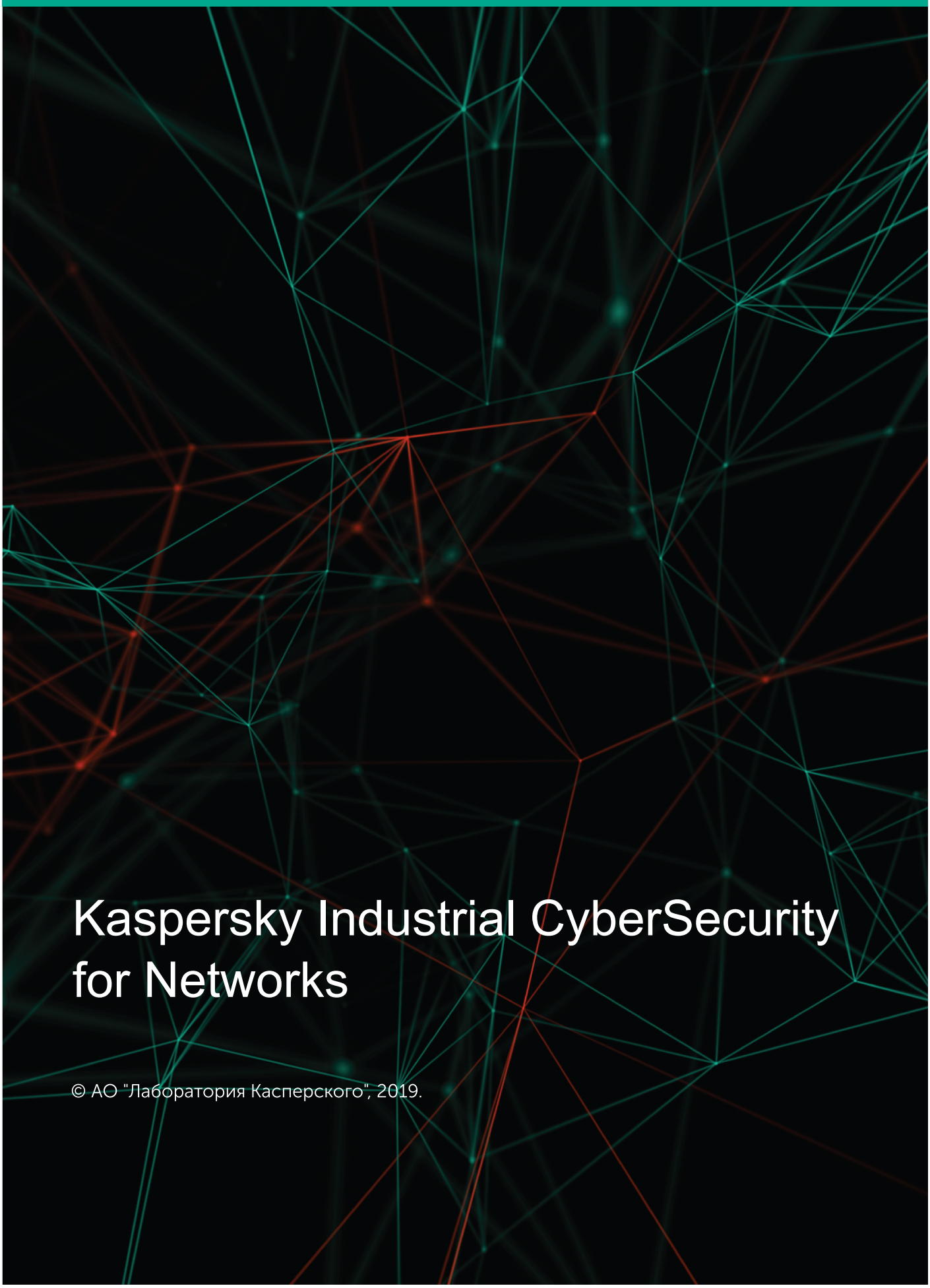
kaspersky



Kaspersky Industrial CyberSecurity for Networks

Содержание

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 контроля активности устройств в промышленной сети, для обнаружения неразрешенных системных команд, передаваемых или получаемых устройствами, а также для выявления попыток установки недопустимых значений параметров технологического процесса. Программа входит в состав решения Kaspersky Industrial CyberSecurity.

Kaspersky Industrial CyberSecurity for Networks выполняет следующие функции:

- Проверяет взаимодействия между устройствами промышленной сети на соответствие заданным правилам контроля сети.
- Контролирует устройства в промышленной сети и обнаруживает активность ранее неизвестных программе устройств и устройств, которые не должны использоваться в промышленной сети или длительное время не проявляют активность. При контроле устройств программа может автоматически обновлять сведения об устройствах на основании данных, полученных в сетевых пакетах.
- Отображает сетевые взаимодействия между устройствами промышленной сети в виде карты сети. При отображении объекты визуально выделяются по различным признакам (например, объекты, требующие внимания).
- 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.
- Анализирует трафик промышленной сети на наличие в сетевых пакетах системных команд, передаваемых или получаемых устройствами, которые участвуют в автоматизации технологического процесса на предприятии (далее также "устройства для контроля процесса"). Обнаруживает в трафике системные команды и ситуации, которые могут быть признаками нарушения безопасности промышленной сети.
- Контролирует операции чтения и записи проектов для программируемых логических контроллеров, сохраняет полученную информацию о проектах и сравнивает эту информацию с ранее полученной информацией.
- 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 сетевых пакетов.
- 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. Правила корреляции могут обновляться при установке обновлений.
- Сохраняет в базе данных трафик, относящийся к зарегистрированным событиям. Трафик может сохраняться автоматически при включенном сохранении трафика для типов событий или по запросу на загрузку трафика.

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

Комплект поставки

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

- скрипт установки программы: kics4net-deploy-<номер версии программы>.bundle.sh;
- пакет для установки Сервера и сенсоров: kics4net-<номер версии программы>.x86_64.rpm;
- пакет для установки Консоли: kics4net-utm-<номер версии программы>.x86_64.rpm;
- пакет для установки СУБД: kics4net-postgresql-<номер версии СУБД>.x86_64.rpm;
- пакет для установки системы обнаружения вторжений: kics4net-suricata-<номер версии системы>.x86_64.rpm;
- пакет для установки Веб-сервера: kics4net-webserver-<номер версии программы>.x86_64.rpm;
- пакет для установки Агента администрирования из состава комплекта поставки Kaspersky Security Center: klnagent64-<номер версии Агента администрирования>.x86_64.rpm;
- пакеты для установки плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center: kics4net-sc-plugin_<номер версии плагина>_<код локализации>.msi;
- пакет с набором proto-файлов для Kaspersky Industrial CyberSecurity for Networks API: kics4net-api-<номер версии программы>.tar.gz;
- файлы с текстом Лицензионного соглашения на русском и английском языках;
- файлы с текстом Политики конфиденциальности на русском и английском языках;
- файлы с информацией о версии (Release Notes) на русском и английском языках;
- файл с информацией о стороннем коде (Legal Notices) на английском языке.

Аппаратные и программные 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;
  - объем оперативной памяти: 32 ГБ;
  - объем свободного пространства на жестком диске: 750 ГБ и дополнительно по 250 ГБ для каждой точки мониторинга на этом компьютере.

- Компьютер, который будет выполнять функции сенсора:
  - центральный процессор: Intel Core i5 / i7;
  - объем оперативной памяти: 4 ГБ и по 2 ГБ для каждой точки мониторинга на этом компьютере;
  - объем свободного пространства на жестком диске: 50 ГБ и по 250 ГБ для каждой точки мониторинга на этом компьютере.

При использовании сенсоров пропускная способность выделенной сети Kaspersky Industrial CyberSecurity между Сервером и сенсорами должна превышать пропускную способность промышленной сети не менее чем в два раза.

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

- Операционная система CentOS 7.6.1810.

  При установке операционной системы рекомендуется выделить все пространство жесткого диска (за вычетом пространства, необходимого для boot- и swap-разделов) для системного (корневого) раздела.

- 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 7.6.1810 должно быть установлено следующее программное обеспечение:
  - среда рабочего стола KDE версии, входящей в состав операционной системы CentOS 7.6.1810;
  - интерпретатор Python версии 2.7;
  - пакет для синхронизации времени chrony версии 3.1 и выше.
- На компьютере, который будет выполнять функции Сервера, должен быть правильно настроен почтовый сервер (Mail Transfer Agent) для отправки сообщений электронной почты получателям уведомлений, настроенным в Консоли программы.

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 установки плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center на компьютере Сервера администрирования Kaspersky Security Center должно быть установлено обновление Windows® KB2999226. Установка обновления требуется, если проблемы, устраняемые этим обновлением, актуальны для установленной версии операционной системы и конфигурации установленного программного обеспечения на компьютере Сервера администрирования (см. описание к указанному обновлению).

Для подключения к Веб-серверу могут использоваться следующие веб-браузеры:

- Google Chrome™ версии 78 и выше.

- Mozilla™ Firefox™ версии 70 и выше.
- Microsoft® Edge версии 44 и выше.

Программа Kaspersky Industrial CyberSecurity for Networks совместима со следующими версиями программ из состава решения Kaspersky Industrial CyberSecurity:

- Kaspersky Security Center версии 10 с установленным Service Pack 3 или версии 11.
- Kaspersky Industrial CyberSecurity for Nodes версии 2.5 или 2.6.

Обзор функциональности Kaspersky Industrial CyberSecurity for Networks

Функциональность для анализа трафика промышленной сети

В Kaspersky Industrial CyberSecurity for Networks анализ трафика промышленной сети обеспечивает следующая функциональность:

- Контроль устройств. Эта функциональность позволяет отслеживать активность устройств и изменение сведений об устройствах на основании данных, полученных в сетевых пакетах. Для автоматического получения сведений об устройствах программа анализирует трафик промышленной сети по правилам определения сведений об устройствах и протоколов взаимодействия устройств. Также совместно с функциональностью контроля процесса обеспечивается контроль чтения и записи проектов для программируемых логических контроллеров. Для контроля устройств в программе формируется таблица, которая содержит сведения, полученные автоматически из трафика или указанные вручную. Настройку контроля устройств можно выполнять при работе с таблицей устройств. Также некоторые возможности настройки доступны при работе с картой сети.
- Контроль сети. Эта функциональность позволяет отслеживать взаимодействия между устройствами промышленной сети. Обнаруженные взаимодействия проверяются на соответствие заданным правилам контроля сети. При обнаружении взаимодействия, которое описано в активном правиле контроля сети, программа считает это взаимодействие разрешенным и не регистрирует событие.
- Контроль технологического процесса (далее также "контроль процесса"). Эта функциональность позволяет отслеживать в трафике значения параметров технологического процесса и системные команды, передаваемые или получаемые устройствами. Для отслеживания значений параметров технологического процесса используются правила контроля процесса, по которым программа определяет недопустимые значения. Списки отслеживаемых системных команд формируются при настройке параметров устройств для контроля процесса.
- Обнаружение вторжений. Эта функциональность позволяет обнаруживать в трафике признаки атак или нежелательную сетевую активность. Для обнаружения используются правила обнаружения вторжений и встроенные алгоритмы проверки сетевых пакетов. При обнаружении в трафике условий, заданных в активном правиле обнаружения вторжений, программа регистрирует событие срабатывания правила. С помощью встроенных алгоритмов проверки сетевых пакетов программа обнаруживает признаки подмены адресов в ARP-пакетах и различные аномалии в протоколах TCP и IP.

Настройку функциональности для анализа трафика промышленной сети выполняет пользователь программы с ролью Администратор.

Kaspersky Industrial CyberSecurity for Networks может использоваться совместно с решением Kaspersky Machine Learning for Anomaly Detection для обеспечения безопасности киберфизической системы (АСУ ТП, интернет вещей, индустриальный интернет вещей) на основе обнаружения и интерпретации аномалий методами машинного обучения в телеметрии от операционных технологий защищаемого объекта.

Функциональность для решения типовых задач оператора

Для решения типовых задач при наблюдении за состоянием технологического процесса в Kaspersky Industrial CyberSecurity for Networks можно использовать учетные записи пользователей программы с ролью Оператор. Эти пользователи могут использовать следующую функциональность:

- **Отображение сведений для мониторинга системы в онлайн-режиме**. Эта функциональность позволяет просматривать наиболее значимые изменения в системе, произошедшие к текущему моменту. При мониторинге системы в онлайн-режиме вы можете просмотреть сведения об устройствах, требующих внимания, и сведения о событиях и инцидентах с наиболее поздним временем последнего появления.

- **Отображение данных на карте сети**. Эта функциональность позволяет визуально отображать обнаруженные взаимодействия между устройствами промышленной сети. При просмотре карты сети вы можете быстро определить проблемные объекты или объекты с другими признаками и просмотреть сведения об этих объектах. Для удобного представления информации предусмотрены возможности распределения устройств на карте сети автоматически или вручную.

- **Отображение сведений о событиях и инцидентах**. Эта функциональность позволяет загрузить зарегистрированные события и инциденты из базы данных Сервера. По умолчанию, чтобы обеспечить возможность мониторинга новых событий и инцидентов, программа загружает события и инциденты с наиболее поздним временем последнего появления. Также вы можете загружать события и инциденты за любой период. При просмотре таблицы событий вы можете изменять статусы событий и инцидентов, копировать и экспортировать данные, загружать трафик и выполнять другие действия.

- **Отображение сведений для мониторинга параметров технологического процесса**. Эта функциональность позволяет просматривать значения параметров технологического процесса, которые обнаружены в трафике на текущий момент. Информация о параметрах представлена в виде таблицы с автоматически обновляемыми значениями параметров.

Функциональность для управления работой программы

Для управление работой программы в части общей настройки и контроля использования пользователь программы с ролью Администратор может использовать следующую функциональность:

- **Управление точками мониторинга**. Эта функциональность позволяет добавить в программу точки мониторинга для получения трафика из промышленной сети. Также с помощью этой функциональности можно временно приостанавливать и возобновлять наблюдение за сегментами промышленной сети, выключая и включая соответствующие точки мониторинга (например, на время проведения профилактических и пусконаладочных работ на АСУ ТП).

- **Управление технологиями**. Эта функциональность позволяет включать и выключать использование технологий и методов для анализа трафика промышленной сети, а также изменять режим работы технологий и методов. Вы можете включать, выключать и изменять режим работы технологий и методов независимо друг от друга.

- **Разделение доступа к функциям программы**. Эта функциональность позволяет разграничить доступ пользователей к функциям программы. Разграничение доступа выполняется на основе ролей учетных записей пользователей программы.

- **Контроль состояния программы**. Эта функциональность позволяет контролировать текущее состояние Kaspersky Industrial CyberSecurity for Networks, а также просматривать сообщения программы и записи аудита действий пользователей за любой период. Доступ к журналу с сообщениями программы имеют также пользователи с ролью Оператор.

- **Обновление баз и программных модулей**. Эта функциональность позволяет загружать и устанавливать обновления, повышающие эффективность анализа трафика и обеспечивающие

максимальную защиту от угроз в промышленной сети. Функциональность обновления доступна после добавления лицензионного ключа в Kaspersky Industrial CyberSecurity for Networks или в Kaspersky Security Center. Вы можете запускать установку обновлений автоматически в соответствии с заданным расписанием или вручную.

- **Функциональность настройки типов регистрируемых событий**. Эта функциональность позволяет сформировать и настроить список типов событий для регистрации в Kaspersky Industrial CyberSecurity for Networks и передачи в сторонние системы (например, в SIEM-систему), а также в Kaspersky Security Center. Также при настройке типов событий вы можете добавить типы событий для регистрации с помощью методов Kaspersky Industrial CyberSecurity for Networks API.

- **Управление журналами**. Эта функциональность позволяет изменить параметры сохранения данных в журналах работы программы. Вы можете настраивать параметры хранения записей в журналах и параметры сохранения трафика в базе данных. Также вы можете изменять уровни ведения журналов работы процессов.

- **Использование интерфейса прикладного программирования**. Эта функциональность позволяет использовать в сторонних программах набор функций, реализуемых через Kaspersky Industrial CyberSecurity for Networks API. С помощью предоставляемых методов Kaspersky Industrial CyberSecurity for Networks API вы можете получать данные о событиях, о тегах, отправлять события в Kaspersky Industrial CyberSecurity for Networks и выполнять другие действия.

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.

Также рекомендуется ограничить доступ к оборудованию, на котором работает программа.

При внедрении Kaspersky Industrial CyberSecurity for Networks рекомендуются следующие меры:

- Ограничение доступа к компьютерам, на которых установлены Сервер и сенсоры Kaspersky Industrial CyberSecurity for Networks, а также к сетевому оборудованию выделенной сети.

- Обеспечение доступа персоналу, обладающему полномочиями по установке и настройке оборудования и программного обеспечения Сервера и сенсоров, а также пользователям программы.

- Контроль физического доступа к оборудованию, на котором работает программа, с помощью технических средств или службы охраны.

- Ограничение доступа к сетевому оборудованию, которое используется для получения данных из промышленной сети и взаимодействия компонентов программы.

- Мониторинг доступа в контролируемые помещения с помощью средств охранной сигнализации.

- Видеонаблюдение в контролируемых помещениях.

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.
- Завершение сеанса подключения к Серверу перед окончанием работы пользователя в веб-браузере или в Консоли программы.

  Для принудительного завершения сеанса подключения в веб-браузере нужно использовать пункт **Выход** в меню пользователя. Для принудительного завершения сеанса подключения в Консоли программы нужно закрыть окно Консоли.

Что нового

В Kaspersky Industrial CyberSecurity for Networks 2.9 появились следующие возможности и доработки:

- Дерево групп устройств – добавлена функциональность работы с деревом групп устройств. Для известных программе устройств можно указывать группы для распределения устройств в соответствии с их назначением, размещением или по другим произвольным признакам.

- Метки для устройств – добавлена функциональность установки и удаления меток для известных программе устройств. Метки могут содержать произвольные текстовые описания устройств.

- Управление точками мониторинга – реализована возможность добавления и удаления точек мониторинга на узлах Сервера и сенсоров без необходимости переустановки компонентов программы. Для приостановки и возобновления обработки трафика можно выключать и включать точки мониторинга (функциональность приостановки и возобновления работы Сервера и / или сенсоров исключена).

- Определение протоколов по содержимому сетевых пакетов – для контроля сети и регистрации событий реализовано определение отдельных протоколов прикладного уровня по данным, которые составляют полезную нагрузку сетевых пакетов.

- Обнаружение неизвестных тегов – добавлена функциональность обнаружения и сохранения информации о тегах, отсутствующих в политике безопасности, но относящихся к устройствам для контроля процесса.

- Расширенная функциональность сохранения трафика для событий – реализованы возможности включения сохранения трафика для инцидентов (при этом будет сохраняться трафик для всех событий, вложенных в инциденты) и получения трафика, отсутствующего в базе данных, из временных файлов дампа трафика (по запросу на загрузку трафика).

- Сворачивание меню на странице веб-интерфейса – реализована возможность сворачивания и разворачивания меню в левой части страницы веб-интерфейса программы. Сворачивание и разворачивание меню выполняется с помощью кнопки.

- Выбор всех элементов в таблицах – добавлена функциональность быстрого выбора всех элементов, удовлетворяющих текущим параметрам фильтрации и поиска в таблицах устройств, правил контроля сети и событий. Выбрать все элементы можно с помощью комбинации клавиш CTRL+A или с помощью флажка в заголовке левой крайней графы таблицы.

- Отображение количества необработанных событий – добавлена информационная панель в раздел **События** для отображения сведений о количестве событий со статусами *Новое* и *В обработке*.

- Поиск узлов на карте сети.

- Сохранение и загрузка видов (параметров отображения) карты сети.

- Использование Kaspersky Security Center для загрузки обновлений – реализована возможность выбора Сервера администрирования Kaspersky Security Center в качестве источника обновлений баз и программных модулей.

- Добавление лицензионного ключа из Kaspersky Security Center – реализована возможность добавления лицензионного ключа в Kaspersky Industrial CyberSecurity for Networks с использованием функциональности Kaspersky Security Center для автоматического распространения лицензионных ключей.

- Расширенная функциональность интерфейса прикладного программирования (API) – добавлена функциональность получения данных об устройствах из таблицы устройств.

- Информация о работе с программой представлена в виде онлайн-справки – сведения об установке, настройке и использовании Kaspersky Industrial CyberSecurity for Networks (в том числе об использовании Kaspersky Industrial CyberSecurity for Networks API) публикуются на странице Kaspersky Online Help. Онлайн-справка предоставляет удобные средства для поиска, просмотра и печати информации, а также для получения электронных документов в формате PDF.

- Расширенная поддержка протоколов прикладного уровня – реализованы дополнительные возможности анализа трафика поддерживаемых протоколов прикладного уровня и добавлены новые поддерживаемые протоколы.

- Расширенная поддержка оборудования – добавлены новые поддерживаемые устройства.

Архитектура программы

Kaspersky Industrial CyberSecurity for Networks включает в себя следующие компоненты:

- *Сервер* – основной компонент, который принимает и обрабатывает информацию о трафике промышленной сети, сохраняет и предоставляет данные (например, события и сведения об устройствах). В программе может использоваться только один Сервер.

- *Веб-сервер* – предоставляет интерфейс для подключения к Серверу через веб-браузер (веб-интерфейс). Используя веб-интерфейс, пользователи программы могут просматривать данные, предоставляемые Сервером, и управлять работой программы. Веб-сервер устанавливается на компьютере, который выполняет функции Сервера. Для безопасного соединения с Веб-сервером используются сертификаты.

- *Консоль* – реализует графический интерфейс для подключения к Серверу. С помощью Консоли пользователи программы могут настраивать функциональность, которая недоступна для управления через веб-интерфейс. Консоль устанавливается на компьютере, который выполняет функции Сервера.

- *Сенсор* – получает копию трафика промышленной сети, обрабатывает полученные данные и передает их Серверу. Сенсоры устанавливаются на отдельных компьютерах (не на компьютере, который выполняет функции Сервера). В программе может использоваться до 32 сенсоров.

Сервер Kaspersky Industrial CyberSecurity for Networks выполняет следующие функции:

- принимает информацию о трафике от сенсоров Kaspersky Industrial CyberSecurity for Networks и / или самостоятельно получает копию трафика промышленной сети;

- регистрирует события и сохраняет их в базе данных;

- контролирует работоспособность программы;

- контролирует действия пользователей программы;

- обрабатывает поступающие запросы от Веб-сервера и Консоли и предоставляет запрашиваемые данные;

- передает события в Kaspersky Security Center и сторонние системы (например, в SIEM-систему).

Веб-сервер, взаимодействуя с Сервером, предоставляет пользователю программы следующие возможности:

- просматривать в онлайн-режиме сведения об устройствах, событиях и технологических параметрах;

- просматривать и обрабатывать зарегистрированные события;

- просматривать и изменять сведения о контролируемых устройствах;

- просматривать сведения о взаимодействиях устройств;

- настраивать функции программы;

- просматривать сведения о работе программы;

- просматривать записи аудита действий пользователей.

Консоль предоставляет пользователю программы следующие возможности:

- настраивать правила контроля процесса;
- формировать список регистрируемых типов событий;
- настраивать передачу событий в сторонние системы;
- настраивать правила обнаружения вторжений;
- настраивать обновление баз и программных модулей.

Сенсор Kaspersky Industrial CyberSecurity for Networks выполняет следующие функции:

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

Сенсоры и / или Сервер получают копию трафика промышленной сети от *точек мониторинга*. 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.

Вы можете добавить не более 8 точек мониторинга на сенсоре и не более 4 точек мониторинга на Сервере. Всего в программе вы можете использовать не более 32 точек мониторинга.

> 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).

Пользователи программы могут подключаться к Серверу через веб-интерфейс или Консоль как на компьютере, который выполняет функции Сервера, так и удаленно. При этом удаленная работа с Консолью возможна только с использованием системы удаленного доступа к рабочему столу.

Для соединения узлов с установленными компонентами Kaspersky Industrial CyberSecurity for Networks и другими компонентами решения Kaspersky Industrial CyberSecurity (Kaspersky Industrial CyberSecurity for 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 через веб-интерфейс;
- компьютер с Kaspersky Industrial CyberSecurity for Nodes;
- компьютер с Kaspersky Security Center;
- сетевой коммутатор.

Установка и удаление программы

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

Типовые схемы развертывания

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

- установка только Сервера без сенсоров;
- установка Сервера с сенсорами.

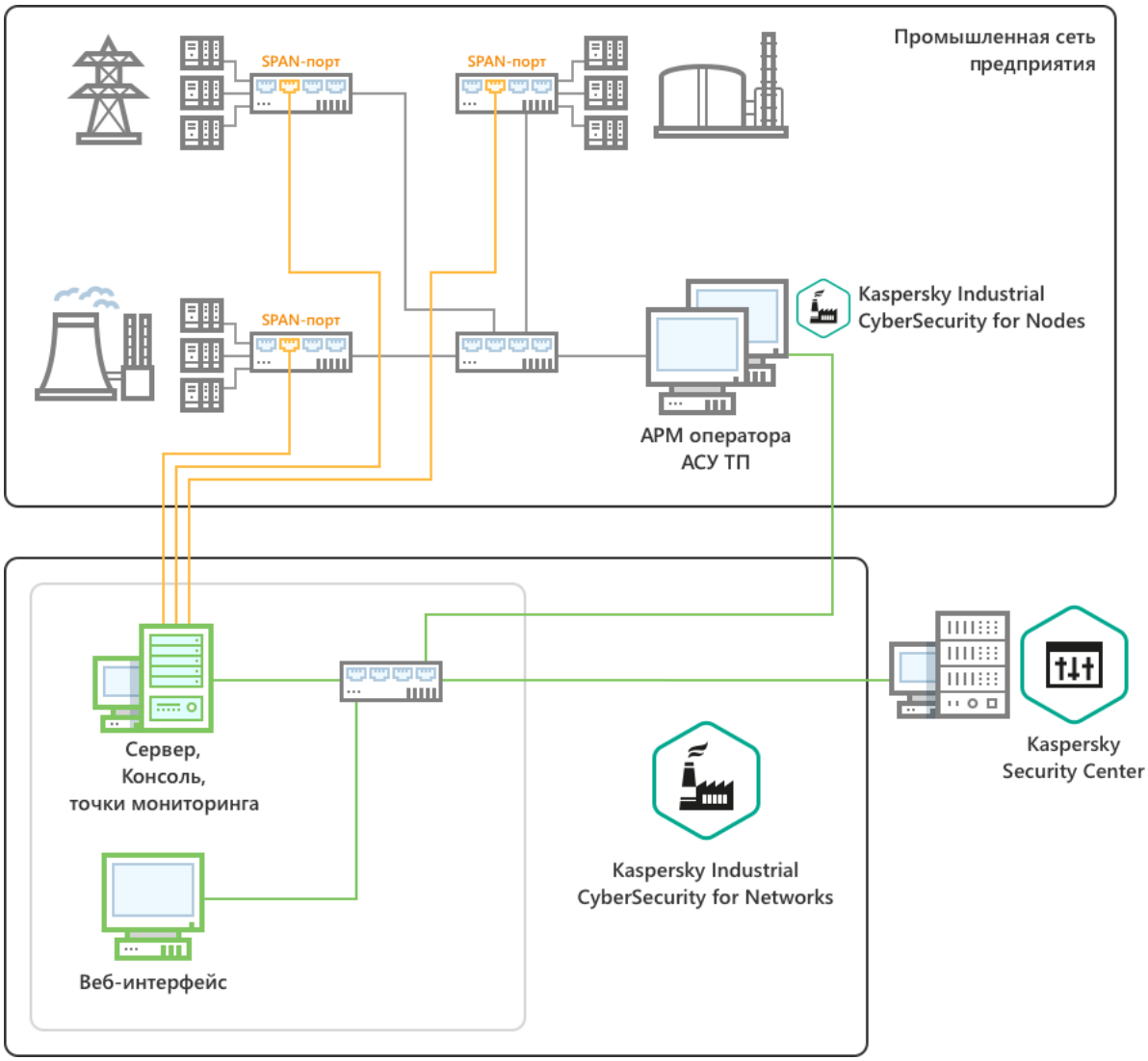
Сервер Kaspersky Industrial CyberSecurity for Networks устанавливается вместе с Консолью. Также при установке Сервера устанавливается Веб-сервер, который обеспечивает подключение к Серверу через веб-интерфейс.

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 Security Center). Минимальное требование к пропускной способности выделенной сети при установке Сервера и сенсоров Kaspersky Industrial CyberSecurity for Networks см. в разделе Аппаратные и программные требования.

Установка Сервера без сенсоров

При установке Сервера без сенсоров весь трафик промышленной сети должен поступать на компьютер, выполняющий функции Сервера. Вы можете применить этот способ установки, если компьютер имеет достаточное количество сетевых интерфейсов, на которые будет поступать трафик из всех сегментов промышленной сети. После установки программы вам нужно добавить точки мониторинга на эти сетевые интерфейсы. Добавление точек мониторинга выполняется при подключении к Серверу через веб-интерфейс. Вы можете использовать не более 4 точек мониторинга на Сервере.

В примере (см. рис. ниже) показана схема 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 сенсоров

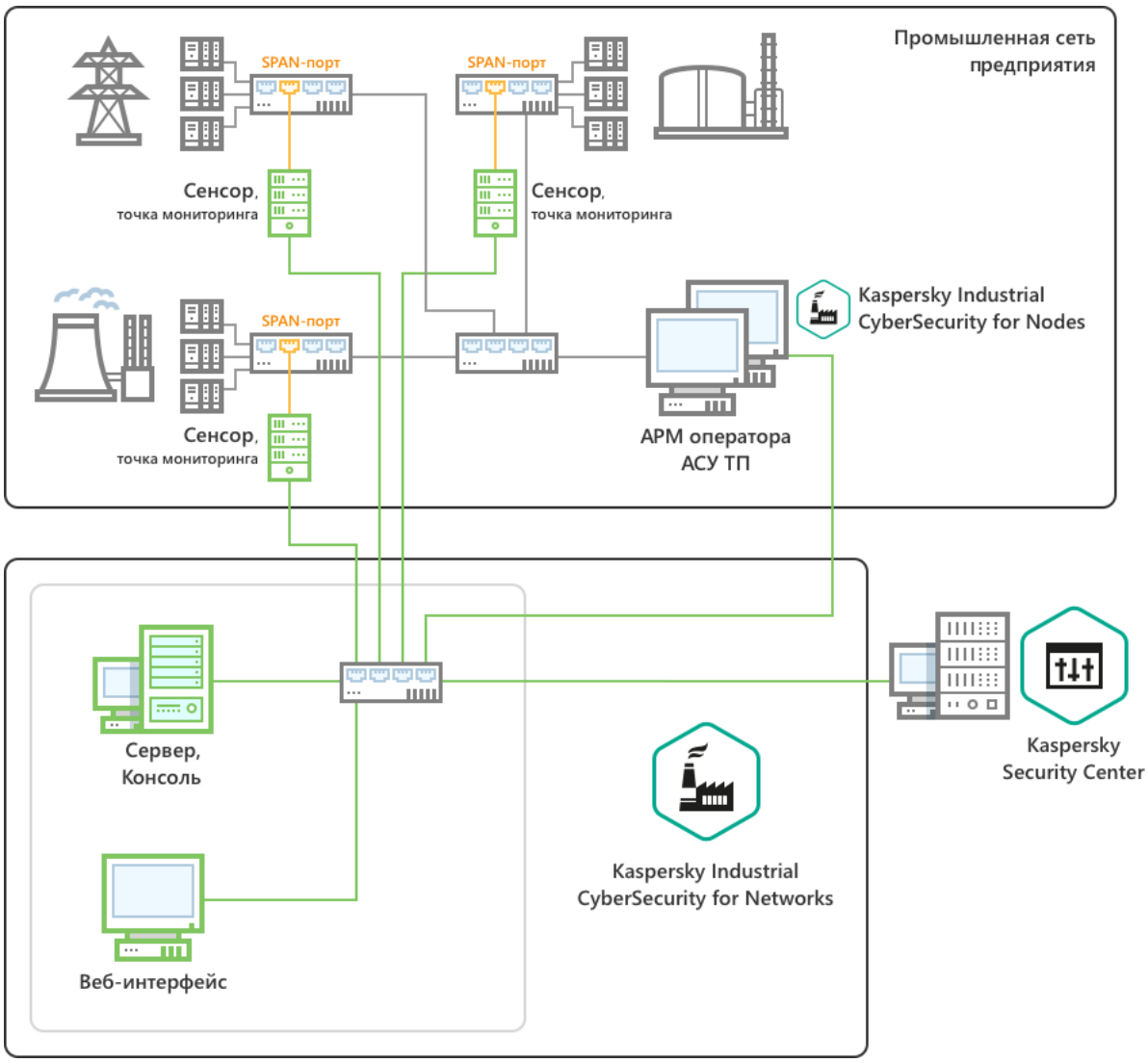
Для установки Сервера и сенсоров вы можете использовать от 2 до 33 компьютеров. На одном из компьютеров устанавливается Сервер. На остальных компьютерах устанавливаются сенсоры, которые будут получать трафик из соответствующих сегментов промышленной сети.

После установки программы на всех компьютерах с установленными сенсорами требуется добавить точки мониторинга. Если компьютер с установленным Сервером имеет сетевой интерфейс, подключенный к промышленной сети, вы также можете добавить точку мониторинга на этот сетевой интерфейс. Добавление точек мониторинга выполняется при подключении к Серверу через веб-интерфейс.

Если компьютер имеет несколько сетевых интерфейсов, на которые поступает трафик из различных сегментов промышленной сети, вам потребуется добавить точку мониторинга на каждый такой интерфейс. При этом вам нужно учитывать ограничения на максимальное количество точек мониторинга:

- не более 8 точек мониторинга на сенсоре;
- не более 4 точек мониторинга на Сервере;
- не более 32 точек мониторинга в программе.

