям программы. Сервер может принимать данные от сенсоров или самостоятельно получать и анализировать данные из вычислительных сетей, к которым подключены сетевые интерфейсы компьютера.

Системная команда

Блок данных в трафике промышленной сети, содержащий команду управления (например, START PLC) или системное сообщение, связанное с функционированием устройств или содержащее результат анализа пакетов (например, REQUEST NOT FOUND).

Событие

Запись, содержащая информацию, которая требует внимания специалиста по безопасности АСУ ТП. Kaspersky Industrial CyberSecurity for Networks сохраняет зарегистрированные события в базе данных. Для просмотра зарегистрированных событий нужно подключиться к Серверу программы через веб-интерфейс. При необходимости можно настроить передачу событий в Kaspersky Security Center и сторонние системы.

Соединение на карте сети

Отображаемый объект на карте сети в виде линии связи между узлами. На карте сетевых взаимодействий обозначает взаимодействие узлов. На топологической карте обозначает физическое подключение узлов.

Тег

Переменная, которая содержит значение какого-либо параметра технологического процесса (например, температуры).

Технология единого входа (SSO)

Механизм, позволяющий пользователю получить доступ к нескольким программным ресурсам, используя одну учетную запись.

Тип риска

Заданный набор параметров для регистрации рисков в Kaspersky Industrial CyberSecurity for Networks. Каждому типу риска присваивается уникальный номер (код типа риска).

Тип события

Заданный набор параметров для регистрации событий в Kaspersky Industrial CyberSecurity for Networks. Каждому типу события присваивается уникальный номер (код типа события).

Топологическая карта

Модель для визуального отображения схемы физических подключений устройств в промышленной сети. Топологическая карта содержит следующие объекты: узлы, представляющие устройства и сетевое оборудование, и соединения, представляющие физические подключения узлов.

Точка мониторинга

Точка приема поступающих данных. Добавляется на сетевой интерфейс узла с установленным Сервером или сенсором Kaspersky Industrial CyberSecurity for Networks и используется для получения копии трафика промышленной сети (например, с порта сетевого коммутатора, настроенного на передачу зеркалированного трафика).

Узел

Компьютер, на котором установлен Сервер или сенсор Kaspersky Industrial CyberSecurity for Networks, либо объект на карте сети, представляющий одно или несколько устройств.

Управляемый коннектор

Программный модуль для обмена данных с программой, предоставляющий возможности автоматической регистрации, запуска и управления. Узлами размещения управляемых коннекторов могут быть только узлы с установленными компонентами программы.

Устройство

Устройство, подключенное к вычислительной сети и идентифицируемое по адресной информации, которую можно сохранить в Kaspersky Industrial CyberSecurity for Networks (например, программируемый логический контроллер, удаленный терминал, интеллектуальное электронное устройство).

Уязвимость устройства

Недостаток в программном или аппаратном обеспечении устройства, используя который злоумышленник может повлиять на работу информационной системы или получить несанкционированный доступ к информации.

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.

Adobe, Flash являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

BACnet – товарный знак компании American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

Apache является либо зарегистрированным товарным знаком, либо товарным знаком Apache Software Foundation.

iPad, iPhone, Mac, Mac OS, macOS и OS X – товарные знаки Apple Inc.

AXIS и AXIS COMMUNICATIONS – зарегистрированные товарные знаки или заявки на регистрацию товарных знаков Axis AB в различных юрисдикциях.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Ubuntu и LTS являются зарегистрированными товарными знаками Canonical Ltd.

Cisco, Cisco AnyConnect, Cisco Catalyst, Cisco Small Business, Aironet, AnyConnect, IOS и Jabber являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Dropbox – товарный знак Dropbox, Inc.

Radmin – зарегистрированный товарный знак Famatech.

Fortinet, FortiGate и FortiOS – товарные знаки или зарегистрированные в США и/или других странах товарные знаки Fortinet, Inc.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

General Electric и Multilin – зарегистрированные товарные знаки компании General Electric.

Google, Android, Chrome, Chromium, Google Chrome и Nexus – товарные знаки Google LLC.

HL7 является зарегистрированным товарным знаком Health Level Seven International и размещение товарного знака не означает одобрение со стороны HL7.

Hitachi – товарный знак Hitachi, Ltd.

EulerOS является товарным знаком Huawei Technologies Co., Ltd.

Intel, Atom, Core и Itanium являются товарными знаками Intel Corporation или ее дочерних компаний.

IBM и DB2 – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Node.js – товарный знак Joyent, Inc.

Juniper – товарный знак или зарегистрированный в США и других странах товарный знак Juniper Networks, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Desktop, Active Directory, ActiveX, AppLocker, Authenticode, BitLocker, BizTalk, Cortana, InPrivate, Internet Explorer, Microsoft Edge, Outlook, PowerShell, SmartScreen, SpyNet, SQL Server, Visual Basic, Visual FoxPro, Win32, Windows, Windows Media, Windows PowerShell, Windows Server, Windows Store, Windows Vista и Windows XP являются товарными знаками группы компаний Microsoft.

MOXA – зарегистрированный товарный знак Moxa Inc.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

DICOM является зарегистрированным товарным знаком National Electrical Manufacturers Association для публикаций Стандартов в отношении цифровой передачи медицинской информации.

ONVIF является товарным знаком ONVIF, Inc.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

OpenVPN – зарегистрированный товарный знак OpenVPN, Inc.

Oracle, Java, JavaScript и Solaris – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, Ansible, CentOS и Fedora – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Remote Utilities – зарегистрированный товарный знак Remote Utilities LLC в США и/или других странах.

Товарный знак BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Schneider Electric – товарный знак компании Schneider Electric.

Sendmail и другие наименования и названия продуктов – товарные знаки или зарегистрированные товарные знаки Sendmail, Inc.

Siemens, Simatic и WinCC – зарегистрированные товарные знаки Siemens AG.

OpenWRT является товарным знаком правообладателя Software Freedom Conservancy (SFC). Kaspersky Industrial CyberSecurity for Networks не связан с OpenWrt.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Dameware – товарный знак, права на который принадлежат компании SolarWinds Worldwide, LLC или аффилированным лицам компании, зарегистрирован в Бюро по патентам и товарным знакам США, а также может быть зарегистрирован или находиться в процессе регистрации в других странах.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

OpenAPI – товарный знак компании The Linux Foundation.

VMware – зарегистрированный товарный знак и/или товарный знак VMware, Inc. в США и других странах.

VxWorks является зарегистрированным товарным знаком ® или знаком обслуживания Wind River Systems, Inc. Данный продукт не связан, не одобрен, не спонсируется и не поддерживается сторонним правообладателем упомянутого товарного знака.