В примере (см. рис. ниже) показана схема 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

Подготовка к установке программы

Перед началом установки Kaspersky Industrial CyberSecurity for Networks убедитесь, что компьютеры удовлетворяют аппаратным и программным требованиям. После этого проверьте выполнение следующих условий:

- К компьютерам есть сетевой доступ, настроен и открыт доступ по протоколу SSH.
- На компьютере, с которого будет выполняться установка, вы можете работать в системе как пользователь без root-прав.

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.

Чтобы подготовить компьютеры к установке программы, выполните следующие действия:

1. Подготовьте учетные записи пользователей:

   - На всех компьютерах, на которых будут установлены компоненты программы, назначьте одинаковый пароль для учетной записи пользователя с root-правами (от имени этого пользователя 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 потребуются при установке программы.

     После установки программы рекомендуется изменить пароли для этих пользователей.

   - На компьютере, который будет выполнять функции Сервера, создайте локальные учетные записи пользователей (или выберите существующие учетные записи), которым будет разрешено запускать Консоль программы. Этим учетным записям не потребуются root-права для исполнения команд. Локальные учетные записи будут использоваться для входа в систему и последующего запуска Консоли программы (при этом после запуска Консоли дополнительно требуется указывать учетные данные пользователя программы, которые могут не совпадать с данными локальной учетной записи). Запомните имена созданных или выбранных локальных учетных записей. Эти данные потребуются при установке программы.

     Локальные учетные записи, которым нужно разрешить запуск Консоли программы, указываются при настройке параметров установки программы. Эти учетные записи автоматически включаются в специальную группу kics4net, которая создается в операционной системе во время установки программы. После установки программы вы можете вручную добавлять нужные учетные записи в группу kics4net с помощью стандартных средств операционной системы.

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 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. На компьютере, с которого будет выполняться установка, создайте произвольную директорию для хранения файлов установки.

5. В созданную директорию скопируйте следующие файлы из комплекта поставки Kaspersky Industrial CyberSecurity for Networks:

   - скрипт установки программы kics4net-deploy-<номер версии программы>.bundle.sh;
   - пакет для установки Сервера и сенсоров: kics4net-<номер версии программы>.x86_64.rpm;
   - пакет для установки Консоли: kics4net-utm-<номер версии программы>.x86_64.rpm;
   - пакет для установки СУБД: kics4net-postgresql-<номер версии СУБД>.x86_64.rpm;
   - пакет для установки системы обнаружения вторжений: kics4net-suricata-<номер версии системы>.x86_64.rpm;
   - пакет для установки Веб-сервера: kics4net-webserver-<номер версии программы>.x86_64.rpm;
   - пакет для установки Агента администрирования из состава комплекта поставки Kaspersky Security Center: klnagent64-<номер версии Агента администрирования>.x86_64.rpm.

     Пакет для установки Агента администрирования нужен, если вы хотите контролировать состояние программы, получать лицензионный ключ и загружать обновления программы с помощью Kaspersky Security Center. Агент администрирования – это компонент Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования Kaspersky Security Center и программами "Лаборатории Касперского", установленными на конкретном узле (рабочей станции или сервере). Подробную информацию об Агенте администрирования вы можете получить в справочной системе для Kaspersky Security Center.

   Директория с перечисленными файлами потребуется при установке, изменении параметров установки и удалении программы.

Команды меню установки

В этом разделе приведены сведения об основных командах меню установки. Меню установки выводится на экран при запуске скрипта установки программы kics4net-deploy-<номер версии программы>.bundle.sh. Этот файл находится в директории, созданной при подготовке к установке программы.

С помощью меню установки вы можете создать или изменить конфигурацию параметров установки программы и запустить процедуру установки в заданной конфигурации.

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.

Главное меню содержит следующие группы команд:

- команды управления Сервером;
- команды управления сенсорами;
- общие команды установки;
- команды выхода из меню установки.

Команды меню установки для управления Сервером

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.
  - **Введите IP-адрес для подключений к Серверу** – задает IP-адрес, по которому к Серверу будут подключаться другие компоненты (например, сенсоры). По умолчанию указан IP-адрес узла для установки Сервера.
  - **Введите имя Сервера** – задает 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.
  - **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. При добавлении функциональности взаимодействия программы с Kaspersky Security Center требуется указать IP-адрес / имя компьютера с Kaspersky Security Center и SSL-порт для подключения.

Если добавлена функциональность взаимодействия программы с Kaspersky Security Center, при установке программы устанавливается компонент Агент администрирования Kaspersky Security Center. 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.

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

- **Введите IP-адрес или имя компьютера с Веб-сервером** – задает IP-адрес / имя компьютера Сервера для подключения через веб-интерфейс.

- **Введите номер порта Веб-сервера** – задает номер порта для подключения через веб-интерфейс. Если указан номер порта по умолчанию (443), при подключении через веб-браузер пользователю будет достаточно ввести только IP-адрес / имя компьютера. В этом случае протокол HTTPS и номер порта определяются автоматически.

- **Введите имя пользователя программы** – задает имя пользователя для подключения к Серверу и работы с программой. 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. Указанное имя пользователя будет использоваться только при подключении к Серверу через веб-интерфейс или в Консоли программы. Для этого пользователя не требуется регистрация в качестве учетной записи операционной системы компьютера Сервера или другого компьютера. Ввод нового пароля для пользователя запрашивается при установке Сервера (если не найдена другая учетная запись пользователя программы с таким же именем).

- **Использовать самоподписанные сертификаты для соединения с Веб-сервером** – позволяет выбрать вариант использования сертификатов для защиты подключения через веб-интерфейс. Вы можете использовать самоподписанный сертификат Веб-сервера или сертификат, изданный доверенным центром сертификации (далее "доверенный сертификат"). Если вы хотите выбрать вариант использования самоподписанного сертификата, требуется ввести символ `y` в этом запросе. Самоподписанный сертификат будет создан при установке Сервера. Если вы хотите выбрать вариант использования доверенного сертификата, требуется ввести символ `n` в этом запросе и затем символ `y` в запросе **Использовать доверенные сертификаты для соединения с Веб-сервером**. Для загрузки доверенного сертификата требуется указать путь к файлу доверенного сертификата. Этот файл будет скопирован в директорию с сертификатами Веб-сервера при установке Сервера. Если не выбран ни один из вариантов (на оба запроса введен символ `n`), при установке Сервера будет либо создан самоподписанный сертификат, либо использован имеющийся сертификат в директории с сертификатами Веб-сервера (если остался сертификат от ранее установленного Сервера).

Если вы хотите использовать в программе доверенный сертификат, он должен быть выдан на тот IP-адрес или на то имя компьютера, которые будут указывать пользователи программы при подключении через веб-интерфейс. Для загрузки доверенного сертификата вы можете использовать файл формата PFX с сохраненным доверенным сертификатом и закрытым ключом. Файл должен быть создан без заданного пароля для доступа к содержимому.

- **Введите имя пользователя операционной системы для запуска Консоли** – задает имя пользователя операционной системы, которому будет разрешено запускать Консоль Kaspersky Industrial

CyberSecurity for Networks. После ввода имени пользователя появляется запрос **Указать имя еще одного пользователя**. Если требуется разрешить запуск Консоли еще одному пользователю, вам нужно ввести символ **y** в этом запросе и затем указать имя другого пользователя (таким способом вы можете последовательно указать несколько пользователей). После того, как вы указали имена всех нужных пользователей, нужно ввести символ **n** в запросе **Указать имя еще одного пользователя**. Разрешение на запуск Консоли предоставляется путем добавления пользователя в группу kics4net при установке Сервера.

> Указанным пользователям предоставляется разрешение только на запуск Консоли. Для работы с Консолью требуется ввести учетные данные пользователя программы в запросе, который выводится сразу после запуска Консоли.

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

  - **Изменить имя Сервера** – изменяет имя Сервера в составе решения Kaspersky Industrial CyberSecurity. Этот пункт меню аналогичен пункту **Введите имя Сервера** в меню **Добавить Сервер**.

  - **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 автоматический запуск kics4net** – выключает автоматический запуск сервиса kics4net при запуске операционной системы.

  - **Задать ограничение занимаемого объема в гигабайтах** – включает ограничение 500 ГБ на общий максимальный объем, который могут занимать файлы программы на жестком диске узла. Этот пункт меню доступен, если текущее ограничение объема задано в процентах. При выборе этого пункта вы можете изменить заданное по умолчанию значение в диапазоне 12–100000 ГБ. При этом если во время установки компонентов программы на этом узле определен объем свободного пространства меньше заданного ограничения (включая объем, который занимают имеющиеся файлы программы, оставшиеся от предыдущей установки компонентов программы на этом узле), то установка завершается с ошибкой.

  - **Задать ограничение занимаемого объема в процентах от свободного пространства** – включает ограничение 90% от свободного дискового пространства на общий максимальный объем, который могут занимать файлы программы на жестком диске узла. Этот пункт меню доступен, если текущее ограничение объема задано в гигабайтах. При выборе этого пункта вы можете изменить заданное по умолчанию значение в диапазоне 1–100%. Во время установки компонентов программы на этом узле будет определен объем свободного пространства на жестком диске, после чего программа выполнит перерасчет заданного значения в гигабайты и сохранит полученный результат в качестве действующего ограничения. При этом если во время установки компонентов программы на этом узле определен объем свободного пространства меньше 12 ГБ (включая объем, который занимают имеющиеся файлы программы, оставшиеся от

предыдущей установки компонентов программы на этом узле), то установка завершается с ошибкой.

- **Изменить заданное ограничение занимаемого объема** – изменяет текущее ограничение максимального объема, который могут занимать файлы программы на жестком диске узла. Диапазон для изменения значений зависит от того, в каких единицах измерения задано текущее ограничение объема (в процентах или в гигабайтах). Особенности определения объема свободного пространства на жестком диске в зависимости от единиц измерения см. в описаниях пунктов меню **Задать ограничение занимаемого объема в гигабайтах** и **Задать ограничение занимаемого объема в процентах от свободного пространства**.

- **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**.

- **Изменить IP-адрес или имя компьютера с Kaspersky Security Center** – изменяет IP-адрес / имя компьютера с Kaspersky Security Center (если добавлена функциональность взаимодействия программы с Kaspersky Security Center).

- **Изменить номер SSL-порта компьютера с Kaspersky Security Center** – изменяет SSL-порт для подключения к компьютеру с Kaspersky Security Center (если добавлена функциональность взаимодействия программы с Kaspersky Security Center).

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

- **Изменить параметры подключения к Серверу через API** – изменяет параметры для входящих и исходящих подключений с использованием Kaspersky Industrial CyberSecurity for Networks API. При изменении параметров вы можете указать другое имя компьютера, на котором запущен gRPC-сервер. Это имя должно совпадать с именем компьютера, выполняющего функции Сервера. Также вы можете создать новые сертификаты для подключения к Kaspersky Industrial CyberSecurity for Networks через API (если изменилось имя компьютера или если требуется обновить текущие сертификаты по другим причинам).

- **Изменить IP-адрес или имя компьютера с Веб-сервером** – изменяет IP-адрес / имя компьютера Сервера для подключения через веб-интерфейс.

- **Изменить номер порта Веб-сервера** – изменяет номер порта для подключения через веб-интерфейс. Если указан номер порта по умолчанию (443), при подключении через веб-браузер пользователю будет достаточно ввести только IP-адрес / имя компьютера. В этом случае протокол HTTPS и номер порта определяются автоматически.

- **Изменить имя пользователя программы** – изменяет ранее заданное имя пользователя для подключения к Серверу и работы с программой. 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. Указанное имя пользователя будет использоваться только при подключении к Серверу через веб-интерфейс или в Консоли программы. Для этого пользователя не требуется регистрация в качестве учетной записи операционной системы компьютера Сервера или другого компьютера. При изменении имени существующего пользователя программы старая учетная запись не удаляется и создается новая учетная запись. Ввод нового пароля для пользователя запрашивается в процессе переустановки программы (если не найдена другая учетная запись пользователя программы с таким же именем).

- **Изменить параметры сертификатов Веб-сервера** – изменяет параметры использования сертификатов для защиты подключения через веб-интерфейс. Изменение параметров использования сертификатов выполняется аналогично пункту **Использовать самоподписанные сертификаты для соединения с Веб-сервером** в меню **Добавить Сервер**.

- **Добавить пользователя операционной системы для запуска Консоли** – добавляет пользователя операционной системы, которому будет разрешено запускать Консоль Kaspersky Industrial CyberSecurity for Networks. Этот пункт меню аналогичен пункту **Введите имя пользователя операционной системы для запуска Консоли** в меню **Добавить Сервер**.

- **Изменить имя пользователя операционной системы для запуска Консоли** – изменяет имя добавленного пользователя операционной системы, которому разрешено запускать Консоль Kaspersky Industrial CyberSecurity for Networks (например, если изменилось имя учетной записи пользователя в операционной системе).

- **Удалить пользователя операционной системы для запуска Консоли** – отменяет разрешение на запуск Консоли для пользователя операционной системы. Отмена разрешения происходит путем удаления пользователя из группы kics4net при переустановке программы.

- **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 меню установки для управления сенсорами

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 следующих запросов:

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

  - **Введите имя сенсора** – задает имя сенсора в составе решения Kaspersky Industrial CyberSecurity. 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.

- **Изменить параметры сенсора** – изменяет параметры добавленного сенсора. С помощью этого пункта меню вы можете изменить доступные для изменения основные параметры сенсора (например, имя) 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:

  - **Изменить имя сенсора** – изменяет имя сенсора в составе решения Kaspersky Industrial CyberSecurity. Этот пункт меню аналогичен пункту **Введите имя сенсора** в меню **Добавить сенсор**.

- **Указать дополнительного пользователя, от имени которого выполняется установка** – задает дополнительную учетную запись пользователя, от имени которого будет выполняться установка на узле сенсора. Этот пункт меню аналогичен пункту **Указать дополнительного пользователя, от имени которого выполняется установка** в меню **Изменить параметры Сервера**.

- **Включить аппаратный таймер наблюдения** – включает использование аппаратного таймера наблюдения. Этот пункт меню аналогичен пункту **Включить аппаратный таймер наблюдения** в меню **Изменить параметры Сервера**.

- **Выключить автоматический запуск kics4net** – выключает автоматический запуск сервиса kics4net при запуске операционной системы.

- **Задать ограничение занимаемого объема в гигабайтах** – включает ограничение 500 ГБ на общий максимальный объем, который могут занимать файлы программы на жестком диске узла. Этот пункт меню доступен, если текущее ограничение объема задано в процентах. При выборе этого пункта вы можете изменить заданное по умолчанию значение в диапазоне 8–100000 ГБ. При этом если во время установки компонентов программы на этом узле определен объем свободного пространства меньше заданного ограничения (включая объем, который занимают имеющиеся файлы программы, оставшиеся от предыдущей установки компонентов программы на этом узле), то установка завершается с ошибкой.

- **Задать ограничение занимаемого объема в процентах от свободного пространства** – включает ограничение 90% от свободного дискового пространства на общий максимальный объем, который могут занимать файлы программы на жестком диске узла. Этот пункт меню доступен, если текущее ограничение объема задано в гигабайтах. При выборе этого пункта вы можете изменить заданное по умолчанию значение в диапазоне 1–100%. Во время установки компонентов программы на этом узле будет определен объем свободного пространства на жестком диске, после чего программа выполнит перерасчет заданного значения в гигабайты и сохранит полученный результат в качестве действующего ограничения. При этом если во время установки компонентов программы на этом узле определен объем свободного пространства меньше 8 ГБ (включая объем, который занимают имеющиеся файлы программы, оставшиеся от предыдущей установки компонентов программы на этом узле), то установка завершается с ошибкой.

- **Изменить заданное ограничение занимаемого объема** – изменяет текущее ограничение максимального объема, который могут занимать файлы программы на жестком диске узла. Диапазон для изменения значений зависит от того, в каких единицах измерения задано текущее ограничение объема (в процентах или в гигабайтах). Особенности определения объема свободного пространства на жестком диске в зависимости от единиц измерения см. в описаниях пунктов меню **Задать ограничение занимаемого объема в гигабайтах** и **Задать ограничение занимаемого объема в процентах от свободного пространства**.

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

Общие команды меню 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 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.

- **Изменить язык интерфейса** – задает язык локализации для компонентов Kaspersky Industrial CyberSecurity for Networks (Консоли, сенсоров и Сервера), а также для данных, которые

предоставляют эти компоненты.

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

Команды выхода из меню установки

Для выхода из меню 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 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 установки программы и не выполнять установку компонентов.

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

Процедура установки программы

Установка компонентов программы выполняется с помощью файлов из комплекта поставки Kaspersky Industrial CyberSecurity for Networks. Перед установкой компонентов требуется выполнить действия для подготовки к установке программы.

Запуск установки компонентов выполняется с помощью скрипта установки программы kics4net-deploy-<номер версии программы>.bundle.sh. Скрипт использует данные, сохраненные в файле параметров установки.

При установке программы по умолчанию выполняется проверка контрольных сумм пакетов в директории с сохраненными файлами из комплекта поставки. Проверка позволяет определить целостность файлов с пакетами для установки программы путем сравнения вычисленных контрольных сумм пакетов с эталонными значениями. Если хотя бы для одного пакета вычисленная контрольная сумма не совпала с эталонным значением, скрипт установки прерывает свою работу.

> Рекомендуется выполнять установку программы с включенной проверкой контрольных сумм пакетов. При необходимости вы можете выключить проверку контрольных сумм пакетов, однако в этом случае не гарантируется правильная установка компонентов программы.

Чтобы установить Kaspersky Industrial CyberSecurity for Networks на компьютеры, выполните следующие действия:

1. На компьютере, с которого будет выполняться установка, перейдите в директорию с сохраненными файлами из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.

2. Введите команду запуска скрипта установки программы:

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

Если по каким-либо причинам требуется выключить проверку контрольных сумм пакетов для установки программы, вы можете ввести команду запуска скрипта с параметром `--skip-checksum-validation`. Этот параметр предназначен только для тестирования и не должен использоваться при нормальной установке программы.

На экране отобразится предложение выбрать язык для меню установки.

3. Выберите язык, который вы хотите использовать в меню установки.

   Выбор используемого языка для меню установки не влияет на язык локализации компонентов Kaspersky Industrial CyberSecurity for Networks. Для изменения языка локализации компонентов используйте пункт меню **Изменить язык интерфейса**.

4. Если при запуске скрипта установки программы не был указан параметр `--skip-checksum-validation`, после выбора языка для меню установки выполняется проверка контрольных сумм пакетов в директории с сохраненными файлами из комплекта поставки. Дождитесь завершения проверки контрольных сумм пакетов.

   Если хотя бы для одного пакета вычисленная контрольная сумма не совпала с эталонным значением, скрипт установки прерывает свою работу. В этом случае замените поврежденные файлы на исходные файлы из комплекта поставки и снова запустите скрипт установки программы.

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

   На экране отобразится главное меню установки.

6. Выполните следующие действия:

   a. С помощью пункта меню **Добавить Сервер** добавьте Сервер Kaspersky Industrial CyberSecurity for Networks. Для Сервера укажите IP-адреса, имя и другие основные параметры в появляющихся запросах.

      Вы можете настроить дополнительные параметры Сервера (например, изменить заданное по умолчанию ограничение занимаемого дискового пространства). Настройка дополнительных параметров выполняется с помощью пункта меню **Изменить параметры Сервера**.

   b. При установке Сервера с сенсорами добавьте узлы сенсоров с помощью пункта меню **Добавить сенсор**. Для сенсоров укажите IP-адреса и имена в появляющихся запросах.

      Вы можете настроить дополнительные параметры сенсоров (например, изменить заданное по умолчанию ограничение занимаемого дискового пространства). Настройка дополнительных параметров выполняется с помощью пункта меню **Изменить параметры сенсора**.

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

   d. С помощью пункта меню **Изменить язык интерфейса** выберите язык локализации компонентов Kaspersky Industrial CyberSecurity for Networks.

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

8. При появлении на экране сообщения о необходимости ознакомиться с условиями Лицензионного соглашения и Политики конфиденциальности нажмите на клавишу **ENTER**.

   На экране отобразится текст Лицензионного соглашения.

9. Внимательно прочитайте Лицензионное соглашение.

   Текст Лицензионного соглашения выводится в программе для текстовых терминалов less. После того, как вы завершили просмотр текста Лицензионного соглашения, на экране отобразится меню для выбора дальнейших действий.

10. Если вы полностью согласны с условиями Лицензионного соглашения, выберите пункт **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.

    > Если вы не согласны с условиями Лицензионного соглашения, то отмените установку программы с помощью пункта **Я отклоняю условия Лицензионного соглашения**.

11. При появлении сообщения о просмотре Политики конфиденциальности нажмите на клавишу **ENTER**.

    На экране отобразится текст Политики конфиденциальности.

12. Внимательно прочитайте Политику конфиденциальности.

    Текст Политики конфиденциальности выводится в программе для текстовых терминалов less. После того, как вы завершили просмотр текста Политики конфиденциальности, на экране отобразится меню для выбора дальнейших действий.

13. Если вы полностью согласны с условиями Политики конфиденциальности, выберите пункт **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**.

    > Если вы не согласны с условиями Политики конфиденциальности, то отмените установку программы с помощью пункта **Я отклоняю условия Политики конфиденциальности**.

    После принятия условий Политики конфиденциальности на экране отобразится приглашение для ввода пароля пользователя, от имени которого выполняется установка.

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

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

15. При появлении запроса для ввода пароля пользователя программы (имя которого было указано при настройке параметров Сервера) введите новый пароль пользователя.

    Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, а также следующие специальные символы: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`.

    Пароль должен удовлетворять следующим требованиям:

    - содержит от 8 до 20 символов;
    - содержит одну или несколько прописных букв;
    - содержит одну или несколько строчных букв;
    - содержит одну или несколько цифр.

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

После завершения установки Kaspersky Industrial CyberSecurity for Networks не выполняет функции по контролю промышленной сети (на сетевые интерфейсы узлов с установленными компонентами программы не добавлены точки мониторинга). Чтобы использовать программу, вам нужно выполнить действия для подготовки программы к работе.

Просмотр Лицензионного соглашения и Политики конфиденциальности

Вы можете ознакомиться с условиями Лицензионного соглашения и Политики конфиденциальности следующими способами:

- Во время установки Kaspersky Industrial CyberSecurity for Networks.
- Прочитав документы license_ru.txt и privacy_policy_ru.txt. Эти документы включены в комплект поставки программы, а также сохраняются в директории установки программы.

Во время установки Kaspersky Industrial CyberSecurity for Networks тексты Лицензионного соглашения и Политики конфиденциальности выводятся с помощью программы для текстовых терминалов less. Эта программа предоставляет возможности прокрутки текста, поиска, копирования и других действий с текстом за исключением функций редактирования.

При просмотре Лицензионного соглашения или Политики конфиденциальности в нижней части экрана отображается информационная строка, в которой содержатся следующие сведения:

- название документа;
- порядковый номер верхней отображаемой строки;
- основные клавиши для навигации по тексту (клавиши управления курсором);
- клавиша для вызова справки о командах программы (**H**);
- клавиша для выхода из программы (**Q**).

После загрузки Лицензионного соглашения или Политики конфиденциальности программа установки ожидает завершения просмотра текста в программе less. Завершение просмотра текста в программе less происходит в следующих случаях:

- при попытке прокрутки текста далее последней строки;
- при нажатии клавиши для выхода из программы **Q**.

После завершения просмотра текста Лицензионного соглашения или Политики конфиденциальности программа установки выводит меню для выбора дальнейших действий. При необходимости вы можете повторно вывести текст с помощью пункта меню **Прочитать Лицензионное соглашение повторно** или **Прочитать Политику конфиденциальности повторно**.

Изменение параметров и переустановка программы

Переустановка компонентов Kaspersky Industrial CyberSecurity for Networks может потребоваться, например, в следующих случаях:

- для добавления нового сенсора;
- для изменения параметров Сервера или сенсоров;
- для изменения языка локализации программы.

Как и процедура установки, переустановка компонентов Kaspersky Industrial CyberSecurity for Networks выполняется с помощью скрипта установки программы kics4net-deploy-<номер версии программы>.bundle.sh.

Для 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 установки программы выполняет поиск копии файла на этом компьютере и на других компьютерах с установленными компонентами программы.

Чтобы переустановить компоненты Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:

1. Запустите скрипт установки программы, выполнив пункты 1–4 процедуры установки.
2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.

   На экране отобразится главное меню 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 установка 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.
   - С помощью пункта меню **Изменить язык интерфейса** выберите язык локализации компонентов Kaspersky Industrial CyberSecurity for Networks.
4. По окончании настройки параметров выберите пункт **Сохранить параметры и начать установку**.
5. Если предыдущая установка Kaspersky Industrial CyberSecurity for Networks была выполнена другим пользователем, выполните следующие действия:

   a. При появлении на экране сообщения о необходимости ознакомиться с условиями Лицензионного соглашения и Политики конфиденциальности нажмите на клавишу **ENTER**.

На экране отобразится текст Лицензионного соглашения.

b. Внимательно прочитайте Лицензионное соглашение.

Текст Лицензионного соглашения выводится в программе для текстовых терминалов less. После того, как вы завершили просмотр текста Лицензионного соглашения, на экране отобразится меню для выбора дальнейших действий.

c. Если вы полностью согласны с условиями Лицензионного соглашения, выберите пункт **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.

> Если вы не согласны с условиями Лицензионного соглашения, то отмените установку программы с помощью пункта **Я отклоняю условия Лицензионного соглашения**.

d. При появлении сообщения о просмотре Политики конфиденциальности нажмите на клавишу **ENTER**.

На экране отобразится текст Политики конфиденциальности.

e. Внимательно прочитайте Политику конфиденциальности.

Текст Политики конфиденциальности выводится в программе для текстовых терминалов less. После того, как вы завершили просмотр текста Политики конфиденциальности, на экране отобразится меню для выбора дальнейших действий.

f. Если вы полностью согласны с условиями Политики конфиденциальности, выберите пункт **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**.

> Если вы не согласны с условиями Политики конфиденциальности, то отмените установку программы с помощью пункта **Я отклоняю условия Политики конфиденциальности**.

После принятия условий Политики конфиденциальности на экране отобразится приглашение для ввода пароля пользователя, от имени которого выполняется установка.

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

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

7. При появлении запроса для ввода пароля пользователя программы (имя которого было указано при настройке параметров Сервера) введите новый пароль пользователя. Запрос пароля выводится в случае, если указанное имя пользователя не совпадает с именем любого другого пользователя программы.

Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, а также следующие специальные символы: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`.

Пароль должен удовлетворять следующим требованиям:

- содержит от 8 до 20 символов;
- содержит одну или несколько прописных букв;
- содержит одну или несколько строчных букв;

- содержит одну или несколько цифр.

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

Установка программы в неинтерактивном режиме

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

Установка Kaspersky Industrial CyberSecurity for Networks в неинтерактивном режиме подразумевает принятие вами условий Лицензионного соглашения и Политики конфиденциальности. При неинтерактивной установке не выводятся тексты Лицензионного соглашения и Политики конфиденциальности. Вам требуется ознакомиться с условиями Лицензионного соглашения и Политики конфиденциальности, прочитав документы license_ru.txt и privacy_policy_ru.txt, которые включены в комплект поставки программы.

Если вы согласны с условиями Лицензионного соглашения и понимаете и соглашаетесь с тем, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны) согласно Политике конфиденциальности, а также если вы подтверждаете, что полностью прочитали и понимаете условия Политики конфиденциальности, то вы можете выполнить установку программы в неинтерактивном режиме в соответствии с нижеописанными параметрами.

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

Чтобы подготовить файл параметров установки с помощью скрипта установки программы, выполните следующие действия:

1. Настройте параметры установки, выполнив пункты 1–6 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 установки в другую директорию.

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

При установке компонентов программы в неинтерактивном режиме не выполняется проверка контрольных сумм пакетов в директории с сохраненными файлами из комплекта поставки. Вы можете проверить контрольные суммы пакетов, выполнив пункты 1–4 процедуры установки перед запуском установки компонентов в неинтерактивном режиме.

Чтобы установить компоненты программы в неинтерактивном режиме, выполните следующие действия:

1. На компьютере, с которого будет выполняться установка, перейдите в директорию с сохраненными файлами из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.

2. Введите команду:

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

   `--silent-mode --accept-eula --accept-privacy-policy`

   где:

   - `--silent-mode` – параметр включения неинтерактивного режима установки (обязательный параметр);
   - `--accept-eula` – параметр принятия условий Лицензионного соглашения (обязательный параметр);
   - `--accept-privacy-policy` – параметр принятия условий Политики конфиденциальности (обязательный параметр).

   Дополнительно к перечисленным обязательным параметрам вы можете указать следующие параметры запуска скрипта установки:

   - `-i <путь к файлу параметров установки>` – указывает полный путь и имя файла параметров 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.

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

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

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

4. При появлении запроса для ввода пароля пользователя программы (имя которого было указано при настройке параметров Сервера) введите новый пароль пользователя. Запрос пароля выводится в случае, если указанное имя пользователя не совпадает с именем любого другого пользователя программы.

   Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, а также следующие специальные символы: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`.

   Пароль должен удовлетворять следующим требованиям:

   - содержит от 8 до 20 символов;
   - содержит одну или несколько прописных букв;
   - содержит одну или несколько строчных букв;
   - содержит одну или несколько цифр.

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 установки программы kics4net-deploy-<номер версии программы>.bundle.sh.

С помощью скрипта установки программы 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 установки программы выполняет действия по усилению защиты на всех компьютерах, на которых установлены компоненты программы.

Для усиления защиты 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 установки программы выполняет поиск копии файла на этом компьютере и на других компьютерах с установленными компонентами программы.

Чтобы усилить защиту компьютеров с установленными компонентами программы, выполните следующие действия:

1. На компьютере, с которого выполнялась установка, перейдите в директорию с сохраненными файлами из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.
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 `SUDO password` введите пароль учетной записи пользователя, от имени которого выполняется 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.

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

Плагин управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center (далее также "плагин управления") должен быть установлен на том компьютере, где установлен Сервер администрирования Kaspersky Security Center. Установку плагина управления нужно выполнять под учетной записью, которая входит в группу локальных администраторов.

Вы можете установить плагин управления одним из следующих способов:

- с помощью мастера;
- из командной строки.

После установки плагин управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center отображается в списке установленных плагинов управления в свойствах Сервера администрирования Kaspersky Security Center. Подробную информацию о работе с Сервером администрирования Kaspersky Security Center вы можете получить в справочной системе для Kaspersky Security Center.

Чтобы установить плагин управления с помощью мастера, выполните следующие действия:

1. На компьютере, где установлен Сервер администрирования Kaspersky Security Center, запустите файл kics4net-sc-plugin_<номер версии плагина>_<код локализации>.msi из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.

   Для запуска используйте файл с кодом локализации, который соответствует языку локализации Kaspersky Security Center.

2. Следуйте указаниям мастера установки.

Чтобы установить плагин управления из командной строки, выполните следующие действия:

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 из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.

3. В командной строке введите команду:

   `kics4net-sc-plugin_<номер версии плагина>_<код локализации>.msi <параметры запуска msi-файлов>`

   где:

   - `<код локализации>` – код локализации плагина управления. Для запуска используйте файл с кодом локализации, который соответствует языку локализации Kaspersky Security Center.
   - `<параметры запуска msi-файлов>` – один или несколько стандартных параметров запуска, которые предусмотрены для установщика Windows. Вы можете получить сведения о доступных параметрах, выполнив запуск файла с параметром `/help`.

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. Добавление точек мониторинга.
2. Добавление пользователей программы.
3. Добавление лицензионного ключа для обновления.
4. Настройка обновления баз и программных модулей
5. Создание политики безопасности.
6. Настройка контроля процесса.
7. Настройка списка типов событий.
8. Применение политики безопасности.
9. Настройка обнаружения вторжений.
10. Настройка контроля устройств.
11. Настройка контроля сети.

Обновление предыдущей версии программы

Для обновления предыдущей версии Kaspersky Industrial CyberSecurity for Networks требуется сначала полностью удалить программу. После этого вы можете выполнить процедуру установки Kaspersky Industrial CyberSecurity for Networks текущей версии.

После установки Kaspersky Industrial CyberSecurity for Networks текущей версии вы можете импортировать в программу следующие данные, оставшиеся от предыдущей версии:

- Политики безопасности. Для импорта используйте политики безопасности, преобразованные с помощью утилиты преобразования политик безопасности.
- Правила обнаружения вторжений. Для импорта выполните процедуру замены правил.

Формат базы данных текущей версии Kaspersky Industrial CyberSecurity for Networks несовместим с форматом базы данных предыдущей версии программы. Поэтому после обновления будет невозможно загрузить события, зарегистрированные в предыдущей версии программы. Чтобы сохранить и просматривать данные о ранее зарегистрированных событиях, вы можете оставить Сервер предыдущей версии и установить Сервер текущей версии на другом компьютере. В этом случае для просмотра ранее зарегистрированных событий вы сможете подключиться к Серверу предыдущей версии программы.

Удаление программы

Удаление Kaspersky Industrial CyberSecurity for Networks выполняется с помощью скрипта установки программы kics4net-deploy-<номер версии программы>.bundle.sh. Этот скрипт позволяет удалять узлы Сервера и сенсоров по отдельности или полностью удалить программу как текущей версии, так и предыдущих версии (начиная с версии 2.0).

Для удаления 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 установки программы выполняет поиск копии файла на этом компьютере и на других компьютерах с установленными компонентами программы.

Чтобы удалить отдельные узлы, выполняющие функции Сервера или сенсоров, выполните следующие действия:

1. Запустите скрипт установки программы, выполнив пункты 1–4 процедуры установки.
2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.

   На экране отобразится главное меню 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 `SUDO password` введите пароль учетной записи пользователя, от имени которого выполняется удаление.

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

Чтобы полностью удалить программу, выполните следующие действия:

1. Запустите скрипт установки программы, выполнив пункты 1–4 процедуры установки.
2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.

   На экране отобразится главное меню 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 удаления. При выборе этого пункта выводятся следующие запросы:

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

   - **Удалить Агент администрирования**. Если вы хотите удалить компонент Kaspersky Security Center Агент администрирования, ведите 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 `SUDO password` введите пароль пользователя, от имени которого выполняется удаление.

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

При удалении Kaspersky Industrial CyberSecurity for Networks не происходит автоматическое удаление дополнительных файлов из комплекта поставки, которые были скопированы на компьютеры вручную (например, пакет Kaspersky Industrial CyberSecurity for Networks API). При необходимости эти файлы можно удалить вручную.

Запуск и остановка программы

Компоненты программы, установленные на компьютере, запускаются автоматически при загрузке операционной системы компьютера.

Kaspersky Industrial CyberSecurity for Networks получает трафик промышленной сети через точки мониторинга. После установки Kaspersky Industrial CyberSecurity for Networks точки мониторинга отсутствуют на узлах с установленными компонентами программы. Для выполнения функций по контролю промышленной сети вам нужно добавить на узлы точки мониторинга. Если требуется приостановить получение и обработку трафика через точку мониторинга, вы можете выключить ее.

Для управления работой программы и просмотра сведений вы можете подключиться к Серверу через веб-браузер или запустить Консоль программы.

Подключение к Серверу через веб-браузер

Вы можете подключиться к Серверу через веб-интерфейс с помощью любого поддерживаемого веб-браузера. Веб-браузер должен быть установлен на компьютере, который имеет доступ по сети к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks.

Чтобы подключиться к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер, выполните следующие действия:

1. Откройте веб-браузер.

2. Введите в адресной строке:
   `https://<имя Сервера>:<порт>`
   где:

   - `<имя Сервера>` – IP-адрес или имя компьютера Сервера, которое было указано при установке Веб-сервера;
   - `<порт>` – номер порта, который был указан при установке Веб-сервера.

   Если при установке Веб-сервера был 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.

3. На странице ввода учетных данных введите имя и пароль пользователя программы.

4. Нажмите на кнопку **Войти**.

   В окне веб-браузера откроется страница веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

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-браузер

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

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

Чтобы завершить сеанс подключения к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер, выполните следующие действия:

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 **Выход**.

   В окне веб-браузера отобразится страница ввода учетных данных.

Запуск Консоли программы

Вы можете запустить Консоль программы на компьютере, который выполняет функции Сервера.

Для запуска Консоли требуется указать учетные данные пользователя программы.

Чтобы запустить Консоль программы, выполните следующие действия:

1. В меню запуска приложений выберите пункт **Приложения → Система → Kaspersky Industrial CyberSecurity for Networks**.

   На экране отобразится окно для ввода учетных данных.
2. Введите имя и пароль пользователя программы.
3. Нажмите на кнопку **Войти**.

   На экране отобразится окно Консоли программы.

Сеанс подключения к Серверу ограничен по времени. Время действия сеанса составляет 10 часов. Если с момента подключения прошло 10 часов, сеанс работы с Консолью прерывается и на экране появляется окно для ввода учетных данных. В этом случае для продолжения работы вам потребуется снова ввести имя и пароль пользователя программы.

Завершение работы Консоли программы

Вы можете завершить работу Консоли программы в любой момент. Например, для последующего запуска Консоли с вводом имени и пароля другого пользователя программы.

После завершения работы Консоли Сервер Kaspersky Industrial CyberSecurity for Networks продолжает работать.

Чтобы завершить работу Консоли Kaspersky Industrial CyberSecurity for Networks,

закройте окно Консоли.

Интерфейс программы

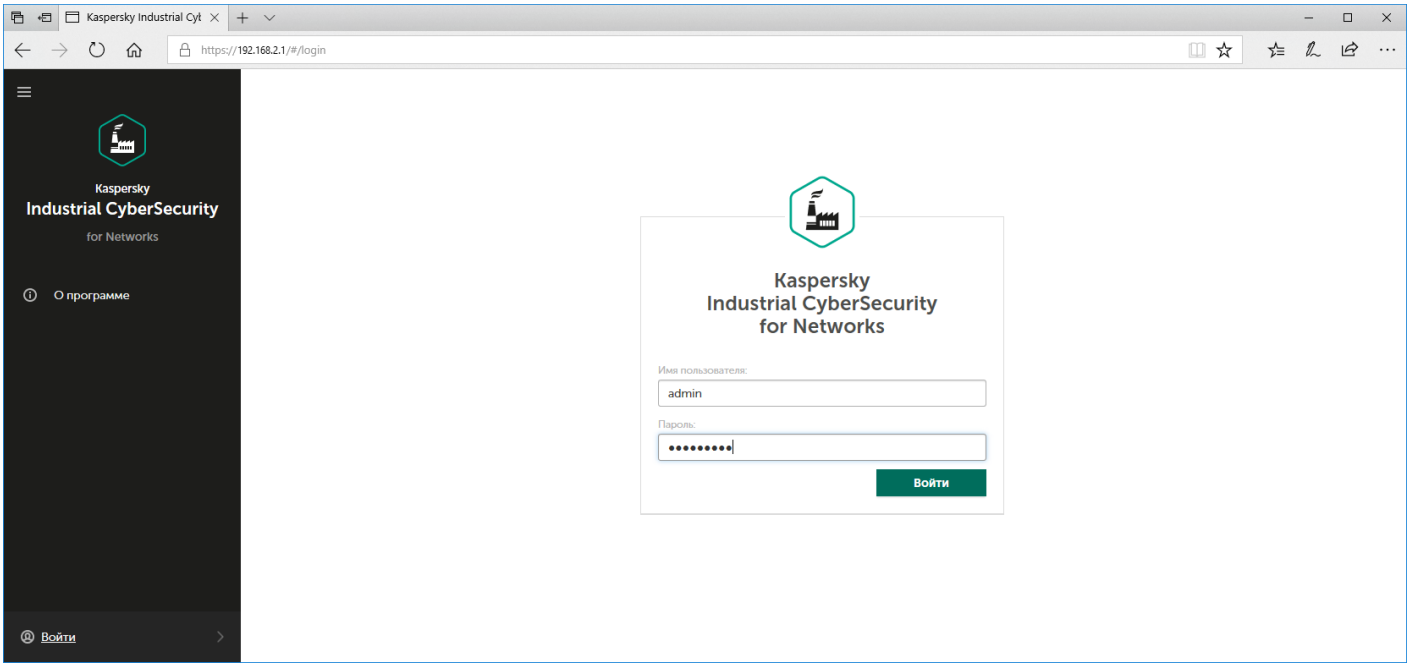
Этот раздел содержит информацию об основных элементах интерфейса программы.

Веб-интерфейс Kaspersky Industrial CyberSecurity for Networks

В этом разделе приведено описание веб-интерфейса программы.

Страница ввода учетных данных для подключения через веб-браузер

Для подключения к Серверу Kaspersky Industrial CyberSecurity for Networks в окне веб-браузера открывается страница ввода учетных данных (см. рис. ниже).



Страница ввода учетных данных в окне веб-браузера

Страница содержит поля ввода имени пользователя и пароля для подключения и кнопку **Войти**.

Меню веб-интерфейса Kaspersky Industrial CyberSecurity for Networks

После подключения к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер открывается страница веб-интерфейса программы.

В левой части страницы отображается меню. Справа отображается содержимое выбранного раздела.

После входа пользователя меню содержит следующие элементы:

- ☰ – разворачивает и сворачивает меню для увеличения свободного пространства на странице. Если меню свернуто, в нем отображаются только изображения элементов.

- – открывает список уведомлений о проблемах в работе программы. При наличии уведомлений рядом отображается значок статуса уведомлений.

- – открывает список фоновых операций. Список содержит информацию о выполнении операций, занимающих длительное время (например, формирование файла при экспорте большого количества событий). При наличии активных фоновых операций рядом отображается количество и статус активных операций (зеленый или красный, если есть операции с ошибками).

- Элементы для перехода к разделам веб-интерфейса:

  - – открывает раздел Мониторинг.

  - – открывает раздел Устройства.

  - – открывает раздел Карта сети.

  - – открывает раздел События.

  - – открывает раздел Теги.

  - – открывает раздел Контроль сети.

  - – 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, рядом отображается сообщение о выключенных функциях защиты. При нажатии на значок или текст открывается окно с информацией о выключенных функциях защиты.

- – 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: русский или английский.

    Выбранный язык локализации веб-интерфейса программы не влияет на язык локализации Сервера Kaspersky Industrial CyberSecurity for Networks и Консоли. Эти компоненты используют 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.

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

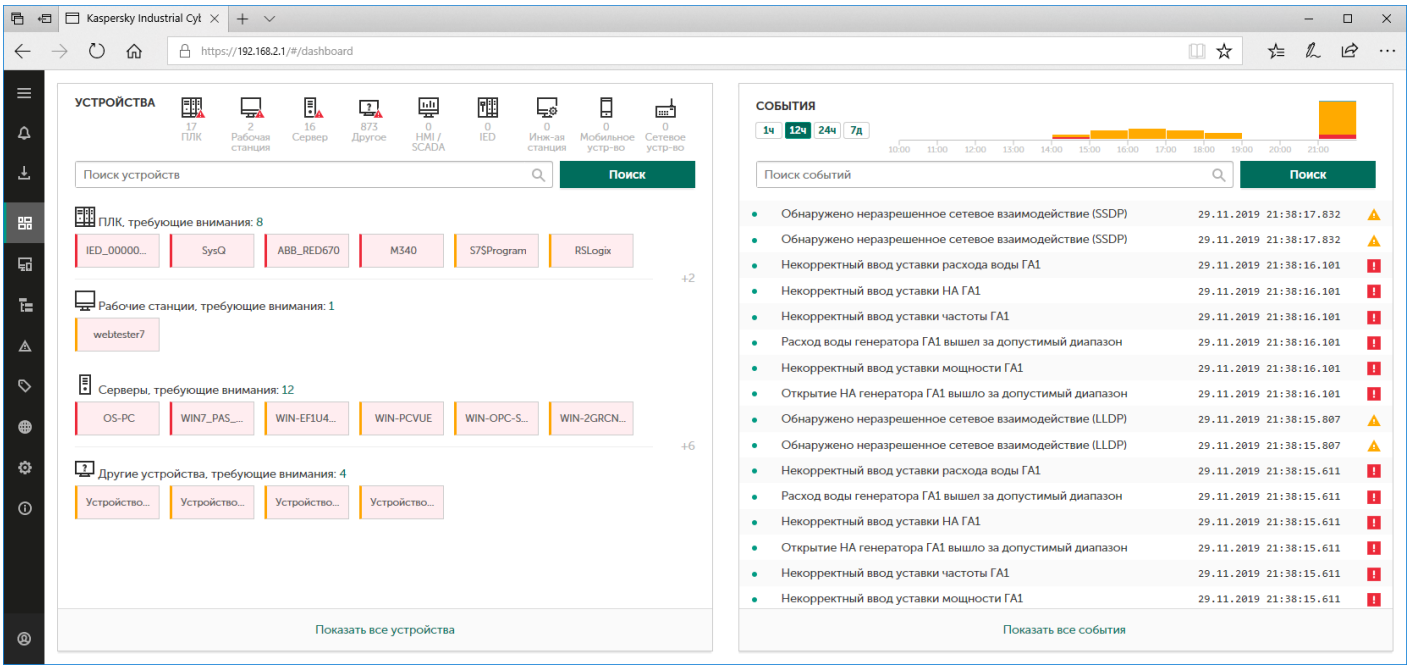
    - **Изменить пароль** – открывает окно для изменения пароля текущего пользователя.

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

    - **Справка** – открывает страницу онлайн-справки для Kaspersky Industrial CyberSecurity for Networks.

Раздел Мониторинг

В разделе **Мониторинг** веб-интерфейса программы (см. рис. ниже) вы можете просматривать в онлайн-режиме сведения о количестве устройств в промышленной сети и о последних зарегистрированных событиях и инцидентах.



Раздел Мониторинг

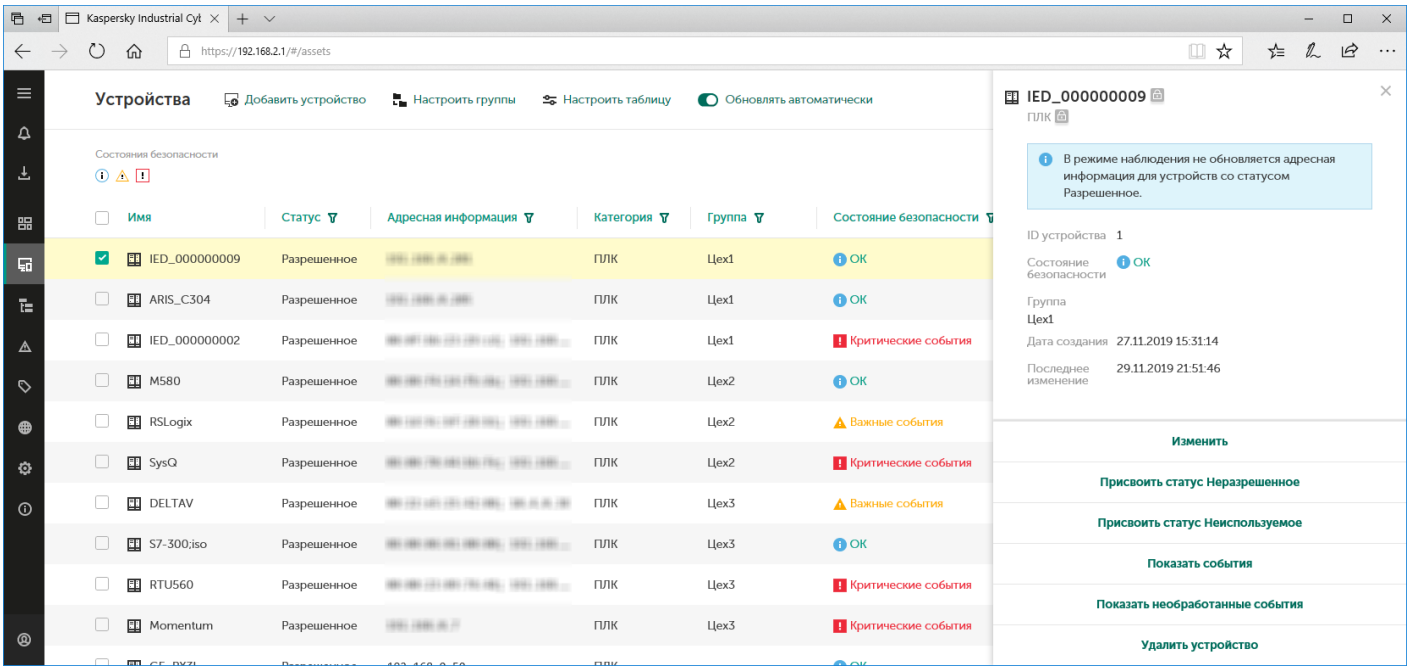
В разделе **Мониторинг** сведения представлены в следующих блоках:

- **Устройства** – содержит информацию об устройствах. Устройства сгруппированы по категориям.
- **События** – содержит информацию о событиях и инцидентах, имеющих наиболее поздние значения даты и времени последнего появления.

Размещение блоков зафиксировано. Размеры блоков автоматически изменяются в зависимости от текущего размера окна веб-браузера.

Раздел Устройства

В разделе **Устройства** веб-интерфейса программы (см. рис. ниже) вы можете просматривать и изменять сведения об устройствах, известных программе.



Раздел Устройства

В верхней части раздела **Устройства** расположена панель инструментов, которая содержит следующие элементы управления таблицей устройств:

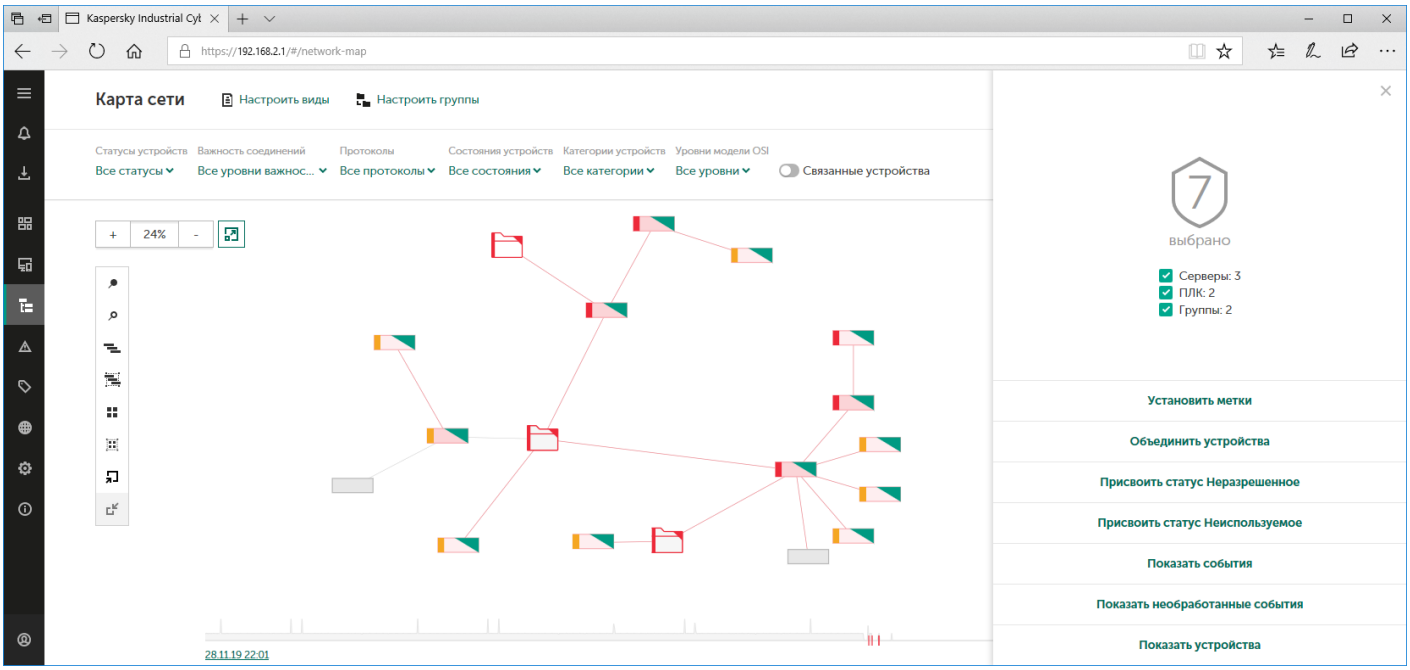
- **Добавить устройство** – добавляет новое устройство в таблицу.
- **Настроить группы** – открывает окно для формирования дерева групп устройств. В окне вы можете добавлять и удалять группы устройств, перемещать их в дереве и переименовывать.
- **Настроить таблицу** – открывает окно для настройки отображения таблицы устройств. В окне вы можете указать отображаемые графы и изменить порядок их отображения.
- **Обновлять автоматически** – включает и выключает автоматическое обновление таблицы устройств.
- Поле ввода для поиска – позволяет ввести запрос для поиска в таблице устройств.
- **Состояния безопасности** – группирует кнопки для выбора варианта фильтрации устройств по состоянию безопасности.
- **Очистить фильтр** – сбрасывает заданные параметры фильтрации и поиска устройств в состояние по умолчанию. Кнопка отображается, если заданы параметры фильтрации или поиска.

В основной части раздела **Устройства** расположена таблица устройств. Таблица содержит графы, указанные при настройке отображаемых граф. Вы можете выполнять сортировку и фильтрацию правил по значениям в графах.

При выборе одного или нескольких устройств в правой части окна веб-интерфейса открывается область деталей. Область содержит сведения о выбранных устройствах и инструменты для работы с ними.

Раздел Карта сети

В разделе **Карта сети** веб-интерфейса программы (см. рис. ниже) вы можете просматривать сведения о взаимодействиях устройств.



Раздел Карта сети

В верхней части раздела **Карта сети** расположена панель инструментов, которая содержит следующие элементы управления:

- **Настроить виды** – открывает окно для сохранения и применения параметров отображения карты сети.
- **Настроить группы** – открывает окно для формирования дерева групп устройств. В окне вы можете добавлять и удалять группы устройств, перемещать их в дереве и переименовывать.
- Поле ввода для поиска – позволяет ввести запрос для поиска узлов на карте сети.
- **Статусы устройств** – позволяет настроить фильтрацию узлов по статусам устройств.
- **Важность соединений** – позволяет настроить фильтрацию соединений по уровням важности связанных с ними событий.
- **Протоколы** – позволяет настроить фильтрацию соединений по протоколам взаимодействий.
- **Состояния устройств** – позволяет настроить фильтрацию узлов по состояниям безопасности устройств.
- **Категории устройств** – позволяет настроить фильтрацию узлов по категориям устройств.
- **Уровни модели OSI** – позволяет настроить фильтрацию соединений по уровням взаимодействий, соответствующих уровням сетевой модели стека сетевых протоколов Open Systems Interconnection (OSI).
- **Связанные устройства** – включает и выключает отображение всех узлов, с которыми были взаимодействия отфильтрованных узлов (независимо от заданных параметров фильтрации).
- **Очистить фильтр** – сбрасывает заданные параметры фильтрации объектов в состояние по умолчанию. Кнопка отображается, если параметры фильтрации заданы.

В области отображения карты сети отображаются узлы, соединения и группы устройств. В левой части области отображения расположены следующие панели инструментов:

- Горизонтальная панель с кнопками + и – для изменения масштаба и кнопкой для автоматического позиционирования карты сети.

- Вертикальная панель со следующими кнопками:

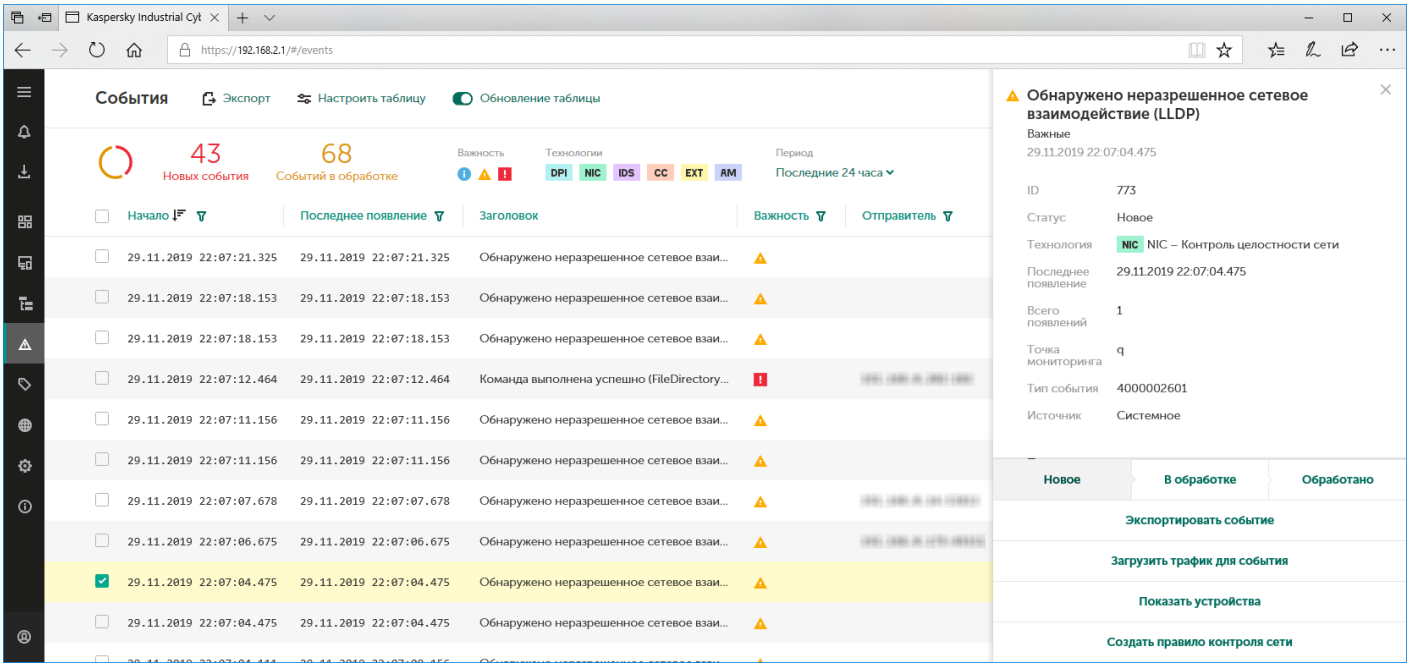
  - – закрепляет все отображаемые узлы и свернутые группы;
  - – открепляет все отображаемые узлы и свернутые группы;
  - – распределяет все узлы и свернутые группы по радиальному принципу;
  - – распределяет выбранные узлы и свернутые группы по радиальному принципу;
  - – выравнивает по сетке все узлы и свернутые группы;
  - – выравнивает по сетке выбранные узлы и свернутые группы;
  - – разворачивает все свернутые группы устройств;
  - – сворачивает все развернутые группы устройств.

При выборе одного или нескольких узлов или свернутых групп, а также при выборе соединения в правой части окна веб-интерфейса открывается область деталей. Область содержит сведения о выбранных объектах и инструменты для работы с ними.

В нижней части раздела **Карта сети** расположена временная шкала, с помощью которой вы можете выбрать период для фильтрации узлов и соединений по времени взаимодействий.

Раздел События

В разделе **События** веб-интерфейса программы (см. рис. ниже) вы можете просматривать и обрабатывать события и инциденты, зарегистрированные программой.



Раздел События

В верхней части раздела **События** расположена панель инструментов, которая содержит следующие элементы управления таблицей:

- **Экспорт** – позволяет экспортировать в файл информацию обо всех событиях и инцидентах с учетом текущих параметров фильтрации и поиска в таблице событий.

- **Настроить таблицу** – открывает окно для настройки отображения таблицы событий. В окне вы можете включить или выключить отображение информационной панели, выбрать режим отображения событий и инцидентов, а также указать отображаемые графы и изменить порядок их отображения.

- **Обновление таблицы** – включает и выключает автоматическое обновление таблицы событий. По умолчанию автоматическое обновление включено. При включенном автоматическом обновлении таблица зарегистрированных событий обновляется в онлайн-режиме. При этом таблица сортируется по графе **Последнее появление** в порядке убывания значений даты и времени возникновения условия для регистрации событий. Если выполнена сортировка по другой графе, таблица событий перестает обновляться.

- Поле ввода для поиска – позволяет ввести запрос для поиска событий и инцидентов в таблице.

- Информационная панель – содержит диаграмму соотношения событий со статусом *Новое* с событиями со статусом *В обработке*. Справа от диаграммы отображается количество событий с этими статусами в базе данных. Вы можете включать и выключать отображение информационной панели в окне для настройки отображения таблицы событий.

- **Важность** – группирует кнопки для включения и выключения фильтрации событий и инцидентов по уровню важности: *Информационные*, *Важные* и *Критические*.

- **Технологии** – группирует кнопки для включения и выключения фильтрации событий по технологиям: *Контроль технологического процесса* (DPI), *Контроль целостности сети* (NIC), *Обнаружение вторжений* (IDS), *Контроль системных команд* (CC), *Внешние системы* (EXT) и *Контроль устройств* (AM).

- **Период** – позволяет выполнить фильтрацию событий и инцидентов по периоду времени. Вы можете выбрать один из четырех стандартных периодов или указать период вручную с помощью варианта **Задать период**. При настройке периода вручную появляются дополнительные поля для выбора даты и времени начала и окончания периода. Если вы указываете период вручную, таблица перестает обновляться.

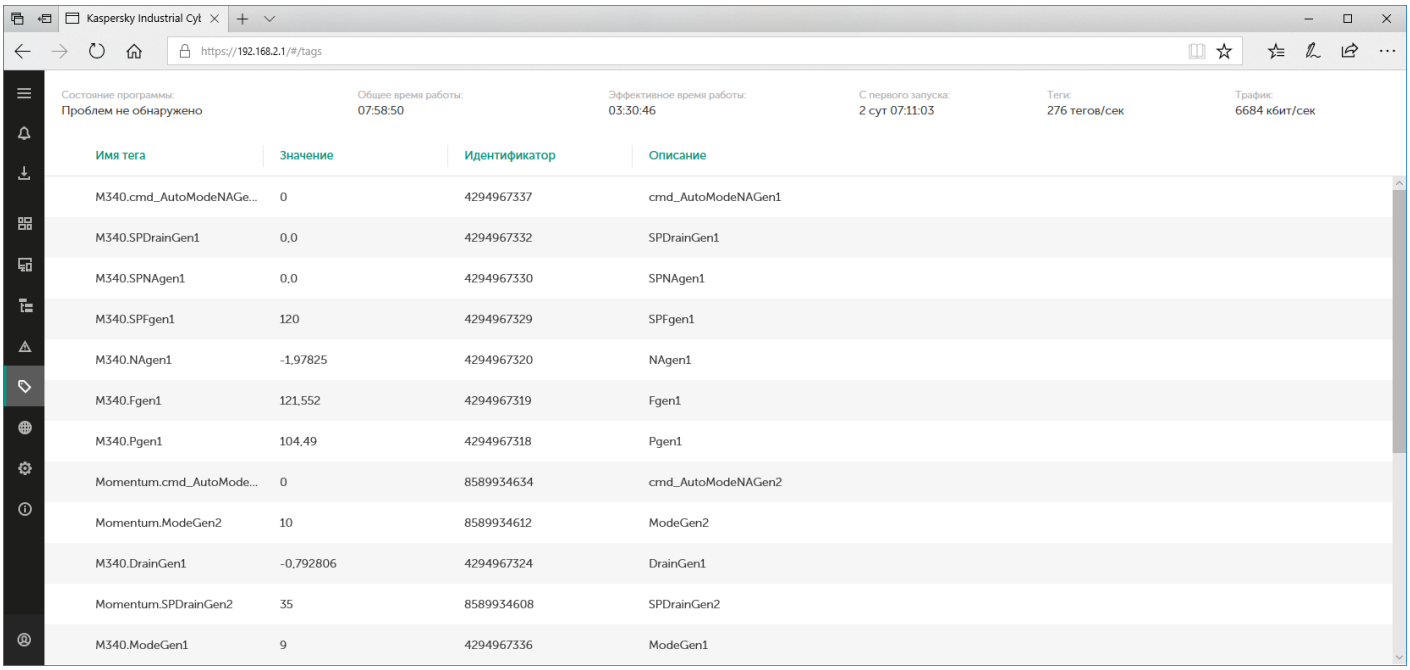
- **Очистить фильтр** – сбрасывает заданные параметры фильтрации и поиска событий в состояние по умолчанию. Кнопка отображается, если заданы параметры фильтрации или поиска.

В основной части раздела **События** расположена таблица, содержащая сведения о зарегистрированных событиях и инцидентах. Сведения представлены в графах, которые указаны для отображения. Вы можете выполнять сортировку и фильтрацию событий и инцидентов по значениям в графах.

При выборе событий или инцидентов в правой части окна веб-интерфейса открывается область деталей. Область содержит сведения о выбранных событиях и инцидентах и инструменты для работы с ними.

Раздел Теги

В разделе **Теги** веб-интерфейса программы (см. рис. ниже) вы можете просматривать теги со значениями параметров технологического процесса, а также контролировать текущее состояние Kaspersky Industrial CyberSecurity for Networks.



Раздел Теги

В верхней части раздела **Теги** отображаются сведения о текущем состоянии Kaspersky Industrial CyberSecurity for Networks:

- **Состояние программы** – текущий статус работы программы. Может отображать следующие сведения о состоянии программы: *Проблем не обнаружено*, *Произошла ошибка*, *Неизвестно*.
- **Общее время работы** – время работы программы от первого запуска Kaspersky Industrial CyberSecurity for Networks до текущего момента. Включает периоды нормальной работы программы (без сбоев) и периоды нарушений в работе программы.
- **Эффективное время работы** – время нормальной работы программы (без сбоев) от последнего запуска Kaspersky Industrial CyberSecurity for Networks до текущего момента.
- **С первого запуска** – время работы программы, прошедшее с первого запуска Kaspersky Industrial CyberSecurity for Networks. Включает периоды нормальной работы программы (без сбоев), периоды нарушений в работе программы и периоды, когда Сервер Kaspersky Industrial CyberSecurity for Networks был выключен.
- **Теги** – скорость обработки тегов (тегов/сек).
- **Трафик** – скорость поступления входящего трафика (кбит/сек).

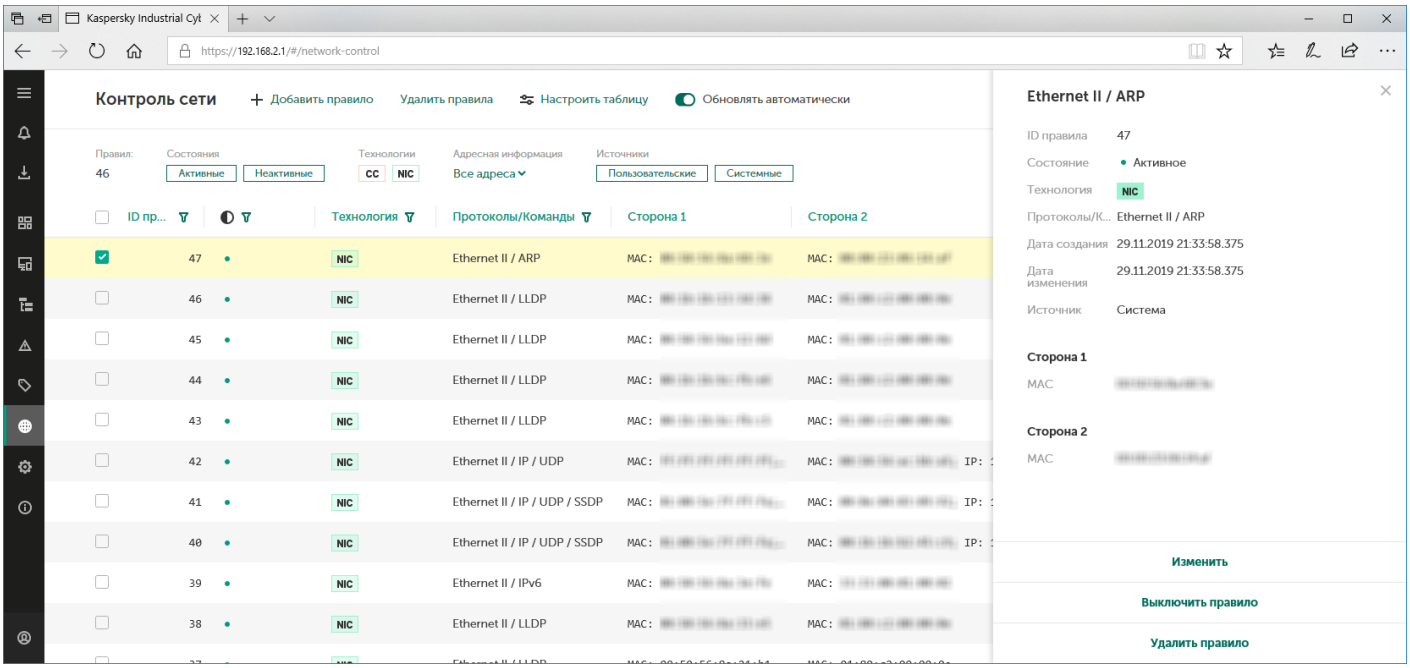
Таблица параметров технологического процесса содержит теги, которые указаны в правилах контроля процесса. В графах таблицы отображается следующая информация о тегах:

- **Имя тега** – название тега, заданное в списке устройств и тегов.
- **Значение** – текущее значение тега.
- **Идентификатор** – числовой идентификатор тега. Присваивается при добавлении тега в список устройств и тегов.
- **Описание** – краткое описание тега, заданное в списке устройств и тегов.

Вы можете выполнять сортировку тегов по значениям в графах, кроме графы **Значение**.

Раздел Контроль сети

В разделе **Контроль сети** веб-интерфейса программы (см. рис. ниже) вы можете управлять правилами контроля сети.



Раздел Контроль сети

В верхней части раздела **Контроль сети** расположена панель инструментов, которая содержит следующие элементы управления таблицей правил контроля сети:

- **Добавить правило** – создает новое правило контроля сети.
- **Настроить таблицу** – открывает окно для настройки отображения таблицы правил контроля сети. В окне вы можете указать отображаемые графы и изменить порядок их отображения.
- **Обновлять автоматически** – включает и выключает автоматическое обновление таблицы правил.
- **Обновить** – появляется в верхней части раздела **Контроль сети**, если выключено автоматическое обновление таблицы правил.
- Поле ввода для поиска – позволяет ввести запрос для поиска в таблице правил.
- **Правил** – отображает общее количество правил контроля сети (включая правила, которые не отображаются в текущий момент).
- **Состояния** – группирует кнопки для фильтрации правил по состоянию.
- **Технологии** – группирует кнопки для фильтрации правил по технологиям: *Контроль системных команд* (CC) и *Контроль целостности сети* (NIC).
- **Адресная информация** – позволяет настроить фильтрацию правил по адресной информации, содержащейся в правилах.
- **Источники** – группирует кнопки для фильтрации правил по источникам.

- **Очистить фильтр** – сбрасывает заданные параметры фильтрации и поиска правил в состояние по умолчанию. Кнопка отображается, если заданы параметры фильтрации или поиска.

В основной части раздела **Контроль сети** расположена таблица правил контроля сети. Таблица содержит графы, указанные при настройке отображаемых граф. Вы можете выполнять сортировку и фильтрацию правил по значениям в графах.

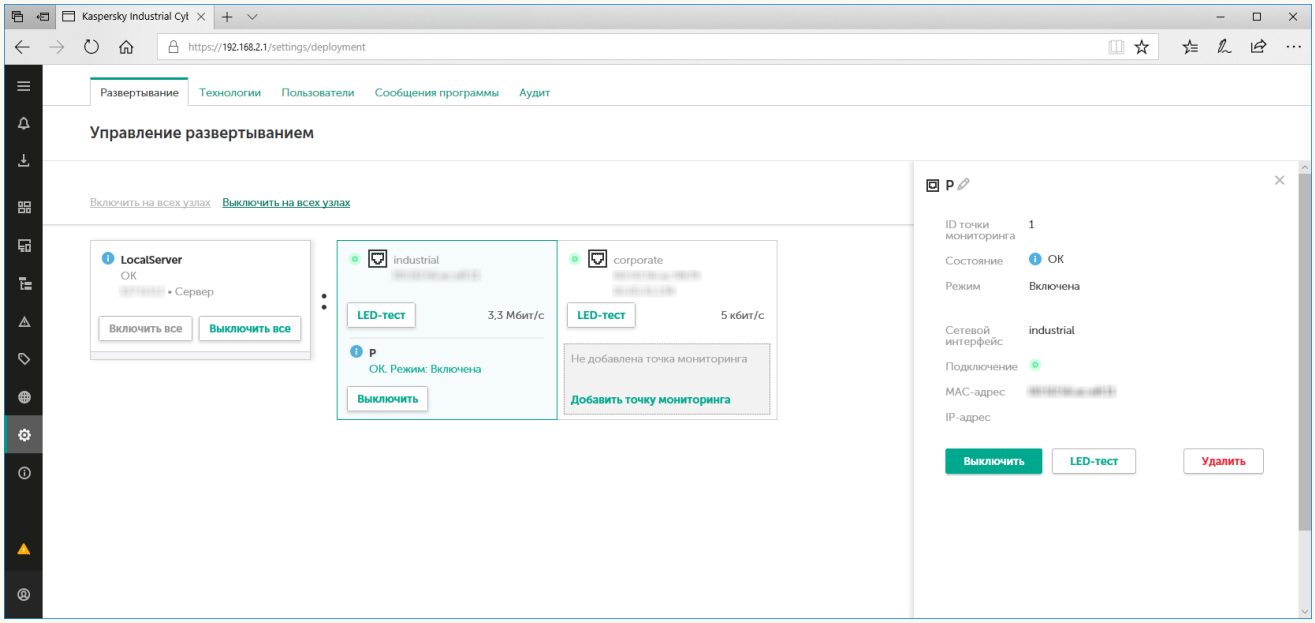
При выборе одного или нескольких правил в правой части окна веб-интерфейса открывается область деталей. Область содержит сведения о выбранных правилах и инструменты для работы с ними.

Раздел Параметры

Раздел **Параметры** веб-интерфейса программы может содержать следующие закладки:

- Развертывание

  На закладке **Развертывание** в разделе **Параметры** (см. рис. ниже) вы можете просматривать сведения об узлах с установленными компонентами программы, о сетевых интерфейсах и точках мониторинга на узлах. Если подключение к Серверу выполнено под учетной записью пользователя с ролью Администратор, на этой закладке также доступно управление точками мониторинга.

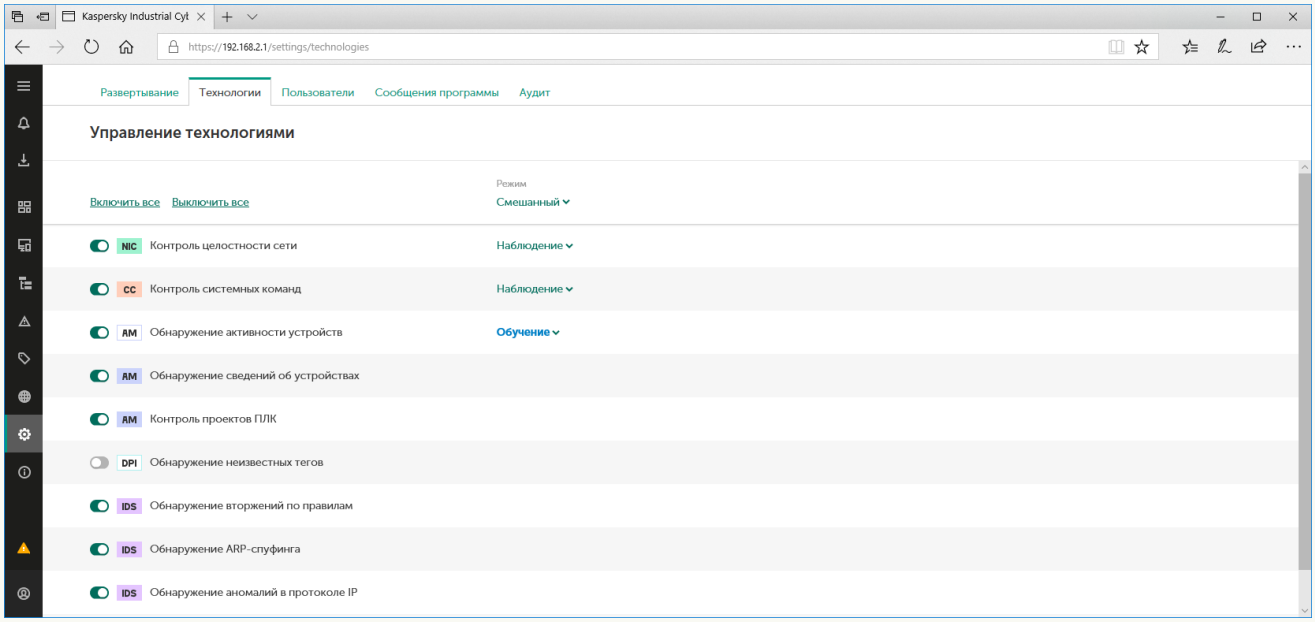
  

  Раздел **Параметры**. Закладка **Развертывание**

  Закладка **Развертывание** содержит карточки узлов с установленными компонентами программы (слева) и карточки сетевых интерфейсов на узлах (справа от каждого узла). При выборе карточки узла или карточки сетевого интерфейса в правой части окна появляется область деталей.

- Технологии

На закладке **Технологии** в разделе **Параметры** (см. рис. ниже) вы можете управлять технологиями и методами для анализа трафика в Kaspersky Industrial CyberSecurity for Networks. Закладка **Технологии** отображается, если подключение к Серверу выполнено под учетной записью пользователя с ролью Администратор.

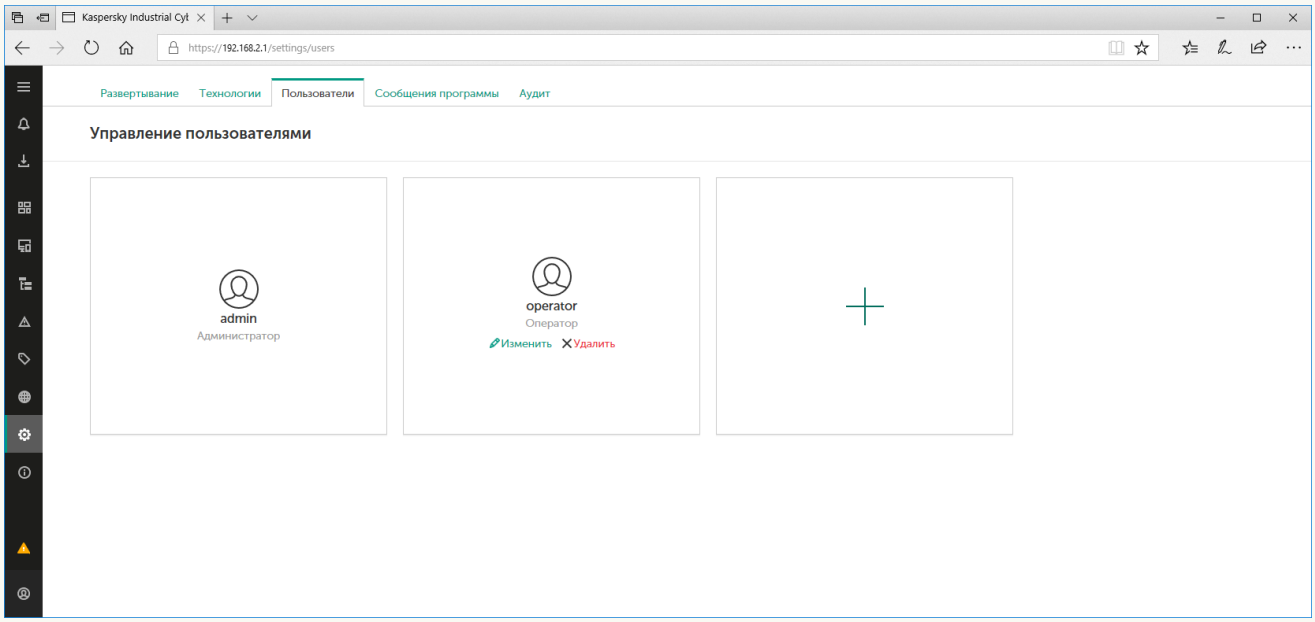


Раздел **Параметры**. Закладка **Технологии**

Закладка **Технологии** содержит список технологий и методов, для которых можно изменять состояния и режимы работы.

- Пользователи

На закладке **Пользователи** в разделе **Параметры** (см. рис. ниже) вы можете управлять учетными записями пользователей программы. Закладка **Пользователи** отображается, если подключение к Серверу выполнено под учетной записью пользователя с ролью Администратор.

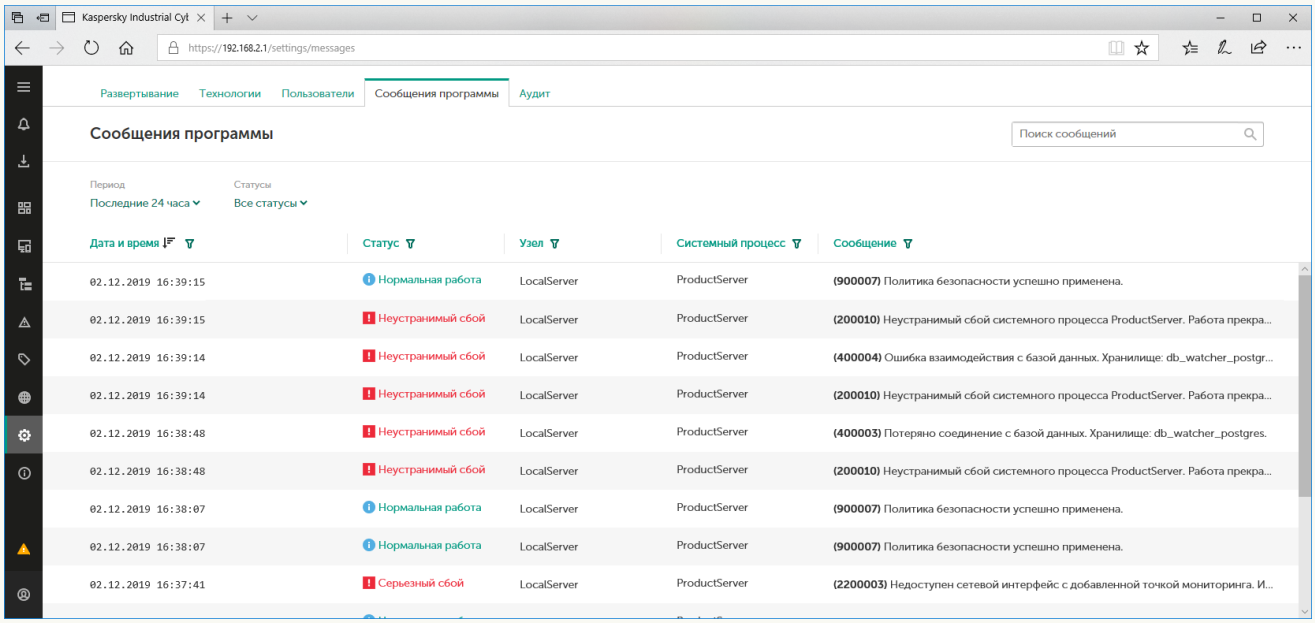


Раздел **Параметры**. Закладка **Пользователи**

Закладка **Пользователи** содержит карточки пользователей программы и карточку со знаком плюс (+) для добавления учетных записей пользователей.

- Сообщения программы

На закладке **Сообщения программы** в разделе **Параметры** (см. рис. ниже) вы можете просматривать сообщения о работе программы.



Раздел **Параметры**. Закладка **Сообщения программы**

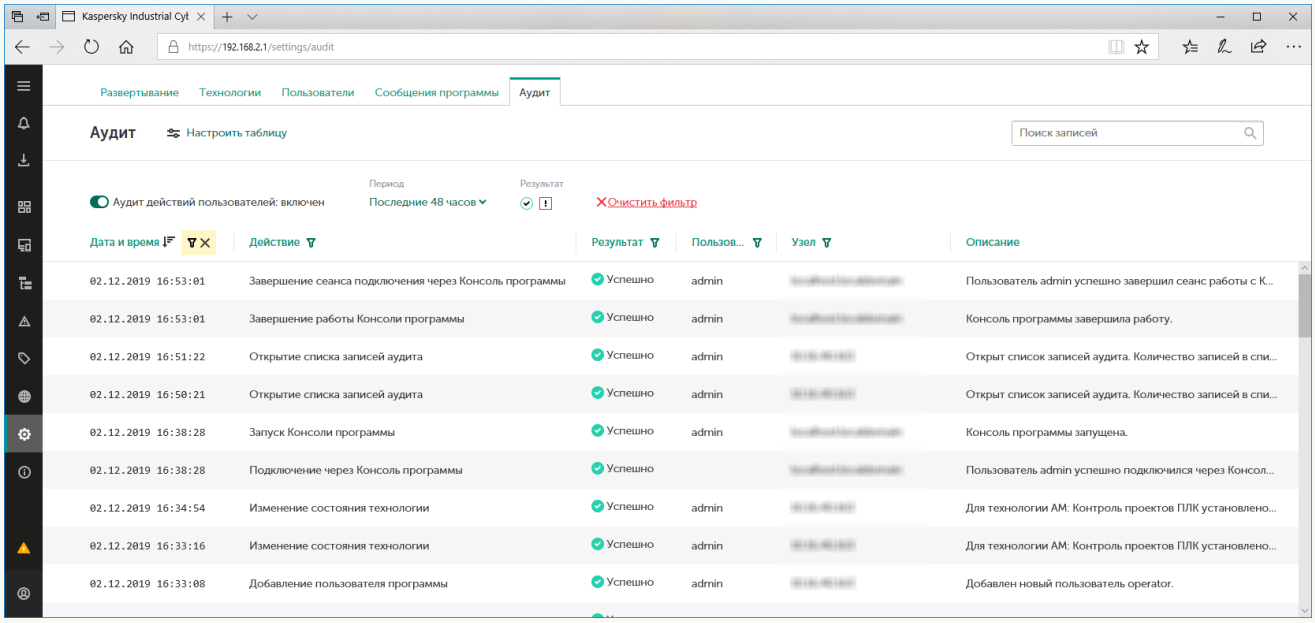
В верхней части закладки **Сообщения программы** расположена панель инструментов, которая содержит следующие элементы управления:

- Поле ввода для поиска – позволяет ввести запрос для поиска сообщений в таблице.
- **Период** – позволяет выполнить фильтрацию сообщений программы по периоду времени. Вы можете выбрать один из четырех стандартных периодов или указать период вручную с помощью варианта **Задать период**. При настройке периода вручную появляются дополнительные поля для выбора даты и времени начала и окончания периода. Если вы указываете период вручную, таблица перестает обновляться.
- **Статусы** – позволяет настроить фильтрацию сообщений по их статусам.
- **Очистить фильтр** – сбрасывает заданные параметры фильтрации и поиска сообщений в состояние по умолчанию. Кнопка отображается, если заданы параметры фильтрации или поиска.

Ниже расположена таблица, содержащая сведения о зарегистрированных сообщениях программы. Вы можете выполнять сортировку и фильтрацию сообщений по значениям в графах таблицы.

- Аудит

На закладке **Аудит** в разделе **Параметры** (см. рис. ниже) вы можете просматривать записи журнала аудита, а также включать и выключать аудит действий пользователей. Закладка **Аудит** отображается, если подключение к Серверу выполнено под учетной записью пользователя с ролью Администратор.



Раздел **Параметры**. Закладка **Аудит**

В верхней части закладки **Аудит** расположена панель инструментов, которая содержит следующие элементы управления:

- **Настроить таблицу** – открывает окно для настройки отображения таблицы записей аудита. В окне вы можете указать отображаемые графы и изменить порядок их отображения.
- Поле ввода для поиска – позволяет ввести запрос для поиска записей в таблице.
- **Аудит действий пользователей: включен / выключен** – включает и выключает аудит действий пользователей.
- **Период** – позволяет выполнить фильтрацию записей аудита по периоду времени. Вы можете выбрать один из четырех стандартных периодов или указать период вручную с помощью варианта **Задать период**. При настройке периода вручную появляются дополнительные поля для выбора даты и времени начала и окончания периода. Если вы указываете период вручную, таблица перестает обновляться.
- **Результат** – группирует кнопки для включения и выключения фильтрации записей аудита по результатам действий: *Успешно* и *Неуспешно*.
- **Очистить фильтр** – сбрасывает заданные параметры фильтрации и поиска записей в состояние по умолчанию. Кнопка отображается, если заданы параметры фильтрации или поиска.

Ниже расположена таблица, содержащая сведения о зарегистрированных записях аудита. Вы можете выполнять сортировку и фильтрацию записей по значениям в графах таблицы.

Состав отображаемых закладок зависит от того, какая роль назначена пользователю, под которым выполнено подключение к Серверу.

Консоль Kaspersky Industrial CyberSecurity for Networks

В этом разделе приведено описание элементов интерфейса Консоли программы.

Элементы интерфейса Консоли Kaspersky Industrial CyberSecurity for Networks

Окно Консоли Kaspersky Industrial CyberSecurity for Networks содержит заголовок, главное меню, область отображения закладок и строку состояния программы.

В заголовке окна Консоли отображается название программы и имя политики безопасности, которая открыта в Консоли. Имя политики безопасности заключено в квадратные скобки. Если изменения в политике безопасности не сохранены, имя политики безопасности отмечено символом *.

Под заголовком окна Консоли отображается главное меню программы, которое содержит следующие пункты:

- **Управление политикой безопасности** – группирует пункты меню для выполнения действий с политиками безопасности Kaspersky Industrial CyberSecurity for Networks:
  - **Создать** – создает новую политику безопасности.
  - **Открыть** – открывает сохраненную политику безопасности из выбранной директории.
  - **Сохранить** – сохраняет изменения текущей политики безопасности (если сохранение выполняется первый раз, открывается окно для выбора директории сохранения).
  - **Сохранить как** – позволяет сохранить политику безопасности в выбранной директории (открывается окно для выбора директории сохранения).
  - **Применить** – применяет текущую политику безопасности на Сервере.
  - **Загрузить с Сервера** – загружает в Консоль политику безопасности, которая применена на Сервере.
  - **Свойства** – открывает окно с информацией о политике безопасности, которая открыта в Консоли, и о политике безопасности, которая применена на Сервере.
  - **Недавние** – содержит пункты, позволяющие быстро открыть одну из политик безопасности, которые открывались в Консоли недавно (каждый пункт меню содержит имя политики безопасности и путь к директории с файлами политики безопасности).
- **Параметры** – группирует пункты меню для открытия окон управления и настройки параметров:
  - **Сервер и сенсоры** – открывает окно для просмотра общих сведений об узлах с установленными компонентами программы и для изменения уровней ведения журналов работы процессов программы.
  - **Журналы** – открывает окно для изменения параметров хранения записей в журналах программы и для изменения параметров сохранения трафика при регистрации событий.
  - **Обновление** – открывает окно для настройки параметров и запуска обновления.
- **Помощь** – группирует следующие пункты меню:
  - **Лицензионный ключ** – открывает окно для просмотра сведений о лицензионном ключе для обновления, а также предоставляет возможности добавления и удаления лицензионного ключа.
  - **О программе** – открывает окно с краткой информацией о программе.

В области отображения закладок расположены следующие закладки:

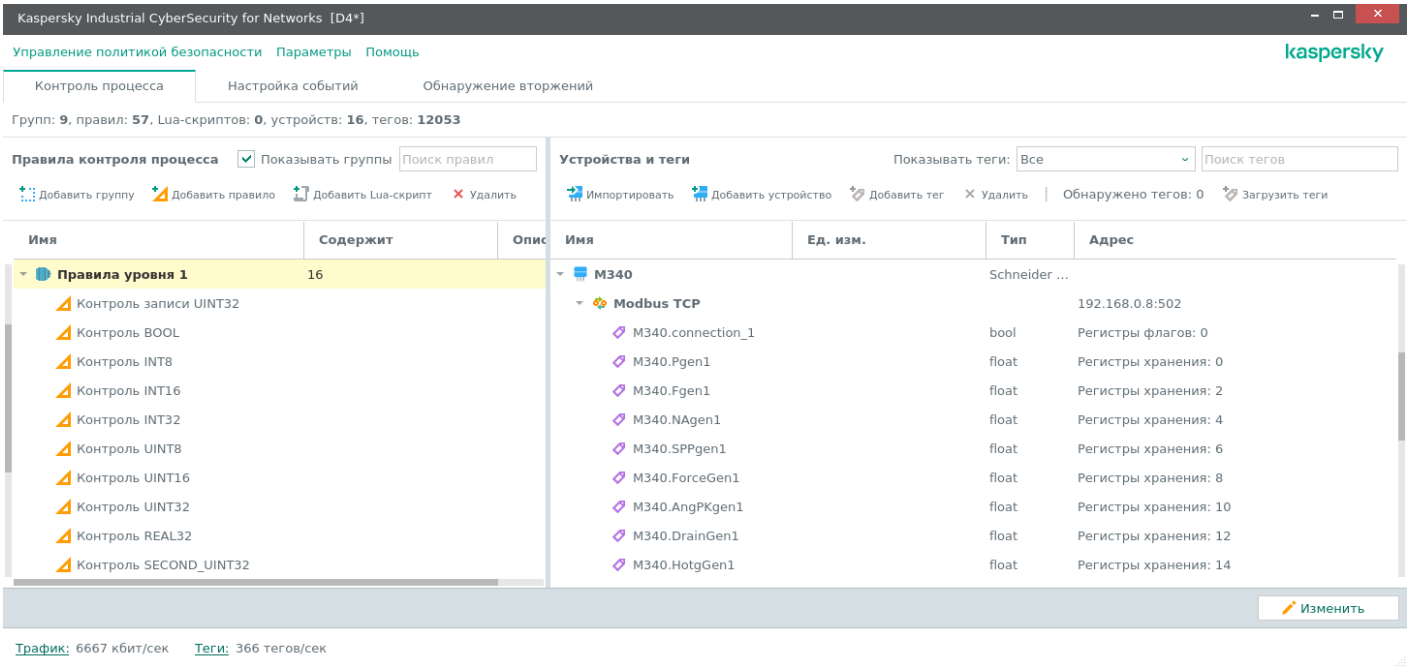
- Контроль процесса.
- Настройка событий.
- Обнаружение вторжений.

В нижней части окна Консоли находится строка состояния Kaspersky Industrial CyberSecurity for Networks. В строке состояния отображается следующая информация:

- **Трафик** – показывает поток трафика в контролируемой сети. Единица измерения – кбит/сек.
- **Теги** – показывает поток тегов. Единица измерения – тегов/сек.
- Информация о состоянии программы при наличии проблем в работе программы.
- Информация о лицензионном ключе при наличии предупреждений о статусе ключа.

Закладка Контроль процесса

В Консоли программы на закладке **Контроль процесса** (см. рис. ниже) вы можете настраивать правила контроля процесса и иерархическую структуру устройств для контроля процесса, отслеживаемых протоколов и тегов.



Закладка Контроль процесса

В верхней части закладки расположена строка с информацией о параметрах контроля процесса. В строке указано количество групп правил, правил, Lua-скриптов, устройств и тегов.

На закладке **Контроль процесса** отображаются две таблицы: слева отображается таблица **Правила контроля процесса**, справа отображается таблица **Устройства и теги**. Над таблицами расположены панели инструментов, которые содержат кнопки для управления списками.

Правила контроля процесса

Таблица правил контроля процесса содержит правила, описывающие условия для регистрации событий в Kaspersky Industrial CyberSecurity for Networks. Вы можете логически объединять правила в группы.

Над таблицей правил контроля процесса расположена панель инструментов, которая содержит следующие элементы управления:

- **Показывать группы** – включает и выключает отображение групп.
- Поле ввода для поиска – позволяет ввести запрос для поиска правил по значениям в отображаемых графах таблицы правил.
- **Добавить группу** – добавляет группу.
- **Добавить правило** – добавляет правило контроля процесса с параметрами условий.
- **Добавить Lua-скрипт** – добавляет правило контроля процесса с Lua-скриптом.
- **Удалить** – удаляет выбранное правило или группу.

Таблица правил контроля процесса содержит следующие графы:

- **Имя** – отображает имя правила или группы.
- **Содержит** – отображает число элементов (групп, правил и Lua-скриптов), входящих в группу.
- **Описание** – отображает краткое описание правила.

Вы можете изменять ширину граф и менять местами графы **Содержит** и **Описание**.

Устройства и теги

Таблица устройств и тегов отображает связь элементов технологического процесса: устройств для контроля процесса, протоколов и тегов. Для представления элементов используется древовидная структура.

Над таблицей устройств и тегов расположена панель инструментов, которая содержит следующие элементы управления:

- **Показывать теги** – позволяет выбрать в раскрывающемся списке вариант отображения тегов:
  - **Все** – в таблице отображаются все теги, созданные в текущей политике безопасности.
  - **В правилах** – в таблице отображаются теги, используемые в каких-либо правилах в текущей политике безопасности.
  - **В текущем правиле** – в таблице отображаются теги, используемые в выбранном правиле контроля процесса.
- Поле ввода для поиска – позволяет ввести запрос для поиска тегов по значениям в отображаемых графах таблицы устройств и тегов, а также по идентификаторам тегов. Для поиска по идентификаторам тегов нужно ввести в строке поиска `id:` и указать искомые идентификаторы через пробел (например, `id: 3 52 675`).
- **Импортировать** – импортирует теги и устройства для контроля процесса из файлов данных.
- **Добавить устройство** – добавляет устройство для контроля процесса.
- **Добавить тег** – добавляет тег для выбранного устройства и протокола.
- **Удалить** – удаляет выбранное устройство или тег.
- **Обнаружено тегов** – отображает количество тегов в хранилище обнаруженных тегов.

- **Загрузить теги** – загружает теги из хранилища обнаруженных тегов.

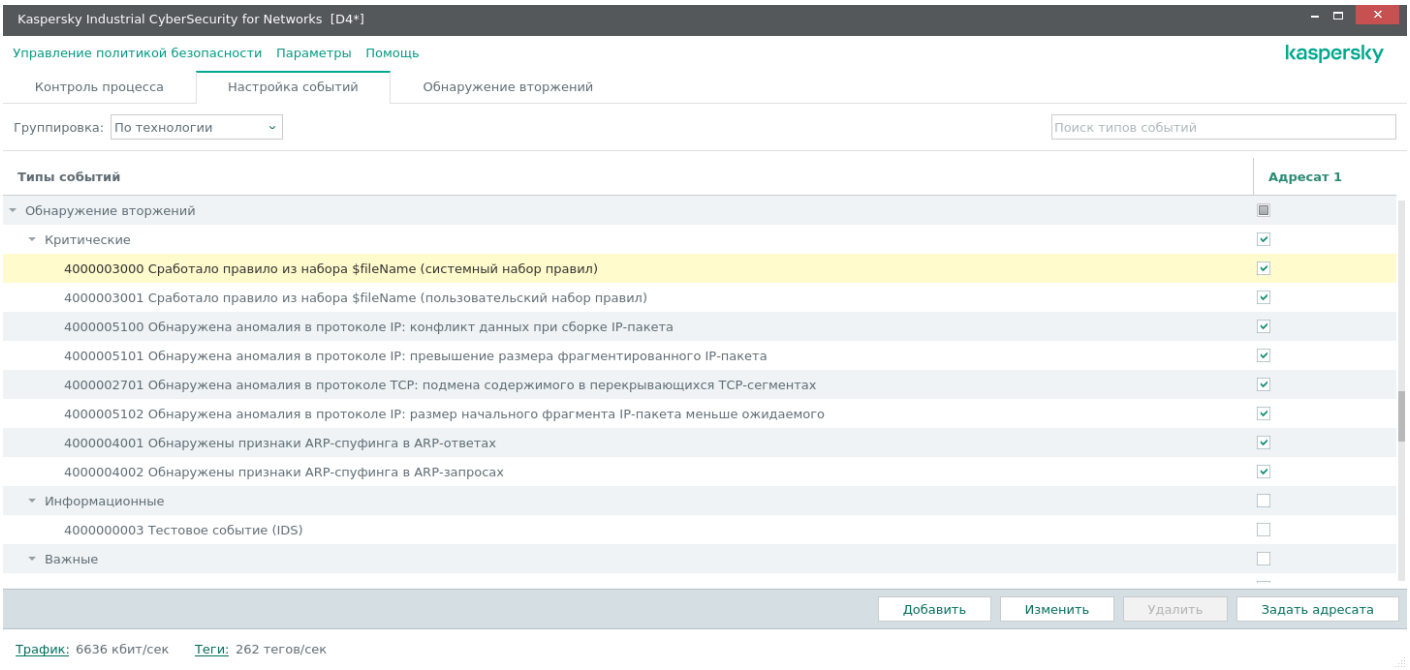
Таблица устройств и тегов содержит следующие графы:

- **Имя** – отображает имя элемента списка.
- **Ед. изм.** – отображает единицу измерения значения тега.
- **Тип** – отображает тип устройства для контроля процесса или тега.
- **Адрес** – отображает адресную информацию. Для протоколов указываются IP-адрес, порт и MAC-адрес устройства для контроля процесса. Для тегов указывается физический адрес тега в памяти устройства.

Вы можете изменять ширину граф и менять местами графы **Ед. изм.**, **Тип** и **Адрес**.

Закладка Настройка событий

На закладке **Настройка событий** (см. рис. ниже) вы можете настраивать типы событий Kaspersky Industrial CyberSecurity for Networks и параметры передачи событий в сторонние системы. *Тип события* – это отображаемый текст события с переменными, не включающий конкретных значений параметров. Значения параметров подставляются Сервером, когда создается событие. События одного типа могут иметь разные значения параметров (например, тегов, протоколов), но одинаковый набор параметров и текст описания события.



Закладка Настройка событий.

Над списком **Типы событий** расположена панель инструментов, которая содержит следующие элементы управления:

- **Группировка** – позволяет выбрать в раскрывающемся списке способ группировки типов событий: **По технологии**, **По важности** или **Нет группировки**.
- Поле ввода для поиска – позволяет ввести запрос для поиска в списке типов событий.

В списке **Типы событий** перечислены номера и заголовки типов событий, которые регистрируются программой.

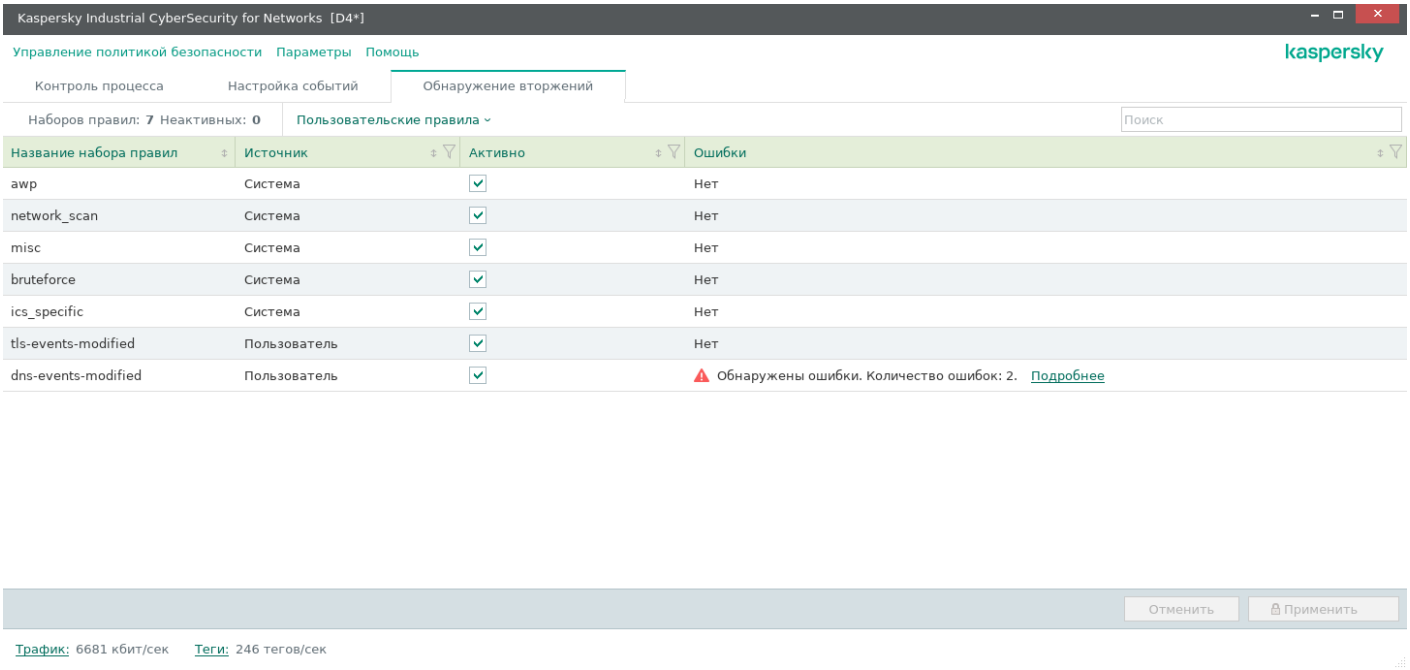
Вы можете настроить передачу событий в сторонние системы (например, в SIEM-систему). Сторонние системы, которые получают события программы, называются *адресатами*. Каждому адресату соответствует отдельная графа в таблице со списком типов событий. В этой графе вы можете установить флажки для включения передачи адресату нужных типов событий.

В нижней части закладки **Настройка событий** расположена строка с кнопками управления списком типов событий:

- **Добавить** – добавляет тип события.
- **Изменить** – изменяет выбранный тип события.
- **Удалить** – удаляет выбранный тип события.
- **Задать адресата** – добавляет адресата.

Закладка Обнаружение вторжений

На закладке **Обнаружение вторжений** (см. рис. ниже) вы можете управлять наборами правил обнаружения вторжений и дополнительными методами обнаружения вторжений.



Закладка Обнаружение вторжений

Над таблицей с наборами правил обнаружения вторжений расположена панель инструментов, которая содержит следующие элементы управления и информационные поля:

- **Наборов правил** – общее количество наборов правил в таблице. Наборы правил включают правила обнаружения вторжений, сгруппированные по некоторым признакам. В программе могут использоваться системные и пользовательские наборы правил.
- **Неактивных** – количество неактивных наборов правил в таблице.

- **Пользовательские правила** – меню для выбора действий с пользовательскими наборами правил. С помощью пунктов меню вы можете загрузить в программу пользовательские наборы правил или удалить все пользовательские наборы правил.

- Поле ввода для поиска – позволяет ввести запрос для поиска по значениям в графе **Название набора правил**.

В основной части закладки расположена таблица с наборами правил обнаружения вторжений. В графах таблицы отображается следующая информация о наборах правил:

- **Название набора правил** – название набора правил обнаружения вторжений. Для пользовательских наборов правил названия совпадают с именами файлов, из которых были загружены наборы правил (без расширения rules).

- **Источник** – значение, определяющее тип набора правил. Возможны два значения: **Система** (для системного набора правил) или **Пользователь** (для пользовательского набора правил).

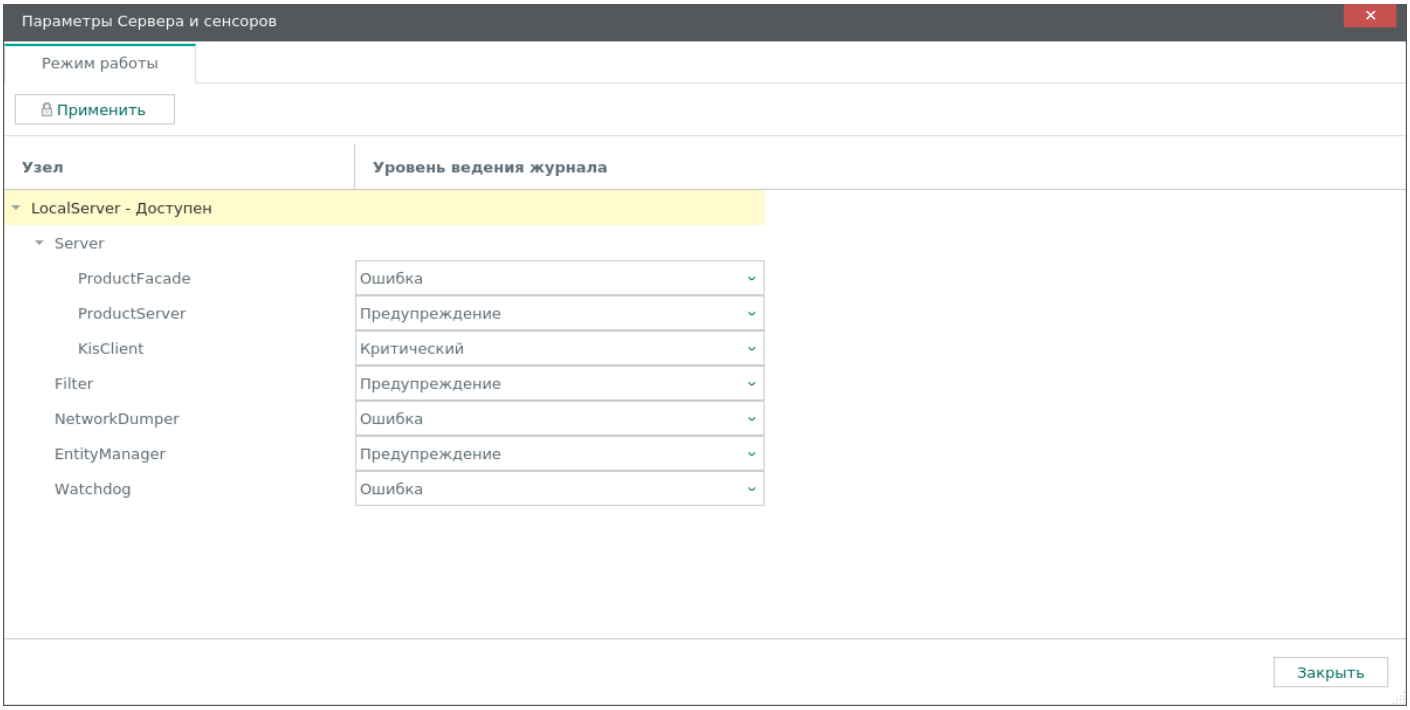
- **Активно** – поле для включения и выключения действия правил. Если флажок установлен, для набора правил включено активное состояние (правила из набора правил применяются при обнаружении вторжений). Если флажок снят, набор правил будет в неактивном состоянии (правила из набора правил не применяются). Состояние наборов правил изменяется после применения изменений.

- **Ошибки** – сведения о наличии ошибок в правилах. Если ошибки не обнаружены, отображается значение **Нет**. При наличии ошибок отображаются сведения о количестве обнаруженных ошибок. Вы можете открыть окно с дополнительными сведениями об ошибках по ссылке **Подробнее** (ссылка появляется при наличии ошибок).

В нижней части закладки **Обнаружение вторжений** расположены кнопки для отмены и применения изменений в состоянии наборов правил (в графе **Активно**).

Окно Параметры Сервера и сенсоров

Окно **Параметры Сервера и сенсоров** (см. рис. ниже) открывается при выборе пункта **Сервер и сенсоры** в меню **Параметры** окна Консоли.



Окно Параметры Сервера и сенсоров

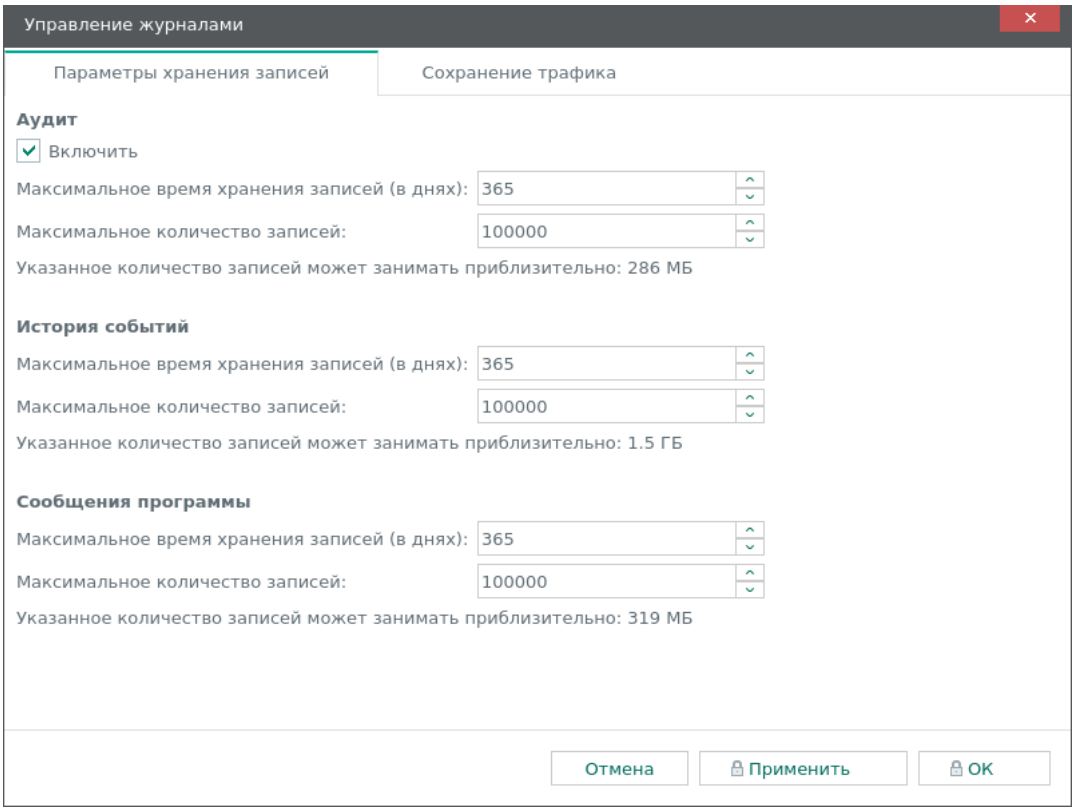
Окно **Параметры Сервера и сенсоров** содержит закладку **Режим работы**. В верхней части закладки расположена кнопка **Применить**, с помощью которой вы можете применить изменения, сделанные для уровней ведения журналов работы процессов.

Ниже расположена таблица с основными сведениями об узлах с установленными компонентами Сервера и сенсоров Kaspersky Industrial CyberSecurity for Networks. В графах таблицы отображается следующая информация:

- **Узел** – имя и текущее состояние узла (*Доступен*, *Недоступен*, *Сбой*, *Состояние неизвестно*). Для каждого узла отображается список процессов, которые обеспечивают функционирование компонентов программы.
- **Уровень ведения журнала** – выбранные уровни ведения журналов работы процессов.

Окно Управление журналами

Окно **Управление журналами** (см. рис. ниже) открывается при выборе пункта **Журналы** в меню **Параметры** окна Консоли.



Окно Управление журналами

Окно **Управление журналами** содержит следующие закладки:

- **Параметры хранения записей** – для изменения параметров хранения журналов в базе данных, а также для включения и выключения аудита действий пользователей.
- **Сохранение трафика** – для изменения параметров сохранения трафика в базе данных программы.

Закладка Параметры хранения записей

Закладка **Параметры хранения записей** содержит блоки параметров **Аудит**, **История событий** и **Сообщения программы**, в которых вы можете управлять параметрами хранения журналов в базе данных. Записи сохраняются в журналах в соответствии со значениями, которые заданы следующими параметрами:

- **Максимальное время хранения записей (в днях)**.
- **Максимальное количество записей**.

С помощью флажка **Включить** в блоке параметров **Аудит** вы можете включать и выключать аудит действий пользователей.

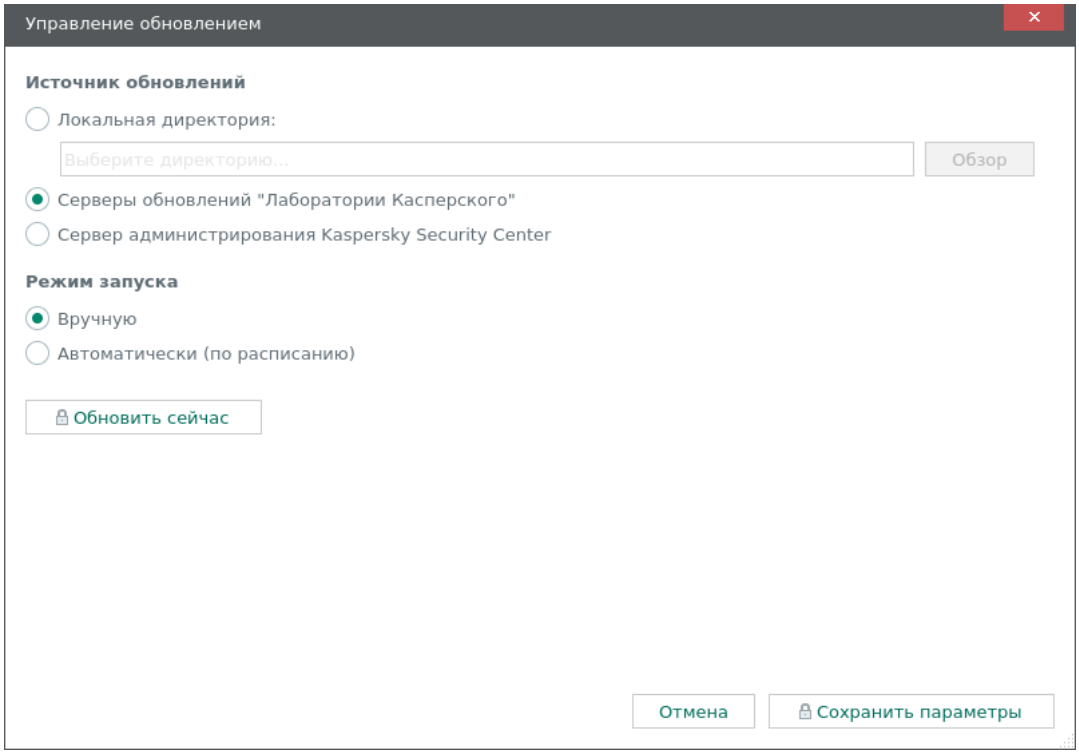
Закладка Сохранение трафика

Закладка **Сохранение трафика** содержит блок параметров **Параметры сохранения трафика**, в котором вы можете управлять параметрами сохранения трафика. Данные о трафике сохраняются в базе данных в соответствии со значениями, которые заданы следующими параметрами:

- **Максимальное количество сохраняемых пакетов**.
- **Максимальное время хранения пакетов (в днях)**.
- **Максимальный объем сохраненного трафика в базе данных (МБ)**.

Окно Управление обновлением

Окно **Управление обновлением** (см. рис. ниже) открывается при выборе пункта **Обновление** в меню **Параметры** окна Консоли. В этом окне вы можете настроить обновление баз и программных модулей.



Окно Управление обновлением

Окно **Управление обновлением** содержит следующие элементы:

- Панель с сообщением о лицензионном ключе для обновления и кнопка **Перейти к добавлению ключа** – отображаются, если лицензионный ключ не добавлен или возникли проблемы с добавленным ключом. С помощью кнопки **Перейти к добавлению ключа** вы можете открыть окно для добавления лицензионного ключа.

- Элементы управления для настройки параметров и запуска обновления (доступны после добавления лицензионного ключа):

  - Блок параметров **Источник обновлений** – для выбора источника обновлений баз и программных модулей. В качестве источника обновлений вы можете указать локальную директорию на компьютере, который выполняет функции Сервера, серверы обновлений "Лаборатории Касперского" или сервер администрирования Kaspersky Security Center.

  - Блок параметров **Режим запуска** – для выбора режима запуска обновления. Вы можете выбрать вариант **Автоматически (по расписанию)** и задать расписание запуска. Также вы можете выбрать вариант **Вручную**, чтобы выключить расписание запуска.

  - Кнопка **Обновить сейчас** – для запуска обновления в текущий момент.

В нижней части окна **Управление обновлением** расположены кнопки для отмены и сохранения изменений в параметрах обновления баз и программных модулей.

Окно Лицензионный ключ для обновления

Окно **Лицензионный ключ для обновления** (см. рис. ниже) открывается при выборе пункта **Лицензионный ключ** в меню **Помощь** окна Консоли. В этом окне вы можете управлять лицензионным ключом для обновления баз и программных модулей.

Окно Лицензионный ключ для обновления

В зависимости от наличия или отсутствия добавленного лицензионного ключа окно **Лицензионный ключ для обновления** может содержать различные сведения и элементы управления.

Если в программу не добавлен лицензионный ключ, окно содержит предупреждение об отсутствии ключа и кнопку **Добавить ключ**.

Если лицензионный ключ добавлен, окно содержит следующие сведения:

- **Ключ** – уникальная буквенно-цифровая последовательность.

- **Действует с** – дата добавления лицензионного ключа в программу.
- **Действует до** – дата окончания срока годности лицензионного ключа с количеством оставшихся дней.
- **Описание** – сведения о доступной функциональности.
- Предупреждение о возникшей проблеме с лицензионным ключом (если есть).

В правой части окна отображается кнопка **Удалить** для удаления лицензионного ключа из программы.

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:

- Во время установки Kaspersky Industrial CyberSecurity for Networks.
- Прочитав документ license_ru.txt. Этот документ включен в комплект поставки программы, а также сохраняется в директории установки программы.

Прочитайте и примите условия Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О 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:

- Во время установки Kaspersky Industrial CyberSecurity for Networks.
- Прочитав документ privacy_policy_ru.txt. Этот документ включен в комплект поставки программы, а также сохраняется в директории установки программы.

Прочитайте и примите условия Политики конфиденциальности во время установки программы. Если вы не согласны с условиями Политики конфиденциальности, вы должны прервать установку 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.

Предусмотрены следующие типы лицензий:

- Base – для использования всей функциональности Сервера и сенсоров, кроме функциональности обновления баз и программных модулей.

  Этот тип лицензии не ограничен по времени и не требует добавления лицензионного ключа в программу.

- Limited Updates – для использования функциональности обновления баз и программных модулей на Сервере и сенсорах.

  Этот тип лицензии ограничен по времени. Для активации функциональности обновления вам нужно добавить в программу лицензионный ключ. По истечении срока действия лицензии этого типа программа продолжает работу, но функциональность обновления становится недоступна. В этом случае, чтобы продолжить использование программы с доступной функциональностью обновления, вам нужно добавить новый лицензионный ключ.

  Информацию о добавленном лицензионном ключе вы можете просмотреть в Консоли программы.

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 для активации функциональности обновления

Лицензионный ключ (далее также "ключ") – последовательность бит, с помощью которой вы можете активировать и затем использовать функциональность обновления баз и программных модулей в соответствии с условиями Лицензионного соглашения. 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 функциональности обновления баз и программных модулей требуется добавить другой лицензионный ключ.

О файле лицензионного ключа для активации функциональности обновления

Файл лицензионного ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл лицензионного ключа предназначен для добавления лицензионного ключа, активирующего функциональность обновления баз и программных модулей.

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 обновления баз и программных модулей с помощью файла лицензионного ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Добавление лицензионного ключа в Консоли программы

Вы можете добавить лицензионный ключ в Kaspersky Industrial CyberSecurity for Networks с помощью Консоли программы или с использованием функциональности автоматического распространения лицензионных ключей в Kaspersky Security Center.

При подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер возможность добавления лицензионного ключа недоступна.

Добавлять лицензионный ключ в Консоли программы могут только пользователи с ролью Администратор.

Чтобы добавить лицензионный ключ в Консоли программы, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Помощь** в окне Консоли выберите пункт **Лицензионный ключ**.

   На экране отобразится окно **Лицензионный ключ для обновления**.
3. Нажмите на кнопку **Добавить ключ**. Кнопка отсутствует, если лицензионный ключ уже был добавлен в программу.

   На экране отобразится окно выбора файла лицензионного ключа.
4. Укажите путь к директории и имя файла лицензионного ключа с расширением key.

5. Нажмите на кнопку открытия файла.

Лицензионный ключ из выбранного файла будет загружен в программу. Информация о добавленном лицензионном ключе отобразится в окне **Лицензионный ключ для обновления**.

Просмотр информации о добавленном лицензионном ключе в Консоли программы

В Консоли Kaspersky Industrial CyberSecurity for Networks вы можете просматривать информацию о добавленном лицензионном ключе. Информация о лицензионном ключе отображается в окне **Лицензионный ключ для обновления**. Дополнительно в строке состояния Консоли могут отображаться предупреждения о статусе лицензионного ключа.

При подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер возможность просмотра информации о добавленном лицензионном ключе недоступна.

Информация о лицензионном ключе в строке состояния

Строка состояния отображается на всех закладках Консоли в нижней части окна Консоли.

При наличии предупреждений о статусе лицензионного ключа в строке состояния отображаются значок предупреждения и текстовое описание.

Цвет значка предупреждения информирует об уровне важности возникшей проблемы. Текстовое описание предупреждения содержит уточняющую информацию. Если описание отображается не полностью, вы можете навести курсор на значок предупреждения для вызова всплывающей подсказки с полным описанием.

Значок предупреждения может быть окрашен в один из следующих цветов:

- Красный.

  Функциональность обновления недоступна (например, из-за истечения срока годности лицензионного ключа).

- Желтый.

  Функциональность обновления активирована, но до истечения срока годности лицензионного ключа остается 14 дней или менее.

Если в строке состояния отображаются значок предупреждения и текстовое описание, вы можете использовать эти элементы для перехода в окно **Лицензионный ключ для обновления**.

*Чтобы перейти в окно **Лицензионный ключ для обновления** с помощью отображаемых элементов в строке состояния,*

нажмите на значок предупреждения о статусе лицензионного ключа или на текстовое описание в строке состояния.

Информация о лицензионном ключе в окне Лицензионный ключ для обновления

Вы можете просмотреть подробные сведения о лицензионном ключе в окне **Лицензионный ключ для обновления**.

*Чтобы открыть окно **Лицензионный ключ для обновления**,*

в меню **Помощь** в окне Консоли выберите пункт **Лицензионный ключ**.

Для добавленного лицензионного ключа в окне **Лицензионный ключ для обновления** отображается следующая информация:

- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Действует с** – дата первого добавления лицензионного ключа в программу.
- **Действует до** – дата окончания срока годности лицензионного ключа с количеством оставшихся дней.
- **Описание** – сведения о доступной функциональности.
- Предупреждение о возникшей проблеме с лицензионным ключом (если есть).

Удаление лицензионного ключа в Консоли программы

В Консоли Kaspersky Industrial CyberSecurity for Networks 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 функциональность обновления баз и программных модулей. Эта функциональность снова активируется при следующем добавлении лицензионного ключа.

При подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер возможность удаления лицензионного ключа недоступна.

Удалять лицензионный ключ могут только пользователи с ролью Администратор.

Чтобы удалить добавленный лицензионный ключ, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Помощь** в окне Консоли выберите пункт **Лицензионный ключ**.

   На экране отобразится окно **Лицензионный ключ для обновления**.
3. Нажмите на кнопку **Удалить**.

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

Лицензионный ключ будет удален из программы.

Обработка и хранение данных в Kaspersky Industrial CyberSecurity for Networks

Этот раздел содержит информацию о предоставлении данных, об используемых журналах и о директориях для хранения данных.

О предоставлении данных

Принимая условия Лицензионного соглашения и Политики конфиденциальности, вы соглашаетесь на обработку в автоматическом режиме информации о персональных данных для обеспечения работы программы. Сведения о получении, обработке и хранении персональных данных вы можете узнать, прочитав тексты Лицензионного соглашения и Политики конфиденциальности.

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 операционной системе компьютера Сервера и добавленных в группу kics4net (пользователи для работы с Консолью программы);
- имена учетных записей пользователей, созданных в программе (пользователи программы);
- IP-адреса или имена компьютеров с установленными компонентами программы;
- IP-адреса, MAC-адреса или имена устройств промышленной сети;
- сведения об устройствах, полученные программой при анализе трафика с помощью правил определения сведений об устройствах и протоколах взаимодействий;
- IP-адрес или имя компьютера с Kaspersky Security Center, а также IP-адреса или имена компьютеров, которые являются серверами сторонних систем для получения событий: Syslog-сервер, SIEM-сервер;
- адреса электронной почты получателей уведомлений о событиях;
- данные в трафике промышленной сети, передаваемые между устройствами и содержащие пользовательские персональные данные (эти данные обрабатываются программой вместе с остальными данными при анализе копии трафика промышленной сети).

Обработка перечисленных данных выполняется с целью анализа нарушений технологического процесса и для обнаружения аномалий сетевого трафика, которые могут являться признаками атак.

Программа сохраняет полученные данные в журналах.

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

Если с помощью скрипта 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 Консоли программы;
  - файлы рабочих данных Сервера и сенсоров;
  - файл параметров установки программы;
  - журнал аудита и журнал сообщений программы.
- Политика безопасности, примененная на Сервере.
- Информация о текущем статусе сервисов, которые обеспечивают работу компонентов программы:
  - kisc4net;
  - kics4net-postgresql;
  - kics4net-webserver;
  - 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 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 программы, который может содержать персональные данные. Также программа не предоставляет доступ к списку пользователей для работы с Консолью программы, поэтому операции чтения этого списка не отслеживаются программой. При этом факты запуска компонентов программы (например, Консоли) и других подключений к Серверу, при которых происходит проверка учетных данных пользователей, отслеживаются программой.

При получении обновлений с серверов "Лаборатории Касперского" программа отправляет следующие данные, необходимые для автоматического выбора нужных обновлений:

- 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.

О журналах

Kaspersky Industrial CyberSecurity for Networks сохраняет данные о своей работе в журналах. В зависимости от типа журнала для размещения данных программа использует базу данных или сохраняет данные в файлах.

Журналы, сохраняемые в базе данных

Программа размещает в базе данных содержимое следующих журналов:

- 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 журнала событий и инцидентов в сторонние системы.

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.

Директории для хранения данных программы

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

Сервер Kaspersky Industrial CyberSecurity for Networks использует для хранения данных следующие директории и их поддиректории:

- Основные директории Сервера:
  - /opt/kaspersky/kics4net/ – директория установки Сервера;
  - /var/opt/kaspersky/kics4net/ – для хранения сертификатов и рабочих данных Kaspersky Industrial CyberSecurity for Networks;
  - /var/log/kaspersky/kics4net/ – для хранения журналов работы процессов, относящихся к Серверу;
  - /etc/opt/kaspersky/kics4net/ – для хранения файлов с паролями к внешним системам.
- Директории СУБД:
  - /opt/kaspersky/kics4net-postgresql/ – директория установки СУБД;
  - /var/opt/kaspersky/kics4net-postgresql/ – для хранения рабочих данных СУБД (конфигурация СУБД, базы данных и другие сведения);
  - /var/log/kaspersky/kics4net-postgresql/ – для хранения журналов работы процессов СУБД;
  - /etc/opt/kaspersky/kics4net-postgresql/ – для хранения дополнительных файлов.
- Директории системы обнаружения вторжений:
  - /opt/kaspersky/kics4net-suricata/ – директория установки системы обнаружения вторжений;
  - /opt/kaspersky/kics4net/share/ids/ – для хранения рабочих данных системы обнаружения вторжений (конфигурация системы обнаружения вторжений, правила и другие сведения);
  - /var/log/kaspersky/kics4net-suricata/ – для хранения журналов работы процессов, относящихся к системе обнаружения вторжений.
- Директории Веб-сервера:
  - /opt/kaspersky/kics4net-webserver/ – директория установки Веб-сервера;
  - /var/opt/kaspersky/kics4net-webserver/ – для хранения рабочих данных Веб-сервера (файлы сертификатов и другие сведения);

- /var/log/kaspersky/kics4net-webserver/ – для хранения журналов работы процессов Веб-сервера (также Веб-сервер сохраняет данные о работе процессов в системном журнале операционной системы).

- Директории с файлами для установки компонентов программы:

  - /home/<user>/.config/kaspersky/kics4net-deploy/ – для хранения журналов работы процессов установки и файла параметров установки (если установка компонентов программы выполнялась с этого компьютера);

  - /var/opt/kaspersky/kics4net-deploy/ – для хранения копии файла параметров установки.

- Директории Консоли программы:

  - /opt/kaspersky/kics4net/ – директория установки Консоли;

  - /home/<user>/.config/kaspersky/kics4net/ – для хранения рабочих данных Консоли (файл конфигурации и другие сведения).

- Директории Агента администрирования:

  - /opt/kaspersky/klnagent64/ – директория установки Агента администрирования;

  - /var/opt/kaspersky/klnagent/ – для хранения рабочих данных Агента администрирования;

  - /var/log/kaspersky/klnagent64/ – для хранения журналов работы процессов Агента администрирования;

  - /etc/opt/kaspersky/klnagent/ – для хранения файлов конфигурации Агента администрирования.

- Стандартные директории операционной системы:

  - /usr/lib/systemd/system/ – для размещения конфигурационных файлов сервисов (например, kics4net.service);

  - /var/run/ – для хранения переменных данных о состоянии системы после загрузки. Компоненты программы могут размещать файлы в самой директории (например, файл klnagent.pid) или в поддиректориях (например, в поддиректории /kics4net/).

Сенсор Kaspersky Industrial CyberSecurity for Networks использует для хранения данных следующие директории и их поддиректории:

- Основные директории сенсора:

  - /opt/kaspersky/kics4net/ – директория установки сенсора;

  - /var/opt/kaspersky/kics4net/ – для хранения сертификатов и рабочих данных Kaspersky Industrial CyberSecurity for Networks;

  - /var/log/kaspersky/kics4net/ – для хранения журналов работы процессов, относящихся к сенсору.

- Директории системы обнаружения вторжений:

  - /opt/kaspersky/kics4net-suricata/ – директория установки системы обнаружения вторжений;

  - /opt/kaspersky/kics4net/share/ids/ – для хранения рабочих данных системы обнаружения вторжений (конфигурация системы обнаружения вторжений, правила и другие сведения);

- /var/log/kaspersky/kics4net-suricata/ – для хранения журналов работы процессов, относящихся к системе обнаружения вторжений.

- Директории с файлами для установки компонентов программы:

  - /home/<user>/.config/kaspersky/kics4net-deploy/ – для хранения журналов работы процессов установки и файла параметров установки (если установка компонентов программы выполнялась с этого компьютера);

  - /var/opt/kaspersky/kics4net-deploy/ – для хранения копии файла параметров установки.

- Стандартные директории операционной системы:

  - /usr/lib/systemd/system/ – для размещения конфигурационных файлов сервисов (например, kics4net.service);

  - /var/run/ – для хранения переменных данных о состоянии системы после загрузки. Компоненты программы могут размещать файлы в самой директории или в поддиректориях.

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

Администрирование Kaspersky Industrial CyberSecurity for Networks

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

Управление точками мониторинга

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).

Вы можете добавлять точки мониторинга как на физические сетевые интерфейсы, так и на логические интерфейсы, объединяющие несколько физических (bond-интерфейсы). При этом невозможно добавить точку мониторинга на физический сетевой интерфейс, который является одним из интерфейсов объединенного логического интерфейса.

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.

Вы можете управлять точками мониторинга и просматривать сведения о точках мониторинга, сетевых интерфейсах и узлах на закладке **Развертывание** в разделе **Параметры** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры**.

3. На закладке **Развертывание** 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 значок ✓ справа от поля ввода.

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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры**.

3. На закладке **Развертывание** 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, используйте ссылку **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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры**.

3. На закладке **Развертывание** 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, используйте ссылку **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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры**.

3. На закладке **Развертывание** выберите карточку сетевого интерфейса с точкой мониторинга, которую вы хотите переименовать.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на значок , который расположен справа от текущего имени точки мониторинга, 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 значок справа от поля ввода.

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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры**.

3. На закладке **Развертывание** 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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры**.

3. На закладке **Развертывание** 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.

Контроль состояния Kaspersky Industrial CyberSecurity for Networks

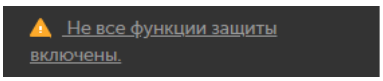
Этот раздел содержит инструкции для контроля состояния программы.

Контроль состояния программы при подключении через веб-интерфейс

Вы можете просматривать информацию о текущем состоянии программы при подключении к Серверу через веб-браузер.

Информация о выключенных функциях защиты

В окне веб-браузера в нижней части меню отображается значок ⚠ и уведомление, если выключены некоторые функции защиты (см. рис. ниже).



Сообщение о выключенных функциях защиты в окне веб-браузера

Значок ⚠ отображается в следующих случаях:

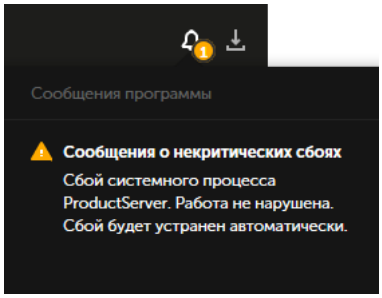
- выключена одна или несколько точек мониторинга;
- выключена одна или несколько функций защиты (например, обнаружение вторжений по правилам);
- включен режим обучения для одной или нескольких функций защиты (например, для технологии Контроль целостности сети).

Чтобы просмотреть информацию о выключенных функциях защиты,

нажмите на значок или текст сообщения о выключенных функциях защиты.

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 веб-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 веб-браузера откроется раздел с информацией, которая относится к уведомлению (например, закладка **Сообщения программы** в разделе **Параметры**).

Информация о текущем состоянии программы

Информацию о текущем состоянии программы вы можете просмотреть в разделе Теги. В поле **Состояние программы** отображается статус наличия или отсутствия проблем в работе программы.

Если программа работает нормально, в поле **Состояние программы** отображается статус *Проблем не обнаружено*.

Если отображается статус *Произошла ошибка* или *Неизвестно*, функции защиты промышленной сети могут выполняться не в полном объеме. Вам нужно принять меры для восстановления нормальной работы 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.

Чтобы просмотреть сообщения программы, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер.
2. Выберите раздел **Параметры** и перейдите на закладку **Сообщения программы**.

   В таблице отобразятся сообщения программы, которые соответствуют заданным параметрам фильтрации и поиска.

Графы таблицы сообщений программы содержат следующую информацию:

- **Дата и время** – дата и время регистрации сообщения программы.
- **Статус** – название статуса сообщения. Для сообщений предусмотрены следующие статусы:
  - *Начало работы*, *Нормальная работа* – для информационных сообщений.
  - *Состояние 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 следующие функции:

- Фильтрация по стандартным периодам

При фильтрации по стандартному периоду таблица сообщений программы обновляется в онлайн-режиме.

Чтобы настроить фильтрацию сообщений программы по стандартному периоду, выполните следующие действия:

1. На закладке **Сообщения программы** в разделе **Параметры** выполните одно из следующих действий:
   - откройте раскрывающийся список **Период** в панели инструментов;
   - нажмите на значок фильтрации в графе **Дата и время**.
2. В раскрывающемся списке выберите один из стандартных периодов:
   - **Последний час**.
   - **Последние 12 часов**.
   - **Последние 24 часа**.
   - **Последние 48 часов**.
3. Если обновление таблицы выключено, в открывшемся окне подтвердите, что вы согласны возобновить обновление таблицы.

В таблице отобразятся сообщения программы за указанный вами период.

- Фильтрация по заданному периоду

При фильтрации по заданному периоду таблица перестает обновляться. В таблице отображаются только те сообщения, которые были зарегистрированы в заданный период.

Чтобы настроить фильтрацию сообщений программы по заданному периоду, выполните следующие действия:

1. На закладке **Сообщения программы** в разделе **Параметры** выполните одно из следующих действий:
   - откройте раскрывающийся список **Период** в панели инструментов;
   - нажмите на значок фильтрации в графе **Дата и время**.
2. В раскрывающемся списке выберите **Задать период**.
3. Если обновление таблицы включено, в открывшемся окне подтвердите, что вы согласны приостановить обновление таблицы.

   Справа от раскрывающегося списка **Период** в панели инструментов появятся дополнительные кнопки, с помощью которых вы можете задать период фильтрации вручную.
4. Нажмите на любую из кнопок со значением даты и времени в полях **От** и **до**.

   Откроется календарь.
5. В поле под календарем слева укажите дату и время начальной границы периода фильтрации. В поле под календарем справа укажите дату и время конечной границы периода фильтрации. Если вы хотите снять ограничение для конечной границы периода, удалите значение в поле под календарем справа.

   Для ввода значения в поле вы можете выбрать дату в календаре (при этом будет указано текущее время) или ввести нужное значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс.
6. Нажмите на кнопку **ОК**.

В таблице отобразятся сообщения программы за указанный вами период.

- Фильтрация по графам таблицы

При фильтрации по графе **Дата и время** вы можете использовать один из стандартных периодов или задать определенный период.

*Чтобы отфильтровать таблицу сообщений программы по графе **Статус** или **Системный процесс**, выполните следующие действия:*

1. На закладке **Сообщения программы** в разделе **Параметры** нажмите на значок фильтрации в нужной графе.

   При фильтрации по статусам вы также можете воспользоваться раскрывающимся списком **Статусы** в панели инструментов.

   Откроется окно фильтрации.

2. Установите флажки напротив значений, по которым вы хотите выполнить фильтрацию.

3. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать таблицу сообщений программы по графе **Узел** или **Сообщение**, выполните следующие действия:*

1. На закладке **Сообщения программы** в разделе **Параметры** нажмите на значок фильтрации в нужной графе.

   Откроется окно фильтрации.

2. В полях **Включая** и **Исключая** введите значения для сообщений программы, которые вы хотите включить в фильтрацию и / или исключить из фильтрации.

3. Если вы хотите применить несколько условий фильтрации, объединенных логическим оператором ИЛИ, в окне фильтрации графы нажмите на кнопку **Добавить условие** и введите условие в открывшемся поле.

4. Если вы хотите удалить одно из созданных условий фильтрации, в окне фильтрации графы нажмите на значок .

5. Нажмите на кнопку **ОК**.

- Поиск сообщений программы

  Чтобы найти нужные сообщения программы,

  на закладке **Сообщения программы** в разделе **Параметры** введите поисковый запрос в поле **Поиск сообщений**. Поиск инициируется во время ввода символов.

  В таблице сообщений программы отобразятся записи, которые удовлетворяют условиям поиска.

  Поиск выполняется по графам **Узел** и **Сообщение**.

- Сброс заданных параметров фильтрации и поиска

  Чтобы сбросить заданные параметры фильтрации и поиска в таблице сообщений программы,

  на закладке **Сообщения программы** в разделе **Параметры** нажмите на кнопку **Очистить фильтр** в панели инструментов (кнопка отображается, если заданы параметры фильтрации и / или поиска).

- Сортировка сообщений программы

  Чтобы отсортировать сообщения программы, выполните следующие действия:

  1. На закладке **Сообщения программы** в разделе **Параметры** нажмите на заголовок графы, по которой вы хотите выполнить сортировку.

  2. Если требуется отсортировать таблицу по нескольким графам, нажмите на клавишу **SHIFT** и, удерживая ее нажатой, нажмите на заголовки граф, по которым нужно выполнить сортировку.

     Таблица будет отсортирована по выбранной графе. При сортировке по нескольким графам строки таблицы сортируются в соответствии с последовательностью выбора граф. Рядом с заголовками граф, по которым выполнена сортировка, отображаются значки, показывающие текущий порядок сортировки: по возрастанию или по убыванию значений.

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.

Просматривать записи аудита могут только пользователи с ролью Администратор.

Чтобы просмотреть записи аудита, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры** и перейдите на закладку **Аудит**.

   В таблице отобразятся записи аудита, которые соответствуют заданным параметрам фильтрации и поиска.

Графы таблицы записей аудита содержат следующую информацию:

- **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** – IP-адрес узла, на котором совершено зарегистрированное действие.
- **Описание** – дополнительные сведения о зарегистрированном действии.

При просмотре таблицы записей аудита вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице записей аудита

  Чтобы настроить список отображаемых в таблице граф, выполните следующие действия:

  1. На закладке **Аудит** в разделе **Параметры** нажмите на кнопку **Настроить таблицу**.

     Откроется окно для настройки отображения таблицы записей аудита.

  2. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр.

  3. Если вы хотите изменить порядок отображения граф, выделите название графы, которую требуется разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

  Выбранные графы отобразятся в указанном вами порядке в таблице записей аудита.

- Фильтрация по стандартным периодам

При фильтрации по стандартному периоду таблица записей аудита обновляется в онлайн-режиме.

Чтобы настроить фильтрацию записей аудита по стандартному периоду, выполните следующие действия:

1. На закладке **Аудит** в разделе **Параметры** выполните одно из следующих действий:
   - откройте раскрывающийся список **Период** в панели инструментов;
   - нажмите на значок фильтрации в графе **Дата и время**.
2. В раскрывающемся списке выберите один из стандартных периодов:
   - **Последний час**.
   - **Последние 12 часов**.
   - **Последние 24 часа**.
   - **Последние 48 часов**.
3. Если обновление таблицы выключено, в открывшемся окне подтвердите, что вы согласны возобновить обновление таблицы.

В таблице отобразятся записи аудита за указанный вами период.

- Фильтрация по заданному периоду

При фильтрации по заданному периоду таблица перестает обновляться. В таблице отображаются только те записи, которые были зарегистрированы в заданный период.

Чтобы настроить фильтрацию записей аудита по заданному периоду, выполните следующие действия:

1. На закладке **Аудит** в разделе **Параметры** выполните одно из следующих действий:
   - откройте раскрывающийся список **Период** в панели инструментов;
   - нажмите на значок фильтрации в графе **Дата и время**.
2. В раскрывающемся списке выберите **Задать период**.
3. Если обновление таблицы включено, в открывшемся окне подтвердите, что вы согласны приостановить обновление таблицы.

   Справа от раскрывающегося списка **Период** в панели инструментов появятся дополнительные кнопки, с помощью которых вы можете задать период фильтрации вручную.
4. Нажмите на любую из кнопок со значением даты и времени в полях **От** и **до**.

   Откроется календарь.
5. В поле под календарем слева укажите дату и время начальной границы периода фильтрации. В поле под календарем справа укажите дату и время конечной границы периода фильтрации. Если вы хотите снять ограничение для конечной границы периода, удалите значение в поле под календарем справа.

   Для ввода значения в поле вы можете выбрать дату в календаре (при этом будет указано текущее время) или ввести нужное значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс.
6. Нажмите на кнопку **ОК**.

В таблице отобразятся записи аудита за указанный вами период.

- Фильтрация по графам таблицы

Вы можете отфильтровать таблицу записей аудита по значениям во всех графах, кроме графы **Описание**.

При фильтрации по графе **Дата и время** вы можете использовать один из стандартных периодов или задать определенный период.

*Чтобы отфильтровать таблицу записей аудита по графе **Действие** или **Результат**, выполните следующие действия:*

1. На закладке **Аудит** в разделе **Параметры** нажмите на значок фильтрации в нужной графе.

   При фильтрации по результатам действий вы также можете воспользоваться соответствующими кнопками в панели инструментов.

   Откроется окно фильтрации.

2. Установите флажки напротив значений, по которым вы хотите выполнить фильтрацию.

3. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать таблицу записей аудита по графе **Пользователь** или **Узел**, выполните следующие действия:*

1. На закладке **Аудит** в разделе **Параметры** нажмите на значок фильтрации в нужной графе.

   Откроется окно фильтрации.

2. В полях **Включая** и **Исключая** введите значения для записей аудита, которые вы хотите включить в фильтрацию и / или исключить из фильтрации.

3. Если вы хотите применить несколько условий фильтрации, объединенных логическим оператором ИЛИ, в окне фильтрации графы нажмите на кнопку **Добавить условие** и введите условие в открывшемся поле.

4. Если вы хотите удалить одно из созданных условий фильтрации, в окне фильтрации графы нажмите на значок .

5. Нажмите на кнопку **ОК**.

- Поиск записей аудита

Чтобы найти нужные записи аудита,

на закладке **Аудит** в разделе **Параметры** введите поисковый запрос в поле **Поиск записей**. Поиск инициируется во время ввода символов.

В таблице записей аудита отобразятся записи, которые удовлетворяют условиям поиска.

Поиск выполняется по всем графам, кроме граф **Дата и время** и **Результат**.

- Сброс заданных параметров фильтрации и поиска

Чтобы сбросить заданные параметры фильтрации и поиска в таблице записей аудита,

на закладке **Аудит** в разделе **Параметры** нажмите на кнопку **Очистить фильтр** в панели инструментов (кнопка отображается, если заданы параметры фильтрации или поиска).

- Сортировка записей аудита

Чтобы отсортировать записи аудита, выполните следующие действия:

1. На закладке **Аудит** в разделе **Параметры** нажмите на заголовок графы, по которой вы хотите выполнить сортировку.

   Вы можете отсортировать таблицу записей аудита по значениям любой графы, кроме графы **Описание**.

2. Если требуется отсортировать таблицу по нескольким графам, нажмите на клавишу **SHIFT** и, удерживая ее нажатой, нажмите на заголовки граф, по которым нужно выполнить сортировку.

Таблица будет отсортирована по выбранной графе. При сортировке по нескольким графам строки таблицы сортируются в соответствии с последовательностью выбора граф. Рядом с заголовками граф, по которым выполнена сортировка, отображаются значки, показывающие текущий порядок сортировки: по возрастанию или по убыванию значений.

Контроль состояния программы в Консоли Kaspersky Industrial CyberSecurity for Networks

В Консоли Kaspersky Industrial CyberSecurity for Networks вы можете просматривать информацию о текущем состоянии программы в строке состояния. Строка состояния отображается в нижней части окна Консоли.

При наличии проблем в работе программы в строке состояния отображаются значок-индикатор проблемы и текстовое описание (см. рис. ниже).

Состояние программы

Цвет значка-индикатора информирует об уровне важности возникшей проблемы. Текстовое описание проблемы содержит уточняющую информацию. Если описание отображается не полностью, вы можете навести курсор на значок-индикатор проблемы для вызова всплывающей подсказки с полным описанием.

Значок-индикатор проблемы может быть окрашен в один из следующих цветов:

- Красный.

  Отсутствует связь между Сервером и Консолью, либо связь установлена, но обнаружены следующие проблемы:

  - на Сервере аварийно завершился один из процессов программы;
  - у программы нет доступа к базе данных.

- Желтый.

  На одном или нескольких узлах обнаружены проблемы, не являющиеся критическими для программы (процессы программы продолжают работу).

- Серый.

  Состояние программы неизвестно, обновляется информация о состоянии программы.

Если проблемы в работе программы отсутствуют, значок-индикатор проблемы в строке состояния не отображается.

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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер.

2. Выберите раздел **Параметры**.

   На закладке **Развертывание** отобразятся карточки узлов (слева) и карточки сетевых интерфейсов, обнаруженных на этих узлах (справа от каждого узла).

3. Если вы хотите просмотреть сведения в развернутом виде (с отображением названий полей), выберите карточку нужного узла или сетевого интерфейса.

В правой части окна веб-интерфейса появится область деталей.

Отображаемые сведения об узлах с установленными компонентами программы

Для узлов отображаются следующие сведения:

- Имя узла, заданное при установке компонентов программы на этом узле.
- Текущее состояние узла в виде значка и текстового описания (в области деталей значок и текстовое описание отображаются в поле **Состояние**). Возможны следующие состояния:
  - *ОК*. 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 *Состояние 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.
- IP-адрес (в области деталей отображается в поле **IP-адрес**).
- Компонент программы, установленный на узле: **Сервер** или **Сенсор** (в области деталей отображается в поле **Тип узла**).

Отображаемые сведения о сетевых интерфейсах

Для сетевых интерфейсов отображаются следующие сведения:

- Значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса (в области деталей отображается в поле **Подключение**). Предусмотрены следующие значки:
  - – сетевой кабель подключен;
  - – сетевой кабель отключен.

  Значок мигает при включенном режиме индикации Ethernet-порта.
- Имя сетевого интерфейса в операционной системе (в области деталей отображается в поле **Сетевой интерфейс**).
- MAC-адрес (в области деталей отображается в поле **MAC-адрес**).
- IP-адрес. Если на сетевом интерфейсе обнаружено несколько IP-адресов, то в карточке сетевого интерфейса отображается только один из них, а в области деталей отображаются не более 16 IP-адресов.
- Скорость поступления входящего трафика на сетевой интерфейс.

Если на сетевой интерфейс добавлена точка мониторинга, дополнительно отображаются следующие сведения:

- Имя точки мониторинга.

- Текущее состояние точки мониторинга в виде значка и текстового описания (в области деталей значок и текстовое описание отображаются в поле **Состояние**). Возможны следующие состояния:
  - *ОК*. Точка мониторинга доступна.
  - *Переключение*. Происходит переключение режима работы точки мониторинга.
  - *Ошибка*. Обнаружена ошибка при переключении режима работы точки мониторинга.
- Текущий режим работы точки мониторинга. В карточке сетевого интерфейса информация о текущем режиме отображается рядом с полем текущего состояния (кроме состояния *Переключение*). В области деталей информация о текущем состоянии отображается в поле **Режим**. Предусмотрены следующие режимы:
  - *Включена*.
  - *Выключена*.

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, выполните следующие действия:

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 (присутствует на компьютере, который выполняет функции Сервера или сенсора);
   - `kics4net-postgresql` – сервис СУБД (присутствует только на компьютере, который выполняет функции Сервера);
   - `kics4net-webserver` – сервис Веб-сервера (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, выполните следующие действия:

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 restart
     sudo service kics4net-webserver restart
     ```

   - Если компьютер выполняет функции сенсора, введите команду:

     ```
     sudo service kics4net 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 сети. 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 устройств. 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 устройств.

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®, выполните следующие действия:

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.

Синхронизация времени Сервера 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 установке Kaspersky Industrial CyberSecurity for Networks вы можете включить синхронизацию времени Сервера с узлами, на которых установлены сенсоры. В этом случае источником времени для узлов с установленными сенсорами будет узел с установленным Сервером.

Для автоматической настройки синхронизации времени Сервера с другими узлами используется протокол Network Time Protocol (NTP). При этом на узлах с установленными сенсорами нельзя настраивать синхронизацию с другими источниками времени и использовать протокол Precision Time Protocol (PTP).

Синхронизацию времени Севера программы 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 NTP и PTP. Пример последовательности действий для настройки синхронизации времени вы можете найти в Базе знаний на веб-сайте "Лаборатории Касперского".

Обновление сертификатов SSL-соединений

Криптографический протокол SSL обеспечивает безопасность передачи данных с использованием сертификатов SSL-соединений. *Сертификат SSL-соединения* (далее "сертификат") – это блок данных, содержащий информацию о владельце сертификата, открытом ключе владельца, датах начала и окончания действия сертификата.

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 к Kaspersky Industrial CyberSecurity for Networks через API.

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, выполните следующие действия:

1. На компьютере, с которого выполнялась установка, перейдите в директорию с сохраненными файлами из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.
2. Введите команду запуска скрипта установки программы с параметром `update-certs`:

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

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

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh. При успешном завершении на экране отобразится сообщение об этом.

Программа начнет использовать обновленные сертификаты на всех узлах с установленными компонентами Kaspersky Industrial CyberSecurity for Networks.

Обновление сертификатов для подключения к Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс

Вы можете обновить сертификаты для подключения к Серверу через веб-интерфейс при переустановке Kaspersky Industrial CyberSecurity for Networks. Для обновления сертификатов в главном меню установки выберите пункт **Изменить параметры Сервера → Изменить параметры сертификатов Веб-сервера** и укажите один из следующих вариантов использования сертификатов:

- Если вы хотите обновить самоподписанные сертификаты, введите символ **y** для запроса **Использовать самоподписанные сертификаты для соединения с Веб-сервером**.
- Если вы хотите обновить доверенные сертификаты, введите символ **y** для запроса **Использовать доверенные сертификаты для соединения с Веб-сервером** и затем введите путь к файлу доверенного сертификата.

Сертификаты будут обновлены после переустановки Kaspersky Industrial CyberSecurity for Networks.

Обновление сертификатов для подключения к Kaspersky Industrial CyberSecurity for Networks через API

Вы можете обновить сертификаты для подключения к Kaspersky Industrial CyberSecurity for Networks через API при переустановке Kaspersky Industrial CyberSecurity for Networks. Для обновления сертификатов в главном меню установки выберите пункт **Изменить параметры Сервера → Изменить параметры подключения к Серверу через API** и введите символ **y** для запроса **Создать новые сертификаты**.

Сертификаты будут обновлены после переустановки Kaspersky Industrial CyberSecurity for Networks.

Обновление баз и программных модулей

В Kaspersky Industrial CyberSecurity for Networks предусмотрена возможность обновления следующих баз и программных модулей:

- системные правила обнаружения вторжений;
- правила получения сведений об устройствах и протоколах взаимодействий;
- правила корреляции событий для регистрации инцидентов;
- модули обработки протоколов прикладного уровня для контроля технологического процесса.

Своевременное обновление баз и программных модулей (далее также "обновление") обеспечивает максимальную защиту промышленной сети с помощью Kaspersky Industrial CyberSecurity for Networks. Рекомендуется обновить базы и программные модули сразу после установки компонентов Kaspersky Industrial CyberSecurity for Networks и затем настроить параметры автоматической установки обновлений.

Вы можете использовать следующие источники обновлений:

- серверы обновлений "Лаборатории Касперского";

- локальная директория на компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks;
- Сервер администрирования Kaspersky Security Center.

Запуск установки обновлений может выполняться автоматически в соответствии с заданным расписанием или вручную.

Для настройки параметров и запуска установки обновлений вручную вы можете использовать Консоль Kaspersky Industrial CyberSecurity for Networks. Просматривать сведения об установленных обновлениях вы можете в Консоли программы (только общие сведения) или при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер (общие сведения, а также дополнительные сведения, сохраняемые в сообщениях программы).

Обновление баз и программных модулей имеет следующие особенности и ограничения:

- Функциональность обновления доступна после добавления лицензионного ключа.
- 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 из локальной директории требуется предоставить группе kics4net доступ к этой директории. Предоставление доступа к директории выполняется с помощью стандартных средств операционной системы.
- Не поддерживается загрузка обновлений из директорий на других компьютерах по протоколам удаленного доступа (FTP, NFS, SMB и другие). Для загрузки обновлений по протоколу удаленного доступа вы можете подключить сетевой ресурс (директорию, которая содержит обновления для загрузки) на компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks. Подключение сетевого ресурса выполняется с помощью стандартных средств монтирования сетевых ресурсов в операционной системе. После подключения сетевого ресурса вы можете выбрать локальную директорию монтирования в качестве источника обновлений.
- 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 указать параметры передачи событий и состояния программы в Kaspersky Security Center 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.

Выбор источника обновлений

После добавления лицензионного ключа вы можете выбрать один из следующих источников обновлений баз и программных модулей:

- серверы обновлений "Лаборатории Касперского";
- локальная директория на компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks;
- Сервер администрирования Kaspersky Security Center.

Выбрать источник обновлений могут только пользователи с ролью Администратор.

Чтобы выбрать источник обновлений, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Параметры** окна Консоли программы выберите пункт **Обновление**.

   Откроется окно **Управление обновлением**.
3. В блоке параметров **Источник обновлений** выберите один из следующих вариантов использования источников обновлений:

   - **Локальная директория** – для загрузки обновлений из указанной локальной директории на компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks.
   - **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. Если выбран вариант **Локальная директория**, укажите путь к директории в локальной файловой системе. Вы можете открыть окно для выбора директории с помощью кнопки **Обзор**.

   > К указанной директории должен быть предоставлен доступ для группы kics4net. При необходимости предоставьте доступ к этой директории с помощью стандартных средств операционной системы.
5. Нажмите на кнопку **Сохранить параметры**.

Выбор режима запуска обновления

После добавления лицензионного ключа вы можете выбрать один из следующих режимов запуска обновления баз и программных модулей:

- вручную;
- автоматически в соответствии с заданным расписанием.

Выбрать режим запуска обновления могут только пользователи с ролью Администратор.

Чтобы выбрать режим запуска обновления, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Параметры** окна Консоли программы выберите пункт **Обновление**.

   Откроется окно **Управление обновлением**.
3. В блоке параметров **Режим запуска** выберите один из следующих вариантов режима запуска обновления:

- **Вручную** – для запуска обновления только вручную.
- **Автоматически (по расписанию)** – для запуска обновления как по расписанию запуска, так и вручную.

4. Если выбран вариант **Автоматически (по расписанию)**, задайте параметры расписания для запуска обновления. Для этого выполните следующие действия:
   a. В раскрывающемся списке 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.
5. Нажмите на кнопку **Сохранить параметры**.

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, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Параметры** окна Консоли программы выберите пункт **Обновление**.
   Откроется окно **Управление обновлением**.
3. Нажмите на кнопку **Обновить сейчас**.

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. Эти сведения выводятся в Консоли программы или при подключении к Серверу через веб-браузер.

Чтобы просмотреть общие сведения об установленных обновлениях в Консоли программы,

в меню **Помощь** окна Консоли программы выберите пункт **О программе**.

Чтобы просмотреть общие сведения об установленных обновлениях при подключении к Серверу через веб-браузер,

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.

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 разграничения доступа пользователей используются учетные записи, созданные в программе. Пользователи могут подключаться к Серверу и работать с программой только под этими учетными записями. Подключения под другими учетными записями, а также анонимные подключения, невозможны.

Для учетных записей, созданных в программе, не требуется регистрация в качестве учетных записей операционной системы компьютера Сервера или другого компьютера.

Первую учетную запись пользователя программы требуется создать при установке Kaspersky Industrial CyberSecurity for Networks. После установки вы можете добавлять учетные записи пользователей программы при подключении к Серверу через веб-интерфейс или при переустановке программы.

В зависимости от используемого способа подключения к Серверу, пользователям доступны следующие наборы функций:

- функции программы, доступные через веб-интерфейс;
- функции программы, доступные в Консоли.

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 пользователей программы.

- Оператор.

  Пользователь с ролью Оператор обладает правами доступа только для мониторинга и просмотра сведений.

Учетной записи пользователя, создаваемой во время установки или переустановки Kaspersky Industrial CyberSecurity for Networks, назначается роль Администратор. Если при переустановке программы указывается имя уже существующей учетной записи пользователя, роль этого пользователя не изменяется.

После установки программы вы можете подключиться к Серверу через веб-интерфейс под учетной записью пользователя с ролью Администратор и сформировать список учетных записей пользователей программы с соответствующими ролями. В программе можно создать до 100 учетных записей пользователей программы.

При подключении к Серверу пользователь получает права доступа, соответствующие роли его учетной записи. Если во время работы пользователя 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 программы на закладке **Пользователи** в разделе **Параметры** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Функции программы, доступные через веб-интерфейс

В этом разделе приведены функции программы, доступные пользователям при подключении к Серверу через веб-интерфейс (см. таблицу ниже).

Доступные функции программы при подключении через веб-интерфейс 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	✓	✓
Добавление точки мониторинга	✓	
Включение точек мониторинга	✓	
Выключение точек мониторинга	✓	
Переименование точки мониторинга	✓	
Удаление точки мониторинга	✓	
Определение Ethernet-порта, связанного с сетевым интерфейсом	✓	

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 своей учетной записи для подключения через веб-интерфейс	✓	✓
Просмотр таблицы устройств	✓	✓
Просмотр сведений об устройстве	✓	✓
Формирование дерева групп устройств	✓	
Добавление устройств вручную	✓	
Объединение устройств	✓	
Удаление устройств	✓	
Изменение статусов устройств	✓	
Управление размещением устройств в дереве групп	✓	
Установка и удаление меток для устройств	✓	
Изменение сведений об устройстве	✓	
Добавление, изменение и удаление пользовательских полей для устройства	✓	
Просмотр событий, связанных с устройствами	✓	✓
Просмотр таблицы правил контроля сети	✓	✓
Создание правил контроля сети вручную	✓	
Изменение параметров правила контроля сети	✓	
Изменение состояния правила контроля сети	✓	
Удаление правил контроля сети	✓	
Управление технологиями	✓	
Мониторинг системы в онлайн-режиме	✓	✓
Работа с картой сети	✓	✓
Перемещение узлов и групп в другие группы на карте сети	✓	
Мониторинг событий и инцидентов	✓	✓
Мониторинг параметров технологического процесса	✓	✓

Функции программы, доступные в Консоли

В этом разделе приведены функции программы, доступные пользователям в Консоли Kaspersky Industrial CyberSecurity for Networks (см. таблицу ниже).

Доступные функции программы в Консоли в зависимости от роли пользователя

Функция программы	Администратор	Оператор
Контроль состояния программы в Консоли Kaspersky Industrial CyberSecurity for Networks	✓	✓
Просмотр информации о добавленном лицензионном ключе	✓	✓
Добавление лицензионного ключа	✓	
Удаление лицензионного ключа	✓	
Просмотр сведений об установке обновлений	✓	✓
Выбор источника обновлений	✓	
Выбор режима запуска обновления	✓	
Запуск обновления вручную	✓	
Создание новой политики безопасности	✓	✓
Сохранение политики безопасности в директории	✓	✓
Открытие политики безопасности из директории	✓	✓
Применение политики безопасности на Сервере	✓	
Загрузка текущей политики безопасности с Сервера	✓	✓
Просмотр свойств политики безопасности	✓	✓
Изменение имени политики безопасности	✓	✓
Настройка контроля процесса	✓	✓ (до применения политики безопасности на Сервере)
Настройка событий	✓	✓ (до применения политики безопасности на Сервере)
Просмотр таблицы с наборами правил обнаружения вторжений	✓	✓
Изменение состояния 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	✓	
Включение и выключение аудита действий пользователей	✓	
Изменение уровней ведения журналов работы процессов	✓	

Просмотр сведений об учетных записях пользователей программы

Просматривать сведения об учетных записях пользователей программы могут только пользователи с ролью Администратор.

Чтобы просмотреть сведения об учетных записях пользователей программы, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры** и перейдите на закладку **Пользователи**.

   На закладке **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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры** и перейдите на закладку **Пользователи**.

3. На закладке **Пользователи** 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.

   Вы можете использовать прописные и строчные буквы латинского алфавита, цифры, а также следующие специальные символы: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`.

Пароль должен удовлетворять следующим требованиям:

- содержит от 8 до 20 символов;
- содержит одну или несколько прописных букв;
- содержит одну или несколько строчных букв;
- содержит одну или несколько цифр.

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

Изменить роль учетной записи пользователя программы 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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Параметры** и перейдите на закладку **Пользователи**.
3. На закладке **Пользователи** 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

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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры** и перейдите на закладку **Пользователи**.

3. На закладке **Пользователи** 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 открытия веб-интерфейса Kaspersky Industrial CyberSecurity for Networks вы можете изменить пароль своей учетной записи, под которой выполнено подключение к Серверу.

Рекомендуется изменять пароль в следующих случаях:

- выполнено первое подключение после создания учетной записи;
- текущий пароль скомпрометирован;
- нужно выполнить регулярную смену пароля в соответствии с требованиями информационной безопасности на предприятии.

Чтобы изменить пароль своей учетной записи, выполните следующие действия:

1. В окне веб-браузера 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-браузер или через Консоль программы.

Политики безопасности

Политика безопасности – это набор данных, которые определяют следующие параметры работы программы:

- параметры контроля процесса;
- параметры регистрации для типов событий.

Остальные параметры работы программы (в том числе параметры контроля устройств, контроля сети и обнаружения вторжений) применяются независимо от действующей политики безопасности.

Программа регистрирует события и отображает значения параметров технологического процесса в соответствии с действующей политикой безопасности, которая исполняется на Сервере в текущий момент. На Сервере одновременно может исполняться только одна политика безопасности.

Вы можете создать, изменить или открыть политику безопасности в Консоли программы. Чтобы Сервер программы начал работать в соответствии с политикой безопасности, ее нужно применить на Сервере. Вы можете создать несколько политик безопасности и сохранить политики безопасности в директориях на компьютере, на котором работает Консоль программы.

Директория, в которую вы сохранили политику безопасности, содержит следующий набор файлов политики безопасности:

- common;
- gate;
- industrial;
- meta_data;
- nic;
- ui;
- version.

Изменение файлов политики безопасности в любом редакторе, кроме Консоли Kaspersky Industrial CyberSecurity for Networks, может привести к нарушению работы Kaspersky Industrial CyberSecurity for Networks при применении такой политики безопасности на Сервере. Программа может перестать выполнять функции по защите промышленной сети.

Вы можете открыть из директории на компьютере и просмотреть ранее сохраненную политику безопасности в Консоли Kaspersky Industrial CyberSecurity for Networks. При открытии политики безопасности текущая политика безопасности перестает отображаться в Консоли программы, но продолжает работать на Сервере до момента применения новой политики.

В Консоли Kaspersky Industrial CyberSecurity for Networks текущей версии не поддерживается возможность открытия политик безопасности, созданных в предыдущей версии программы. Вы можете импортировать политики безопасности предыдущей версии программы с помощью утилиты преобразования политик безопасности.

Политику безопасности можно открыть из директории независимо от состояния подключения Консоли к Серверу Kaspersky Industrial CyberSecurity for Networks. Если подключение к Серверу отсутствует, в Консоли программы на закладках **Контроль процесса** и **Настройка событий** отображаются данные открываемой политики. При этом в окне Консоли программы выводится информация о том, что подключение к Серверу отсутствует.

Если вы хотите просмотреть в Консоли действующую политику безопасности, вы можете загрузить текущую политику безопасности с Сервера. Для загрузки политики безопасности с Сервера требуется подключение Консоли к Серверу программы.

Вы можете просмотреть основные сведения о политике безопасности, открытой в Консоли программы, и о политике безопасности, которая исполняется на Сервере, в окне **Свойства политики безопасности**. В этом окне отображаются следующие сведения:

- **Имя** – имя политики безопасности.
- **Применена** – время последнего применения на Сервере (для политики безопасности, которая исполняется на Сервере).
- **Сохранена** – время последнего сохранения в директорию (для политики безопасности, которая открыта в Консоли программы).
- **Идентификатор** – идентификатор экземпляра политики безопасности.
- **Путь** – путь к директории, в которой сохранена политика безопасности (для политики безопасности, которая открыта в Консоли программы).

Создание новой политики безопасности

Вы можете создать новую политику безопасности при работе с Консолью программы.

Параметры, заданные в созданной политике безопасности, начинают действовать в Kaspersky Industrial CyberSecurity for Networks после применения на Сервере.

Чтобы создать новую политику безопасности, выполните следующие действия:

1. В меню **Управление политикой безопасности** в окне Консоли программы выберите пункт **Создать**.
2. Если в текущей политике безопасности есть несохраненные изменения, откроется окно с запросом для продолжения. Выполните нужное действие:
   - Если вы хотите сохранить изменения в текущей политике безопасности, нажмите на кнопку **Да**.
   - Если вы не хотите сохранить изменения, нажмите на кнопку **Нет**.

   Откроется окно для ввода имени новой политики безопасности.
3. Введите имя новой политики безопасности и нажмите на кнопку **ОК**. Рекомендуется использовать латинские символы.
4. Настройте параметры контроля процесса и параметры регистрации для типов событий.
5. Сохраните политику безопасности.

Сохранение политики безопасности в директории

Вы можете сохранить политику безопасности, которая открыта в Консоли программы, в виде набора файлов в директории.

Чтобы сохранить изменения в текущей политике безопасности, выполните следующие действия:

1. В окне Консоли откройте меню **Управление политикой безопасности**.
2. Выберите пункт **Сохранить**.

Чтобы сохранить политику безопасности с выбором другой директории, выполните следующие действия:

1. В окне Консоли откройте меню **Управление политикой безопасности**.
2. Выберите пункт **Сохранить как**.
3. В появившемся окне укажите путь для сохранения политики безопасности.
4. Нажмите на кнопку **Выбрать**.

Открытие политики безопасности из директории

Вы можете открыть политику безопасности следующими способами:

- выбрать директорию с сохраненными файлами политики безопасности;
- выбрать недавно открывавшуюся политику безопасности.

Чтобы открыть политику безопасности с выбором директории, выполните следующие действия:

1. В меню **Управление политикой безопасности** в окне Консоли выберите пункт **Открыть**.
2. Если в текущей политике безопасности есть несохраненные изменения, откроется окно с запросом для продолжения. Выполните нужное действие:
   - Если вы хотите сохранить изменения в текущей политике безопасности, нажмите на кнопку **Да**.
   - Если вы не хотите сохранить изменения, нажмите на кнопку **Нет**.

   Откроется окно для выбора директории с файлами политики безопасности.
3. Выберите директорию, в которой расположены файлы политики безопасности.

Данные открытой политики безопасности загрузятся в Консоль Kaspersky Industrial CyberSecurity for Networks. В заголовке окна Консоли отобразится название открытой политики безопасности.

Чтобы открыть недавно открывавшуюся политику безопасности, выполните следующие действия:

1. В меню **Управление политикой безопасности** → **Недавние** в окне Консоли выберите имя политики безопасности, которую вы хотите открыть.
2. Если в текущей политике безопасности есть несохраненные изменения, откроется окно с запросом для продолжения. Выполните нужное действие:

- Если вы хотите сохранить изменения в текущей политике безопасности, нажмите на кнопку **Да**.
- Если вы не хотите сохранить изменения, нажмите на кнопку **Нет**.

Данные выбранной политики безопасности загрузятся в Консоль Kaspersky Industrial CyberSecurity for Networks. В заголовке окна Консоли отобразится название выбранной политики безопасности.

Применение политики безопасности на Сервере

Применять текущую политику безопасности на Сервере Kaspersky Industrial CyberSecurity for Networks могут только пользователи с ролью Администратор.

Чтобы применить политику безопасности на Сервере, выполните следующие действия:

1. Убедитесь, что в Консоли программы отображается политика безопасности, которую вы хотите применить на Сервере.
2. В меню **Управление политикой безопасности** в окне Консоли программы выберите пункт **Применить**.
3. Если для текущего сеанса работы с Консолью указаны учетные данные пользователя с ролью Оператор, откроется окно с запросом смены пользователя. Нажмите на кнопку **Да** в окне запроса и введите имя и пароль пользователя с ролью Администратор в следующем окне.

   Откроется окно с запросом подтверждения на применение политики безопасности.
4. Подтвердите применение политики безопасности. Для этого нажмите на кнопку **Да** в окне запроса.

   На экране отобразится индикатор выполнения, который показывает процесс применения политики безопасности.

Сервер и связанные с ним сенсоры автоматически начнут работать согласно новой политике безопасности. Вы можете просмотреть, какая политика безопасности исполняется на Сервере программы, в окне **Свойства политики безопасности**.

Загрузка в Консоль политики безопасности с Сервера

При загрузке политики безопасности с Сервера Kaspersky Industrial CyberSecurity for Networks в Консоли программы перестает отображаться ранее открытая политика безопасности.

Чтобы загрузить политику безопасности с Сервера, выполните следующие действия:

1. В меню **Управление политикой безопасности** в окне Консоли выберите пункт **Загрузить с Сервера**.
2. Если в текущей политике безопасности есть несохраненные изменения, откроется окно с запросом для продолжения. Выполните нужное действие:
   - Если вы хотите сохранить изменения в текущей политике безопасности, нажмите на кнопку **Да**.
   - Если вы не хотите сохранить изменения, нажмите на кнопку **Нет**.

Данные политики безопасности, примененной на Сервере, отобразятся в Консоли Kaspersky Industrial CyberSecurity for Networks.

Просмотр свойств политики безопасности

Чтобы просмотреть свойства политики безопасности, выполните следующие действия:

1. В меню **Управление политикой безопасности** в окне Консоли выберите пункт **Свойства**.

   На экране отобразится окно **Свойства политики безопасности**. В окне выводятся сведения о политике безопасности, которая открыта в Консоли, и о политике безопасности, которая применена на Сервере.

2. Просмотрите свойства политики безопасности и нажмите на кнопку **ОК**, чтобы закрыть окно.

Изменение имени политики безопасности

Вы можете переименовать политику безопасности, которая открыта в Консоли программы. Если вы хотите переименовать политику безопасности, которая исполняется на Сервере, вам нужно загрузить политику безопасности с Сервера, переименовать ее в Консоли, и затем применить на Сервере.

Чтобы изменить имя политики безопасности, выполните следующие действия:

1. В меню **Управление политикой безопасности** в окне Консоли программы выберите пункт **Свойства**.

   На экране отобразится окно **Свойства политики безопасности**.

2. В поле **Имя** введите новое имя политики безопасности и нажмите на кнопку **ОК**.

   В заголовке окна Консоли программы отобразится новое имя политики безопасности.

3. Сохраните политику безопасности.

Об утилите преобразования политик безопасности

Утилита преобразования политик безопасности config_converter (далее также "утилита config_converter") предназначена для преобразования политик безопасности, созданных в Kaspersky Industrial CyberSecurity for Networks версии 2.8, для работы в текущей версии программы.

Утилита config_converter расположена в директории установки Kaspersky Industrial CyberSecurity for Networks: /opt/kaspersky/kics4net/bin/.

Для запуска утилиты config_converter используются следующие параметры командной строки:

- `--cfg-version` – версия программы, в которой создана исходная политика безопасности.

  По умолчанию задана версия 2.8.

- `-i` – путь к директории с исходной политикой безопасности. Это обязательный параметр.

- `-o` – путь к директории, в которую будет помещена преобразованная политика безопасности. Это обязательный параметр.

  Если указанная директория не существует, то она будет создана автоматически.

- `-F` – автоматическая перезапись файлов в директории с преобразованной политикой безопасности.

  Если параметр `-F` задан, то перед преобразованием утилита config_converter автоматически удалит все файлы в директории, в которую будет помещена преобразованная политика безопасности.

  Если параметр `-F` не задан, то утилита config_converter предложит выбрать, нужно ли перезаписывать файлы в директории, в которую будет помещена преобразованная политика безопасности. Если вы укажете вариант `Нет`, то преобразование выполняться не будет.

- `-h` – отображение краткой справки по параметрам командной строки.

- `-l` – язык интерфейса утилиты config_converter. По умолчанию задан русский язык. Чтобы использовать английский язык, для параметра нужно указать значение `english`.

Преобразование и импорт политики безопасности

Вы можете преобразовать политику безопасности Kaspersky Industrial CyberSecurity for Networks предыдущей версии с помощью утилиты преобразования политик безопасности. После преобразования политики безопасности ее можно импортировать в текущую версию программы.

Чтобы преобразовать и импортировать политику безопасности, созданную в предыдущей версии программы, выполните следующие действия:

1. Откройте консоль операционной системы и перейдите в директорию /opt/kaspersky/kics4net/bin/.

2. В командной строке введите команду:

   ```
   ./config_converter -i <имя директории с исходной политикой> \
   -o <имя директории для преобразованной политики>
   ```

   Пример:
   ```
   ./config_converter -i /home/user1/policy1 -o /home/user1/policy2
   ```

   После завершения работы утилиты config_converter проверьте наличие преобразованной политики безопасности в заданной директории.

3. Откройте преобразованную политику безопасности в Консоли программы.

4. При необходимости дополнительно настройте параметры контроля процесса и параметры регистрации для типов событий, после чего сохраните политику безопасности.

5. Примените политику безопасности на Сервере.

Контроль процесса

В Kaspersky Industrial CyberSecurity for Networks контроль технологического процесса осуществляется для устройств, которые передают и принимают параметры технологического процесса и системные команды. Устройства для контроля процесса могут быть различных типов из числа поддерживаемых программой.

Для контроля технологического процесса в трафике промышленной сети вы можете использовать правила контроля процесса и функциональность отслеживания системных команд.

Правило контроля процесса – это набор условий для значений тегов. В правилах контроля процесса описываются ситуации, которые необходимо обнаруживать в трафике промышленной сети (например, превышение тегом указанного значения).

При выполнении условий правила в Kaspersky Industrial CyberSecurity for Networks регистрируется событие. Вы можете указать нужный тип регистрируемого события при настройке правила контроля процесса.

Отслеживание системных команд обеспечивает регистрацию событий обнаружения в трафике переданных системных команд. При настройке параметров устройств для контроля процесса вы можете выбрать нужные системные команды для отслеживания. Эта функциональность может использоваться независимо от правил контроля процесса.

Списки с правилами контроля процесса и с устройствами и тегами для контроля процесса входят в политику безопасности. Применять текущую политику безопасности на Сервере могут только пользователи с ролью Администратор. При этом возможности внесения изменений и сохранения политики безопасности в директории (в том числе с измененными параметрами для контроля процесса) доступны как пользователям с ролью Администратор, так и пользователям с ролью Оператор.

Вы можете сформировать список правил контроля процесса и список устройств и тегов для контроля процесса в Консоли Kaspersky Industrial CyberSecurity for Networks на закладке Контроль процесса.

При подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер возможность работы с правилами контроля процесса и устройствами для контроля процесса недоступна.

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;
  - Allen-Bradley® серий ControlLogix®, CompactLogix™;
  - BECKHOFF® серий CX;
  - Honeywell C300 для систем управления Experion PKS / PlantCruise;
  - Honeywell ControlEDGE серии 900;
  - Emerson DeltaV серий MD, MD Plus, MQ;
  - Emerson серии ControlWave;
  - General Electric RX3i;
  - 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;
- Yokogawa ProSafe-RS;
- Yokogawa серий AFV10, AFV30, AFV40;
- ПЛК с системой исполнения для CODESYS V3;
- Прософт-Системы Regul R500.

- Интеллектуальные электронные устройства (далее IED):
  - ABB серии Relion™: REF615, RED670, REL670, RET670;
  - General Electric серии MULTILIN: B30, C60;
  - 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 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.
- Устройства, относящиеся к сетевому оборудованию:
  - Моха серии NPort IA 5000;
  - устройства ввода-вывода, поддерживающие протоколы DCE/RPC, FTP, IEC 60870-5-101, IEC 60870-5-104, Modbus TCP, OPC DA, OPC UA Binary, протокол взаимодействия устройств по технологии WMI.

Для перечисленных типов устройств Kaspersky Industrial CyberSecurity for Networks анализирует взаимодействия по следующим протоколам прикладного уровня:

- ABB SPA-Bus;
- Allen-Bradley EtherNet/IP;
- BECKHOFF ADS/AMS;
- CODESYS V3 Gateway;
- DCE/RPC и протоколы на его основе (OPC DA, протокол взаимодействия устройств по технологии WMI);
- DMS для устройств ABB AC 700F;
- DNP3;
- Emerson ControlWave Designer;
- Emerson DeltaV;
- FTP;
- General Electric SRTP;
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104;
- IEC 61850: GOOSE, MMS (включая MMS Reports), Sampled Values;
- Mitsubishi MELSEC System Q;
- Modbus TCP;
- OMRON FINS;
- OPC UA Binary;
- Siemens Industrial Ethernet;
- Siemens S7comm™, S7comm-plus;
- Yokogawa Vnet/IP;
- Релематика BDUBus;
- модификация протокола MMS для устройств ABB AC 800M;
- модификация протокола Modbus TCP для устройств ЭКРА серии 200;
- протокол взаимодействия устройств Foxboro FCP270, FCP280;
- протокол взаимодействия устройств Moxa серии NPort IA 5000;
- протокол начальной настройки устройств Прософт-Системы;
- протокол обмена данными с устройствами Emerson серии ControlWave;
- протокол устройств с системным ПО Siemens DIGSI 4;

- протоколы взаимодействия устройств в системах управления Honeywell Experion PKS / PlantCruise;
- протоколы обнаружения и взаимодействия устройств Honeywell ControlEDGE серии 900.

Дерево устройств и тегов для контроля процесса

Дерево устройств и тегов для контроля процесса – это иерархическая структура, которая отображает связь устройств для контроля процесса (например, ПЛК), их протоколов и тегов. Входящие в эту структуру теги вы можете использовать в правилах контроля процесса.

Для элементов дерева используются следующие значки:

- – устройство для контроля процесса;
- – протокол;
- – тег.

Об устройствах и тегах для контроля процесса

Устройство для контроля процесса – это устройство, которое используется для автоматизации технологического процесса на предприятии (например, программируемый логический контроллер).

Тег – это параметр технологического процесса, передаваемый в промышленной сети (например, контролируемая температура). Значения тегов передаются устройствами по определенным протоколам.

В Kaspersky Industrial CyberSecurity for Networks для контроля процесса поддерживаются различные типы устройств и протоколов.

После установки программы используются исходные модули обработки протоколов прикладного уровня по технологии Контроль технологического процесса. Вы можете обновлять модули обработки протоколов, устанавливая обновления.

Для описания логических связей между устройствами, поддерживаемыми протоколами и тегами вам нужно сформировать иерархическую структуру из этих элементов в виде дерева. Вы можете формировать дерево устройств и тегов следующими способами:

- Добавлять вручную устройства, протоколы (при добавлении устройств или при изменении параметров устройств) и теги.
- Добавлять теги из хранилища обнаруженных тегов.
- Импортировать теги и устройства из файлов данных.

После добавления тегов в дерево вы можете указать нужные теги в правилах контроля процесса.

Программа отслеживает значения только тех тегов, которые указаны в правилах контроля процесса.

Вы можете контролировать значения тегов в таблице зарегистрированных событий или просматривать в онлайн-режиме в разделе Теги.

Параметры устройства для контроля процесса или тега отображаются в Консоли программы на закладке **Контроль процесса**. Область редактирования параметров появляется в нижней части закладки при добавлении или изменении устройства для контроля процесса или тега.

Параметры устройств для контроля процесса

Устройствам для контроля процесса могут быть заданы следующие параметры:

- **Тип устройства** – тип устройства из числа поддерживаемых типов устройств для контроля процесса в Kaspersky Industrial CyberSecurity for Networks. Поддерживаемые типы устройств перечислены в раскрывающемся списке.
- **Имя устройства** – имя, которое отображается в списке устройств для контроля процесса.
- **Системные команды** – параметры отслеживания системных команд для устройства.

  В строке **Системные команды** представлены следующие элементы:

  - Поле **Всего** – отображает общее количество системных команд для выбранных протоколов.
  - Поле **Отслеживается** – отображает количество отслеживаемых системных команд, при обнаружении которых программа регистрирует события.
  - Ссылка **Выбрать системные команды** – открывает окно **Отслеживаемые системные команды**, в котором вы можете выбрать из списка системные команды для отслеживания.
- **Протокол** – используемый протокол. В раскрывающемся списке перечислены доступные протоколы для устройств указанного типа, трафик которых вы можете отслеживать.

  При выборе протокола Modbus TCP справа от раскрывающегося списка появляется флажок **Менять местами машинные слова в 32-битных значениях**. С помощью этого флажка вы можете включить или выключить поддержку обратной последовательности машинных слов в 32-битных значениях данных по протоколу Modbus TCP.

  При выборе протокола IEC 60870-5-101 справа от раскрывающегося списка появляется ссылка **Дополнительные параметры**. По ссылке открывается окно **Дополнительные параметры**, в котором вы можете настроить следующие параметры протокола:

  - **Адрес ASDU два байта**. Флажок включает / выключает режим двухбайтовой адресации для блоков данных прикладного уровня (Application Service Data Unit, ASDU). Если режим выключен, используется однобайтовая адресация.
  - **Инициатор**. Флажок включает / выключает использование дополнительного байта для адреса инициатора в идентификаторе блока данных.
  - **Размер блока для адреса канала**. Раскрывающийся список позволяет выбрать количество байт в блоке адреса канального уровня.
  - **Размер блока для адреса объекта**. Раскрывающийся список позволяет выбрать количество байт в блоке адреса объекта информации.
- **Адрес** – в зависимости от выбранного протокола позволяет указать IP-адрес и порт, MAC-адрес устройства или идентификатор домена (для протокола IEC 61850: GOOSE).

Вы можете добавить дополнительные протоколы и адреса для устройства с помощью кнопок **Добавить протокол** и **Дополнительный адрес устройства**. Для удаления дополнительных протоколов и адресов используйте кнопки × слева от названий параметров.

Параметры тегов

Для тегов предусмотрены следующие параметры:

- Основные параметры:
  - **Имя тега** – отображаемое название тега.
  - **Тип данных** – тип данных тега.
  - **Описание** – дополнительные сведения о теге.
  - **Единица измерения** – единица измерения параметра технологического процесса, который представлен тегом.
  - **Идентификатор** – порядковый номер тега. Идентификатор тега задается автоматически.
- Параметры, уточняющие пределы значений в зависимости от выбранного типа данных тега:
  - **Масштабируемый тег** – определяет пределы масштабирования тега в полях ввода минимумов и максимумов для входных и выходных значений.
  - **Максимальная длина строки** – определяет количество символов для тега со строковым типом данных.
- Параметры, определяющие данные тега в зависимости от протокола:
  - **Область**.
  - **Область памяти**.
  - **Адрес тега**.
  - **Адрес ASDU**.
  - **Номер блока**.
  - **Бит**.
  - **Номер банка**.
  - **Количество бит**.
  - **Группа**.
  - **Индекс**.
  - **Локальные идентификаторы (LID)**.
  - **Идентификатор среды выполнения (RID)**.
  - **Номер БД**.

- Приложение.
- Экземпляр POU.
- Смещение переменной.
- MSD-идентификатор тега.
- MSD-версия проекта.

В области редактирования выделены параметры, для которых обязательно должны быть указаны значения.

Для получения данных о параметрах технологического процесса с устройств, поддерживающих протоколы стандарта IEC 60870-5-104, в Kaspersky Industrial CyberSecurity for Networks нужно использовать соответствующие типы данных тегов. Сведения о соответствии типов блоков данных прикладного уровня (ASDU) в протоколах стандарта IEC 60870-5-104 и типов данных тегов в Kaspersky Industrial CyberSecurity for Networks вы можете найти в Базе знаний на веб-сайте "Лаборатории Касперского".

Об обнаружении неизвестных тегов

Kaspersky Industrial CyberSecurity for Networks может анализировать трафик для обнаружения и сохранения информации о неизвестных тегах. Неизвестными считаются теги, которые отсутствуют в политике безопасности, но относятся к устройствам и протоколам, присутствующим в дереве устройств и тегов для контроля процесса. Для проверки обнаруженных тегов программа использует политику безопасности, которая исполняется на Сервере.

Режим обнаружения неизвестных тегов

Получение из трафика информации о неизвестных тегах выполняется при работе программы в режиме обнаружения неизвестных тегов. Вы можете включать и выключать этот режим.

При работе программы в режиме обнаружения неизвестных тегов возможно некоторое снижение производительности модулей обработки протоколов прикладного уровня. Поэтому по умолчанию после установки программы обнаружение неизвестных тегов выключено. Рекомендуется включать режим обнаружения неизвестных тегов на время, достаточное для обнаружения всех тегов, которые могут относиться к устройствам и протоколам в политике безопасности. После добавления обнаруженных тегов в политику безопасности рекомендуется выключить этот режим.

Обнаружение неизвестных тегов поддерживается для следующих протоколов:

- Allen-Bradley EtherNet/IP;
- CODESYS V3 Gateway;
- DMS для устройств ABB AC 700F;
- DNP3;
- Emerson DeltaV;

- IEC 60870: IEC 60870-5-101, IEC 60870-5-104;
- IEC 61850: MMS;
- OPC DA;
- OPC UA Binary;
- Yokogawa Vnet/IP;
- протокол обмена данными с устройствами Emerson серии ControlWave.

Хранилище обнаруженных тегов

Теги, полученные из трафика в режиме обнаружения неизвестных тегов, сохраняются в хранилище обнаруженных тегов. Это хранилище предназначено для временного хранения информации о тегах до их добавления в политику безопасности.

Информация о тегах не дублируется в хранилище. Если один и тот же тег обнаружен в трафике несколько раз, в хранилище обновляются сведения о дате и времени последнего обнаружения этого тега.

Для хранилища обнаруженных тегов действуют следующие ограничения:

- размер хранилища – не более 100 МБ;
- количество тегов в хранилище – не более 100 000.

При достижении любого из указанных ограничений программа удаляет из хранилища самые старые теги, чтобы сохранить новые обнаруженные теги. Старыми считаются теги, которые были обнаружены раньше остальных.

Очистка хранилища выполняется автоматически при добавлении тегов в политику безопасности.

Включение и выключение обнаружения неизвестных тегов

Вы можете включать и выключать обнаружение неизвестных тегов при подключении к Серверу через веб-браузер.

По умолчанию после установки программы обнаружение неизвестных тегов выключено. Рекомендуется включать режим обнаружения неизвестных тегов после предварительной подготовки программы. Для предварительной подготовки вам нужно добавить в дерево устройств и тегов все устройства и протоколы, для которых вы хотите обнаружить теги в трафике. Добавление устройств и протоколов выполняется в Консоли программы. Вы можете добавить устройства и протоколы вручную или импортировать из файлов данных. После добавления устройств и протоколов вам нужно применить текущую политику безопасности на Сервере.

Включать и выключать обнаружение неизвестных тегов могут только пользователи с ролью Администратор.

Чтобы включить или выключить обнаружение неизвестных тегов, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры** и перейдите на закладку **Технологии**.

3. С помощью переключателя **Обнаружение неизвестных тегов** включите или выключите обнаружение неизвестных тегов.

4. После включения или выключения режима обнаружения дождитесь перевода переключателя в нужное состояние (*Включено* или *Выключено*).

   Процесс занимает некоторое время. Переключатель при этом будет недоступен.

Добавление устройства для контроля процесса

Вы можете добавить нужные устройства для контроля процесса в Консоли программы.

Добавление устройств типа **Устройство IEC 61850** выполняется с помощью импорта тегов и устройств из файлов данных.

Чтобы добавить новое устройство для контроля процесса, выполните следующие действия:

1. Выберите закладку **Контроль процесса** в окне Консоли.

2. В области **Устройства и теги** нажмите на кнопку **Добавить устройство**.

   В нижней части закладки отобразится область редактирования устройств.

3. Настройте параметры:

   - выберите тип устройства;
   - введите имя устройства;
   - укажите один или несколько протоколов, по которым осуществляется взаимодействие с устройством;
   - задайте параметры одного или нескольких адресов для взаимодействия с устройством;
   - при необходимости измените параметры отслеживания системных команд для устройства. По умолчанию для указанных протоколов устройства отслеживаются все системные команды, кроме тех, которые часто возникают при нормальной работе устройства.

4. Сохраните параметры устройства с помощью кнопки **ОК**.

   В дереве устройств и тегов для контроля процесса отобразится устройство и связанные с ним протоколы для отслеживания.

Добавление тегов из хранилища обнаруженных тегов

При добавлении тегов из хранилища обнаруженных тегов программа автоматически распределяет добавляемые теги в дереве устройств и тегов. Теги добавляются в политику безопасности, которая открыта в Консоли.

В политику безопасности в Консоли могут быть добавлены не все теги из хранилища обнаруженных тегов. Вы можете добавить только те теги, для которых в политике безопасности присутствуют соответствующие устройства и протоколы. Если политика безопасности в Консоли не содержит устройство и / или протокол, к которым относится тег из хранилища, этот тег невозможно добавить в политику.

> Если вы хотите добавить все теги из хранилища обнаруженных тегов, вам нужно загрузить в Консоль политику безопасности с тем же составом устройств и протоколов, который использовался при обнаружении неизвестных тегов. Для этого, например, вы можете загрузить в Консоль текущую политику безопасности с Сервера (если в этой политике безопасности не изменялся состав устройств и протоколов после обнаружения неизвестных тегов).

При добавлении тегов программа последовательно обрабатывает теги, имеющиеся в хранилище обнаруженных тегов. Каждый обработанный тег автоматически удаляется из хранилища. Программа удаляет из хранилища все обработанные теги – как добавленные в политику безопасности, так и не добавленные.

Добавлять теги из хранилища обнаруженных тегов в политику безопасности в Консоли могут как пользователи с ролью Администратор, так и пользователи с ролью Оператор.

Чтобы добавить теги из хранилища обнаруженных тегов в политику безопасности в Консоли, выполните следующие действия:

1. Запустите Консоль программы.

2. Выберите закладку **Контроль процесса** в окне Консоли.

3. Нажмите на кнопку **Загрузить теги**. Кнопка доступна, если хранилище обнаруженных тегов не пустое (в поле **Обнаружено тегов** отображается ненулевое значение).

   Запустится процесс добавления тегов и на экране отобразится окно **Добавление обнаруженных тегов**. После завершения процесса добавления тегов в окне появится информация о количестве обнаруженных тегов, имевшихся в хранилище, и о количестве тегов, добавленных в политику безопасности.

   > Вы можете прервать процесс добавления тегов с помощью кнопки **Отмена** (кнопка отображается до завершения процесса). В этом случае в политику безопасности добавятся только теги из числа обработанных на момент прерывания процесса. Необработанные теги не будут удалены из хранилища обнаруженных тегов.

4. Закройте окно **Добавление обнаруженных тегов**.

Добавленные теги отобразятся в дереве устройств и тегов на закладке **Контроль процесса**. Вы можете изменять параметры добавленных тегов и указывать эти теги в правилах контроля процесса.

После добавления тегов из хранилища обнаруженных тегов рекомендуется применить политику безопасности на Сервере и выключить обнаружение неизвестных тегов.

Если после добавления тегов политика безопасности не была применена на Сервере и при этом включено обнаружение неизвестных тегов, то добавленные в политику теги могут быть снова обнаружены как новые и помещены в хранилище тегов. Это связано с тем, что при обнаружении тегов программа проверяет их по политике безопасности, которая применена на Сервере. Однако при добавлении тегов из хранилища программа проверяет их наличие в той политике безопасности, которая загружена в Консоль (а не в политике безопасности на Сервере). Если при добавлении тегов найдены такие же теги в политике безопасности в Консоли, то эти теги не дублируются в политике.

Добавление тега вручную

Чтобы вручную добавить новый тег, выполните следующие действия:

1. Выберите закладку **Контроль процесса** в окне Консоли.

2. В дереве устройств и тегов выберите устройство и его протокол, для которого вы хотите добавить тег. Необходимо выбрать протокол, в котором поддерживается передача тегов. Вы также можете выбрать один из имеющихся тегов для протокола.

   После выбора протокола (или одного из тегов этого протокола) становится активной кнопка **Добавить тег**. Кнопка будет неактивной, если выбран протокол, в котором передача тегов не поддерживается (например, системный протокол FTP).

3. Нажмите на кнопку **Добавить тег**.

   В нижней части закладки отобразится область редактирования тегов.

4. Настройте параметры:

   - укажите обязательные параметры, названия которых выделены шрифтом (например, имя тега, тип данных);

   - при необходимости укажите другие параметры из числа доступных для тега в зависимости от протокола и выбранного типа данных (например, единица измерения, пределы масштабирования).

5. Сохраните параметры тега с помощью кнопки **ОК**.

В дереве устройств и тегов отобразится новый тег для выбранного протокола.

Изменение параметров устройства для контроля процесса или тега

Чтобы изменить параметры устройства для контроля процесса или тега, выполните следующие действия:

1. Выберите закладку **Контроль процесса** в окне Консоли.

2. В дереве устройств и тегов выберите элемент, параметры которого вы хотите изменить.

3. Нажмите на кнопку **Изменить** в правом нижнем углу закладки.

4. Если выбран тег, на экране отобразится запрос на продолжение. В этом случае подтвердите свое решение для изменения параметров тега.

   В нижней части экрана отобразится область редактирования устройств или тегов.

5. При настройке параметров для устройства выполните следующие действия:

   a. Введите имя устройства.

   b. Укажите один или несколько протоколов, по которым осуществляется взаимодействие с устройством.

   c. Задайте параметры одного или нескольких адресов для взаимодействия с устройством.

   d. При необходимости измените параметры отслеживания системных команд для устройства.

6. При настройке параметров для тега выполните следующие действия:

   a. Укажите обязательные параметры, названия которых выделены шрифтом (например, имя тега, тип данных).

   b. При необходимости укажите другие параметры из числа доступных для тега в зависимости от протокола и выбранного типа данных (например, единица измерения, пределы масштабирования).

7. Сохраните изменения с помощью кнопки **ОК**.

Удаление устройства для контроля процесса или тега

Чтобы удалить устройство для контроля процесса или тег, выполните следующие действия:

1. Выберите закладку **Контроль процесса** в окне Консоли.

2. В дереве устройств и тегов выберите элемент, который вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

4. Подтвердите удаление устройства или тега.

Выбранный элемент будет удален из списка.

Поиск тегов

Вы можете выполнять поиск тегов по значениям в любой графе.

Для фильтрации найденных тегов вы можете выбрать один из следующих параметров фильтрации:

- все теги, созданные в текущей политике безопасности;
- теги, используемые в каких-либо правилах контроля процесса;
- теги, используемые в выбранном правиле контроля процесса.

Чтобы найти нужные теги, выполните следующие действия:

1. В правом верхнем углу области **Устройства и теги** введите поисковый запрос в поле **Поиск тегов**. Для поиска по идентификаторам тегов введите в строке поиска `id:` и далее через пробел введите искомые идентификаторы (например, `id: 3 52 675`). Поиск инициируется во время ввода символов.

   В дереве устройств и тегов отобразятся теги, которые удовлетворяют условиям поиска. Найденные теги будут отображены вместе с устройствами и протоколами, к которым относятся эти теги.

2. При необходимости выберите нужный параметр фильтрации в раскрывающемся списке **Показывать теги**:

   - **Все** – чтобы отобразить все найденные теги.
   - **В правилах** – чтобы отобразить найденные теги во всех имеющихся правилах контроля процесса.
   - **В текущем правиле** – чтобы отобразить найденные теги только выбранного правила контроля процесса.

   В дереве устройств и тегов будут отображены элементы, которые удовлетворяют критерию фильтрации.

3. Если вы выбрали параметр фильтрации **В текущем правиле** и хотите отобразить найденные теги в другом правиле контроля процесса, выберите нужное правило в таблице правил контроля процесса.

Импорт тегов и устройств для контроля процесса из файлов данных

Вы можете добавить в политику безопасности Kaspersky Industrial CyberSecurity for Networks теги и устройства для контроля процесса, созданные ранее с помощью других систем (например, SCADA). Kaspersky Industrial CyberSecurity for Networks импортирует теги и устройства для контроля процесса из файлов данных.

Чтобы импортировать пользовательские теги и устройства для контроля процесса в Kaspersky Industrial CyberSecurity for Networks с помощью файлов данных, выполните следующие действия:

1. Выберите закладку **Контроль процесса** в окне Консоли.

2. Нажмите на кнопку **Импортировать**.

   На экране отобразится окно выбора директории с файлами данных для импорта.

3. Укажите путь к директории, в которой расположены файлы данных.

4. Нажмите на кнопку выбора директории.

   Если список устройств и тегов не пустой, в появившемся окне укажите способ импорта: **Дополнение** или **Поверх**. При выборе способа **Дополнение** импортируемые устройства будут добавлены к списку имеющихся устройств. При выборе способа **Поверх** имеющиеся устройства в списке будут заменены импортируемыми устройствами.

5. Подтвердите импорт данных с помощью кнопки **ОК**.

Импортированные устройства для контроля процесса и связанные с ними протоколы и теги отобразятся в списке на закладке **Контроль процесса**.

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 устройствами (например, START PLC), так и системные сообщения, связанные с функционированием устройств или содержащие результаты анализа пакетов (например, REQUEST NOT FOUND).

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 доступные параметры для этого типа события в Консоли программы на закладке Настройка событий.

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-браузер.

Чтобы настроить отслеживание системных команд для устройства, выполните следующие действия:

1. Выберите закладку **Контроль процесса** в окне Консоли.
2. В списке устройств и тегов выберите устройство, для которого вы хотите настроить отслеживание системных команд.
3. Нажмите на кнопку **Изменить**.

   В нижней части окна отобразится область редактирования устройств.
4. В области редактирования устройств в строке **Системные команды** нажмите на ссылку **Выбрать системные команды**.

   На экране отобразится окно **Отслеживаемые системные команды** со списком системных команд, доступных для отслеживания.

   > Список отслеживаемых системных команд формируется в зависимости от указанных протоколов для устройства. Если в списке отсутствуют нужные системные команды, закройте окно **Отслеживаемые системные команды** и добавьте в параметры устройства все недостающие протоколы, которые могут использоваться устройством.
5. В окне **Отслеживаемые системные команды** установите флажки у тех системных команд, которые вы хотите отслеживать.
6. Нажмите на кнопку **ОК**.
7. Сохраните изменения с помощью кнопки **ОК**.
8. Примените политику безопасности.

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	DEFAULT PASSWORD

	Siemens S7comm	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
Прософт-Системы Regul R500, ПЛК с системой исполнения для CODESYS V3	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 сети включен в режиме наблюдения с применением технологии Контроль системных команд.
- В таблице правил контроля сети отсутствуют правила для технологии Контроль системных команд, которые разрешают системные команды с паролями по умолчанию. Например, такие правила могут быть автоматически созданы в режиме обучения контроля сети. Если в таблице правил контроля сети присутствуют правила, разрешающие системные команды с паролями по умолчанию, рекомендуется перевести эти правила в неактивное состояние.
- Для нужных устройств включено отслеживание системных команд с паролями по умолчанию.

Правила контроля процесса

В программе могут использоваться следующие правила контроля процесса:

- правила с заданными условиями;
- правила с Lua-скриптами.

Вы можете объединять правила контроля процесса в группы для логической организации правил по произвольным признакам (например, поместить в разные группы правила, относящиеся к определенным устройствам). С помощью групп вы можете сформировать иерархическую структуру из групп и вложенных в них правил. Поддерживается до восьми уровней вложенности.

Для элементов дерева используются следующие значки:

- – группа;
- – правило с заданными условиями;
- – правило с Lua-скриптом.

О правилах контроля процесса

Правило контроля процесса с заданными условиями представляет собой набор условий для значений тегов. Несколько условий вы можете связать логическими операторами И / ИЛИ. Для нескольких условий вы можете указать приоритеты, которые будут определять порядок применения условий в правиле. При выполнении условий, заданных в правиле, регистрируется событие. Вы можете выбрать нужный тип события для правила. Правило может содержать не более восьми условий.

Правило, содержащее Lua-скрипт, представляет собой скрипт на языке Lua с описанием алгоритма для регистрации события.

Если вы используете Lua-скрипты для создания правил контроля процесса, то вы можете использовать *глобальный скрипт* – скрипт на языке Lua, в котором инициализируются глобальные переменные и функции Lua. Эти глобальные переменные и функции вы можете указать в Lua-скрипте любого конкретного правила. Заданный глобальный Lua-скрипт автоматически исполняется при применении политики безопасности. При создании политики безопасности глобальный Lua-скрипт пустой и не содержит исполняемого кода. В политике безопасности может существовать только один глобальный Lua-скрипт, который можно просматривать и изменять при работе с любым правилом, содержащим Lua-скрипт.

Параметры правила контроля процесса отображаются в области редактирования, которая появляется под списком правил при добавлении или изменении правила.

В левой части области редактирования правила вы можете настроить следующие параметры:

- Имя и описание правила.
- Для правил, в которых заданы условия для значений тегов – параметры условий, при нарушении которых будет регистрироваться событие. Сведения об условиях см. в разделе Типы условий для правил контроля процесса.
- Для правил, представляющих собой Lua-скрипт – тип Lua-скрипта (**Скрипт правила** или **Глобальный скрипт**) и текст скрипта на языке Lua. При создании скрипта правила в поле ввода отображается шаблон Lua-скрипта с краткими комментариями. Вы можете открыть окно с подробными комментариями для создания скрипта с помощью кнопки вызова справки над полем ввода скрипта. Сведения о применяемых функциях и переменных см. в разделе Функции и переменные для Lua-скрипта.

В правой части области редактирования правила вы можете настроить тип события, которое будет регистрироваться при соответствии условиям правила.

С помощью раскрывающегося списка **Событие** вы можете выбрать существующий тип события или добавить новый тип. Рядом с раскрывающимся списком расположены следующие кнопки управления:

- – редактирует выбранное событие;
- – добавляет новое событие.

Для типа события в области редактирования правила используются те же параметры типов событий, которые представлены на закладке Настройка событий.

Правила с заданными условиями для значений тегов

В правиле контроля процесса, которое задает условия для значений тегов, нужно указать тип каждого условия. У каждого типа есть определенное число дополнительных параметров, которые включают и сами теги.

Вы можете указывать типы условий при выполнении следующих действий:

- Создание правила контроля процесса с параметрами условий

  Чтобы создать правило, выполните следующие действия:

  1. Выберите закладку **Контроль процесса** в окне Консоли.
  2. Если список правил контроля процесса содержит группы, выберите группу, в которую нужно поместить новое правило. Вы можете выбрать саму группу или одно из существующих правил этой группы.
  3. Нажмите на кнопку **Добавить правило**.
     В нижней части закладки отобразится область редактирования правила.
  4. Выполните следующие действия:
     a. Введите имя и описание правила.
     b. Задайте условия.
     c. Выберите или настройте тип регистрируемого события.
  5. Нажмите на кнопку **ОК**.
     Новое правило отобразится в списке.
  6. Чтобы изменения вступили в силу, примените политику безопасности.

  Сервер программы начнет регистрировать события при выполнении условий правила.

- Изменение правила контроля процесса с параметрами условий

  Чтобы изменить правило, выполните следующие действия:

  1. Выберите закладку **Контроль процесса** в окне Консоли.
  2. В списке правил контроля процесса выделите правило, которое вы хотите изменить.
  3. Нажмите на кнопку **Изменить**.
     В нижней части закладки отобразится область редактирования правила.
  4. Выполните следующие действия:
     a. Введите имя и описание правила.
     b. Задайте условия.
     c. Выберите или настройте тип регистрируемого события.
  5. Нажмите на кнопку **ОК**.
  6. Чтобы изменения вступили в силу, примените политику безопасности.

  Сервер программы начнет регистрировать события в соответствии с изменениями в правиле.

В раскрывающемся списке типов условий вы можете выбрать один из следующих вариантов:

- **Равно** – значение контролируемого тега равно заданному значению.

  В этом типе условия используются два параметра:

  - Параметр 1: контролируемый тег типа int, bool, string.
  - Параметр 2: заданное значение (константа или тег).

- **Не равно** – значение контролируемого тега не равно заданному значению.

  В этом типе условия используются два параметра:

  - Параметр 1: контролируемый тег типа int, bool, string.
  - Параметр 2: заданное значение (константа или тег).

- **Меньше** – значение контролируемого тега меньше заданного минимально допустимого значения.

  В этом типе условия используется два параметра:

  - Параметр 1: контролируемый тег типа int, float.
  - Параметр 2: минимально допустимое значение (константа или тег).

- **Больше** – значение контролируемого тега больше заданного максимально допустимого значения.

  В этом типе условия используются два параметра:

  - Параметр 1: контролируемый тег типа int, float.
  - Параметр 2: максимально допустимое значение (константа или тег).

- **Отклонение превышает допуск** – значение контролируемого тега отличается от заданного значения более, чем указано в параметре допуска.

  В этом типе условия используются три параметра:

  - Параметр 1: контролируемый тег типа int, float.
  - Параметр 2: заданное значение (константа или тег).
  - Параметр 3: допуск в процентах от заданного значения (константа – число без знака в диапазоне от 0,001 до 100).

- **Вне диапазона** – значение контролируемого тега выходит за границы указанного диапазона.

  В этом типе условия используются три параметра:

  - Параметр 1: контролируемый тег типа int, float.
  - Параметр 2: нижняя граница диапазона (константа или тег).
  - Параметр 3: верхняя граница диапазона (константа или тег).

- **Значение изменилось** – значение контролируемого тега изменяется.

  В этом типе условия используется один параметр: контролируемый тег любого типа.

- **Бит тега равен** – значение отслеживаемого бита в контролируемом теге равно указанному значению.

В этом типе условия используются три параметра:

- Параметр 1: контролируемый тег типа int, unsigned int.
- Параметр 2: порядковый номер отслеживаемого бита в теге (целое число в диапазоне, который соответствует типу данных выбранного тега: от 1 до 8, 16, 32 или 64).
- Параметр 3: значение отслеживаемого бита в теге (указывается в виде одного из двух целых чисел: ноль или единица).

- **Обнаружение** – контролируемый тег обнаружен в отслеживаемом трафике.

  В этом типе условия используется один параметр: контролируемый тег любого типа.

- **Изменение превышает допуск** – изменение значения контролируемого тега относительно предыдущего зафиксированного значения этого тега превышает допуск.

  В этом типе условия используются два параметра:

  - Параметр 1: контролируемый тег типа int, float.
  - Параметр 2: допуск в процентах от предыдущего значения (константа – число без знака в диапазоне от 0,001 до 100).

- **Бит тега изменился** – значение отслеживаемого бита в контролируемом теге изменяется.

  В этом типе условия используются два параметра:

  - Параметр 1: контролируемый тег типа int, unsigned int.
  - Параметр 2: порядковый номер отслеживаемого бита в теге (целое число в диапазоне, который соответствует типу данных выбранного тега: от 1 до 8, 16, 32 или 64).

Чтобы указать тег для параметра, вы можете выбрать нужный тег в раскрывающемся списке или перетащить тег из списка **Устройства и теги**.

В раскрывающемся списке справа от поля с выбранным тегом вы можете выбрать, какое последнее значение тега используется в правиле. Предусмотрены следующие варианты использования:

- **Чтение** – последнее значение тега, перехваченное при чтении тега из устройства;
- **Запись** – последнее значение тега, перехваченное при записи тега в устройство;
- **Чтение и запись** – последнее значение тега, перехваченное при чтении или записи тега.

В правиле контроля процесса можно указать несколько условий. Для применения нескольких условий вы можете выбрать логические операции (И / ИЛИ) и указать их приоритеты, аналогичные скобкам в логических выражениях. Вы можете добавлять условия с помощью кнопки **Добавить условие**. Для удаления дополнительного условия используйте кнопку x слева от условия.

Правила, использующие Lua-скрипты

Функция в Lua-скрипте правила, описанная на языке Lua, вызывается при изменении значения какого-либо тега, используемого в функции. Впервые функция вызывается при получении всех значений тегов, используемых в функции.

Вы можете изменять функции в Lua-скриптах при выполнении следующих действий:

- Создание правила контроля процесса с Lua-скриптом

  Чтобы создать Lua-скрипт правила, выполните следующие действия:

  1. Выберите закладку **Контроль процесса**.
  2. Если список правил контроля процесса содержит группы, выберите группу, в которую нужно поместить новое правило. Вы можете выбрать саму группу или одно из существующих правил этой группы.
  3. Нажмите на кнопку **Добавить Lua-скрипт**.

     В нижней части закладки отобразится область редактирования Lua-скрипта.
  4. В области редактирования Lua-скрипта над полем ввода скрипта выберите вариант **Скрипт правила**.
  5. Выполните следующие действия:

     a. Введите имя и описание правила.

     b. Введите код скрипта на языке Lua.

     В поле ввода скрипта отображается шаблон функции на языке Lua с краткими комментариями. Чтобы открыть окно с подробными комментариями для создания скрипта, нажмите на кнопку вызова справки над полем ввода скрипта.

     c. Выберите или настройте тип регистрируемого события.
  6. Нажмите на кнопку **ОК**.

     Новый Lua-скрипт отобразится в списке.
  7. Чтобы изменения вступили в силу, примените политику безопасности.

- Создание или изменение глобального Lua-скрипта

  Чтобы изменить глобальный Lua-скрипт, выполните следующие действия:

  1. Выберите закладку **Контроль процесса**.
  2. Откройте область редактирования Lua-скрипта. Для этого вы можете использовать один из следующих способов:
     - Если список правил контроля процесса не содержит правил, содержащих Lua-скрипты, создайте новое правило с Lua-скриптом. Для этого выполните следующие действия:
       - Если список правил контроля процесса содержит группы, выберите группу, в которой будет создано правило, содержащее Lua-скрипт. Вы можете выбрать саму группу или одно из существующих правил этой группы.
       - Нажмите на кнопку **Добавить Lua-скрипт**.
     - Если список правил контроля процесса содержит хотя бы одно правило с Lua-скриптом, выполните следующие действия:
       - Выберите любое правило, содержащее Lua-скрипт.
       - Нажмите на кнопку **Изменить**.
  3. В области редактирования Lua-скрипта над полем ввода скрипта выберите вариант **Глобальный скрипт**.
  4. В поле ввода скрипта введите код скрипта на языке Lua.

     Чтобы открыть окно с комментариями для создания глобального скрипта, нажмите на кнопку вызова справки над полем ввода скрипта.
  5. Нажмите на кнопку **ОК**.
  6. Чтобы изменения вступили в силу, примените политику безопасности.

  Заданные глобальные переменные и функции глобального Lua-скрипта вы можете использовать при создании или изменении правил, содержащих Lua-скрипты.

- Изменение Lua-скрипта в правиле контроля процесса

Чтобы изменить Lua-скрипт правила, выполните следующие действия:

1. Выберите закладку **Контроль процесса**.
2. В списке правил контроля процесса выделите правило с Lua-скриптом, который вы хотите изменить.
3. Нажмите на кнопку **Изменить**.
   В нижней части закладки отобразится область редактирования Lua-скрипта.
4. В области редактирования Lua-скрипта над полем ввода скрипта выберите вариант **Скрипт правила**.
5. Выполните следующие действия:
   a. Введите имя и описание правила.
   b. Введите код скрипта на языке Lua.
      Чтобы открыть окно с подробными комментариями для создания скрипта, нажмите на кнопку вызова справки над полем ввода скрипта.
   c. Выберите или настройте тип регистрируемого события.
6. Нажмите на кнопку **ОК**.
7. Чтобы изменения вступили в силу, примените политику безопасности.

Сервер программы начнет регистрировать события в соответствии с изменениями в правиле.

Для описания тегов в коде функции используется выражение вида:

```
X = tag'имя_тега'[.R/.W/.RW],
```

где используются следующие значения модификатора: `.R` – тег перехвачен при чтении из устройства, `.W` – тег перехвачен при записи в устройство, `.RW` – любое последнее значение тега. Указывать модификатор не обязательно. Если модификатор не указан, то используется любое последнее значение тега.

При создании правила с помощью Lua-скрипта вы можете использовать дополнительные переменные с произвольными именем и значением.

Для добавления переменой используется функция:

```
_AddEventParam('имя_параметра', значение_параметра)
```

Добавленную переменную вы можете использовать в параметрах пользовательских типов событий. Добавленная переменная может быть использована в виде `$extra.<имя_параметра>.`

Вы можете использовать функции для добавления записи 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):

- `_WriteCriticalLog(аргумент_функции)` создает в журнале запись с уровнем *Критический*.
- `_WriteErrorLog(аргумент_функции)` создает в журнале запись с уровнем *Ошибка*.
- `_WriteWarningLog(аргумент_функции)` создает в журнале запись с уровнем *Предупреждение*.
- `_WriteInfoLog(аргумент_функции)` создает в журнале запись с уровнем *Информационный*.
- `_WriteDebugLog(аргумент_функции)` создает в журнале запись с уровнем *Отладочный*.
- `print(аргумент_функции1, аргумент_функции2,…)` создает в журнале запись с уровнем *Отладочный*, которая может содержать несколько аргументов функции. 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 в окне Параметры Сервера и сенсоров.

Создание группы в списке правил контроля процесса

Чтобы создать группу, выполните следующие действия:

1. Выберите закладку **Контроль процесса**.
2. Если новую группу нужно добавить в состав имеющейся группы, выберите группу, которая будет являться родительской.
3. Нажмите на кнопку **Добавить группу**.

   На экране отобразится окно **Имя группы**.
4. Введите имя группы.
5. Нажмите на кнопку **ОК**.

   Новая группа отобразится в списке.
6. При необходимости переместите группу в списке.

Перемещение элемента в списке правил контроля процесса

Чтобы переместить элемент списка, выполните следующие действия:

1. Выберите закладку **Контроль процесса**.
2. В списке правил контроля процесса выделите элемент, который вы хотите переместить.
3. Перетащите элемент мышью в нужное место списка.

Переименование элемента в списке правил контроля процесса

Чтобы переименовать элемент списка, выполните следующие действия:

1. Выберите закладку **Контроль процесса**.
2. В списке правил контроля процесса выделите элемент, который вы хотите изменить.
3. Нажмите на кнопку **Изменить**.
4. На экране отобразится область редактирования (если выбрано правило) или окно **Имя группы** (если выбрана группа).
5. Введите новое имя элемента.

6. Нажмите на кнопку **ОК**.

Удаление элемента в списке правил контроля процесса

Чтобы удалить элемент списка, выполните следующие действия:

1. Выберите закладку **Контроль процесса**.
2. В списке правил контроля процесса выберите элемент, который вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Откроется окно с запросом подтверждения.
4. Нажмите на кнопку **Да**.

Элемент будет удален из списка.

Поиск правил контроля процесса

Вы можете выполнять поиск правил контроля процесса и групп по значениям в графах **Имя** и **Описание**.

Чтобы найти нужные правила контроля процесса и группы, выполните следующие действия:

1. В правом верхнем углу области **Правила контроля процесса** введите поисковый запрос в поле **Поиск правил**. Поиск инициируется во время ввода символов.

   В списке правил контроля процесса отобразятся правила и группы, которые удовлетворяют условиям поиска.
2. Если вы хотите исключить группы из результатов поиска, снимите флажок **Показывать группы**.

Выделение тегов, используемых в правилах контроля процесса

Для просмотра тегов, используемых в правилах контроля процесса, вы можете выделять теги, которые связаны с выбранными правилами. В зависимости от выбранного элемента в списке правил контроля процесса, программа выделяет следующие теги:

- теги выбранного правила контроля процесса;
- теги правил выбранной группы.

Чтобы выделить в списке теги, которые используются в выбранном правиле или правилах выбранной группы,

выберите нужный элемент в списке правил контроля процесса (группу или отдельное правило).

В дереве **Устройства и теги** будут выделены все теги, связанные с выбранным элементом. Для выделения тегов используется светло-зеленый цвет. Чтобы отобразить выделенные теги на экране, раскройте соответствующие узлы дерева и при необходимости переместите ползунок справа от дерева по вертикальной оси.

Настройка событий

В Консоли программы вы можете настраивать типы регистрируемых событий Kaspersky Industrial CyberSecurity for Networks. При настройке вы можете создавать, изменять и удалять типы событий, а также настраивать передачу событий в сторонние системы.

Список типов регистрируемых событий отображается в Консоли Kaspersky Industrial CyberSecurity for Networks на закладке **Настройка событий**. Каждый тип события соответствует одной из используемых программой технологий.

При подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер возможность работы со списком типов событий недоступна.

Список типов событий входит в политику безопасности. Применять текущую политику безопасности на Сервере могут только пользователи с ролью Администратор. При этом возможности внесения изменений и сохранения политики безопасности в директории (в том числе с измененными параметрами для типов событий) доступны как пользователям с ролью Администратор, так и пользователям с ролью Оператор.

Список типов событий содержит системные и пользовательские типы событий. *Системные типы событий* создаются программой при установке и не могут быть удалены из списка. Программа использует системные типы событий для регистрации основных событий по технологии Контроль технологического процесса и для регистрации любых событий по другим технологиям. Вы можете создавать дополнительные типы событий для технологий Контроль технологического процесса и Внешние системы. Такие типы событий называются *пользовательскими типами событий*.

Для пользовательских типов событий доступны все возможности удаления, изменения параметров и выбора адресатов. Для системных типов событий доступны возможности выбора адресатов и изменения отдельных параметров регистрации.

С помощью пользовательских типов событий вы можете настроить получение событий от внешних систем. Для этого в Консоли программы нужно создать типы событий специально для получения от внешней системы. При создании типа события ему присваивается уникальный номер (этот номер сохраняется в качестве значения параметра **Код**). После этого во внешней системе нужно настроить отправку событий в программу с помощью методов Kaspersky Industrial CyberSecurity for Networks API. При отправке события в Kaspersky Industrial CyberSecurity for Networks внешняя система будет указывать номер типа события, заданный параметром **Код**. По этому номеру Сервер Kaspersky Industrial CyberSecurity for Networks определит тип события и зарегистрирует его как событие по технологии Внешние системы.

Для типов событий предусмотрены следующие параметры:

- **Код** – уникальный номер типа события, который будет отображаться в списке типов событий на закладке **Настройка событий**. В таблице зарегистрированных событий номер типа события отображается в графе **Тип события**. Номер типа события автоматически присваивается программой при создании типа события. Этот параметр невозможно изменить.

- **Уровень важности** – уровень важности, который будет указан для события при регистрации: *Критические*, *Важные* и *Информационные*. Параметр доступен для изменения только для пользовательских типов событий.

- **Технология** – технология регистрации события. Параметр доступен только для пользовательских типов событий. Можно указать технологию Контроль технологического процесса или Внешние системы.

- **Заголовок** – текст заголовка события. Отображается в списке типов событий на закладке **Настройка событий**. В таблице зарегистрированных событий заголовок типа события отображается в графе **Заголовок**. Также заголовки типов событий отображаются в блоке **События** в разделе **Мониторинг** веб-интерфейса программы. Параметр доступен для изменения только для пользовательских типов событий.

- **Описание** – дополнительный текст, который будет отображаться в таблице зарегистрированных событий в графе **Описание**. Параметр доступен для изменения только для пользовательских типов событий.

- **Сохранять трафик** – флажок, позволяющий включить / выключить автоматическое сохранение трафика, который был зафиксирован в системе до и после регистрации события. Трафик сохраняется в базе данных программы. Если автоматическое сохранение трафика включено, вы можете настроить параметры сохранения трафика по ссылке **Настроить**.

  > 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.

- **Время разрешения повтора** – максимальный период времени, по истечении которого разрешается повторная регистрация события. Если до истечения заданного периода времени снова 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.

  > Для зарегистрированных событий время разрешения повтора может наступить раньше заданного периода. Повторная регистрация события разрешается, если событию присвоен статус *Обработано*, а также если перезагружен компьютер, который выполняет функции Сервера.

Тексты заголовков и описаний в параметрах типов событий могут содержать переменные. При регистрации событий Сервер подставляет текущие значения переменных.

Вы можете просматривать зарегистрированные события при подключении к Серверу через веб-браузер.

Режимы группировки типов событий

Вы можете группировать список типов событий по следующим критериям:

- По технологии. Внутри каждой технологии элементы группируются по уровням важности.
- По важности. Внутри каждого уровня важности элементы группируются по технологиям.

По умолчанию группировка типов событий выключена.

Чтобы сгруппировать типы событий,

в панели инструментов закладки **Настройка событий** выберите нужный режим в раскрывающемся списке **Группировка**.

Поиск типов событий

Вы можете выполнять поиск кодов и заголовков в списке типов событий.

Чтобы найти нужный тип событий,

в панели инструментов закладки **Настройка событий** введите поисковый запрос в поле **Поиск типов событий**. Поиск инициируется во время ввода символов.

В списке типов событий отобразятся элементы, которые удовлетворяют условиям поиска (при поиске не учитываются значения параметра **Описание** в типах событий).

Создание типов событий

Вы можете создавать пользовательские типы событий для технологий Контроль технологического процесса и Внешние системы.

Созданные типы событий по технологии Внешние системы могут использоваться для получения событий в Kaspersky Industrial CyberSecurity for Networks от внешних систем.

Чтобы создать тип события, выполните следующие действия:

1. На закладке **Настройка событий** нажмите на кнопку **Добавить**.

   В нижней части закладки **Настройка событий** отобразится область редактирования параметров.

2. Выполните следующие действия:

   a. Задайте уровень важности события: *Критические*, *Важные* или *Информационные*.

   b. Выберите технологию регистрации события.

   c. Введите заголовок события.

   d. Введите описание события.

   e. При необходимости включите и настройте сохранение трафика.

   f. При необходимости измените время разрешения повтора события.

3. Нажмите на кнопку **ОК**.

   Новый тип события отобразится в списке.

Вы можете выбрать новый тип события при создании правила контроля процесса на закладке **Контроль процесса**. События нового типа будут регистрироваться после применения политики безопасности на Сервере

Изменение типов событий

Чтобы изменить тип события, выполните следующие действия:

1. На закладке **Настройка событий** выберите нужный тип события и нажмите на кнопку **Изменить**.

   Откроется окно с предупреждением.

2. Нажмите на кнопку **ОК**.

   В нижней части закладки **Настройка событий** отобразится область редактирования параметров.

3. Выполните следующие действия:

   a. Задайте уровень важности события: *Критические*, *Важные* или *Информационные* (доступно только для пользовательских событий).

   b. Введите заголовок события (доступно только для пользовательских событий).

   c. Введите описание события (доступно только для пользовательских событий).

   d. Настройте сохранение трафика.

   e. Настройте время разрешения повтора события.

4. Нажмите на кнопку **ОК**.

Изменение уровня важности или заголовка события отобразится в списке типов событий.

Настройка автоматического сохранения трафика при регистрации событий

При создании или изменении типов событий вы можете включить 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. Параметры сохранения трафика определяют количество сохраняемых сетевых пакетов и ограничения по времени.

Если автоматическое сохранение трафика выключено для типа события, 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 системных типов событий, которым присвоены коды 8000000000, 8000000001, 8000000002 и 8000000003), 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.

Включить и настроить сохранение трафика для инцидентов достаточно для одного из типов событий с кодами 8000000000, 8000000001, 8000000002 или 8000000003. Программа автоматически применяет изменения, сделанные с одним из этих типов событий, к остальным трем типам.

Чтобы настроить параметры сохранения трафика для типа события, выполните следующие действия:

1. В области редактирования параметров типа события установите флажок **Сохранять трафик**.

2. Откройте окно **Сохранение трафика для события** по ссылке **Настроить**.

3. В окне **Сохранение трафика для события** настройте сохранение трафика до момента регистрации события. Для этого укажите нужные значения в полях **Пакетов до наступления события** и / или **Миллисекунд до наступления события**. 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.

4. Настройте сохранение трафика после момента регистрации события. Для этого укажите нужные значения в полях **Пакетов после наступления события** и / или **Миллисекунд после наступления события**. 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.

5. Нажмите на кнопку **ОК**.

Удаление типов событий

Вы можете удалить из списка пользовательские типы событий, которые не связаны с правилами контроля процесса. Удаление системных типов событий недоступно.

Чтобы удалить тип события, выполните следующие действия:

1. На закладке **Настройка событий** выберите тип события для удаления.
2. Нажмите на кнопку **Удалить**.

   На экране отобразится запрос на подтверждение удаления.
3. В окне запроса нажмите на кнопку **ОК**.

О передаче событий в сторонние системы

При настройке типов событий вы можете указать сторонние системы, в которые будут передаваться зарегистрированные события. Такие сторонние системы называются *адресатами*. Kaspersky Industrial CyberSecurity for Networks может передавать информацию о событиях одновременно нескольким адресатам.

Kaspersky Industrial CyberSecurity for Networks может передавать информацию о событиях следующим адресатам:

- SIEM-сервер;
- Syslog-сервер;
- электронная почта;
- Kaspersky Security Center.

Для передачи событий в Kaspersky Security Center на Сервере Kaspersky Industrial CyberSecurity for Networks требуется добавить функциональность взаимодействия программы с Kaspersky Security Center. Вы можете добавить эту функциональность при установке или переустановке Kaspersky Industrial CyberSecurity for Networks.

> Для передачи событий в другие сторонние системы добавлять функциональность взаимодействия программы с Kaspersky Security Center не требуется.

Для адресатов предусмотрены следующие параметры:

- **Имя адресата** – имя, которое отображается в заголовке графы на закладке **Настройка событий**.
- **Тип адресата** – выбранный тип адресата. В зависимости от выбранного типа вы можете настроить следующие дополнительные параметры:
  - Для SIEM-сервера и Syslog-сервера: адрес и порт сервера.

Содержание и порядок сведений о событиях, передаваемых адресатам SIEM-сервер и Syslog-сервер, могут отличаться от содержания и порядка сведений, отображаемых в таблице событий.

- Для электронной почты: параметры уведомлений.

  Уведомление – это сообщение электронной почты, которое содержит события Kaspersky Industrial CyberSecurity for Networks. К уведомлениям применяются следующие параметры:

  - Адрес отправителя уведомления.
  - Адрес получателя уведомления. Несколько адресов разделяются запятыми.
  - Тема уведомления.
  - Шаблон события – шаблон текстового описания для событий в уведомлении. Шаблон определяет содержание и порядок отображения сведений о каждом событии в уведомлении. Шаблон составляется с использованием переменных.
  - Текст уведомления. В тексте уведомления вы можете указать переменную `$events`, которая при создании уведомления Сервером заменяется списком строк с информацией о событиях. Каждая строка соответствует шаблону события с текущими значениями переменных.
  - Количество уведомлений в сутки. Определяет максимальное количество уведомлений за сутки, начиная с нуля часов в часовом поясе Сервера. Если уведомлений больше, получателям отправляется сообщение электронной почты о превышении максимального количества уведомлений о событиях. В этом случае новые уведомления отправляться не будут до конца текущих суток.
  - Количество событий в каждом уведомлении. Определяет максимальное количество событий, сведения о которых можно поместить в одно уведомление. Если событий больше, то формируется два или более уведомлений с тем же ограничением (в пределах суточного ограничения).

- Для Kaspersky Security Center: количество передаваемых событий в сутки. Параметр определяет максимальное количество передаваемых событий за сутки, начиная с нуля часов в часовом поясе Сервера. Если событий для передачи больше, в Kaspersky Security Center не отправляются остальные события, регистрируемые до конца текущих суток.

Параметры, определяющие максимальное количество передаваемых событий, применяются к событиям, зарегистрированным в Kaspersky Industrial CyberSecurity for Networks. Если в каком-либо событии указаны сведения о нескольких сетевых взаимодействиях, это событие преобразуется для адресата в отдельные записи о событиях (по одному событию на каждое сетевое взаимодействие). Поэтому список событий для адресата может содержать больше событий, чем задано параметром, который определяет максимальное количество событий.

Добавление адресата

Чтобы добавить адресата, выполните следующие действия:

1. В Консоли программы выберите закладку **Настройка событий**.
2. Нажмите на кнопку **Задать адресата**.

   На экране отобразится окно **Адресаты**.

3. Выполните следующие действия:

   a. Введите имя адресата.

   b. Выберите тип адресата и задайте остальные параметры отправки событий.

4. Нажмите на кнопку **ОК**.

На закладке **Настройка событий** отобразится графа, в заголовке которой будет указано имя добавленного адресата.

Изменение параметров адресата

Чтобы изменить параметры адресата, выполните следующие действия:

1. В Консоли программы выберите закладку **Настройка событий**.
2. Нажмите на заголовок графы с именем адресата, параметры которого вы хотите изменить.

   На экране отобразится окно **Адресаты**.
3. При необходимости выполните следующие действия:

   a. Введите имя адресата.

   b. Задайте параметры отправки событий.
4. Нажмите на кнопку **ОК**.

Если вы изменили имя адресата, новое имя отобразится в заголовке графы на закладке **Настройка событий**.

Настройка передачи событий в сторонние системы

Чтобы настроить передачу событий Kaspersky Industrial CyberSecurity for Networks в сторонние системы, выполните следующие действия:

1. В Консоли программы выберите закладку **Настройка событий**.
2. Убедитесь, что в списке типов событий отображаются адресаты, которым вы хотите передавать события программы.

   Если нужный адресат отсутствует, добавьте его в список.
3. В строках типов событий или групп (подгрупп) типов событий установите флажки для нужных адресатов.

Программа будет отправлять адресатам события выбранных типов после применения политики безопасности на Сервере.

Удаление адресата

Чтобы удалить адресата, выполните следующие действия:

1. В Консоли программы выберите закладку **Настройка событий**.
2. Нажмите на заголовок графы с именем адресата, которого вы хотите удалить.

   На экране отобразится окно **Адресаты**.
3. Нажмите на кнопку **Удалить адресата**.

Переменные Kaspersky Industrial CyberSecurity for Networks для настройки событий

Вы можете использовать переменные Kaspersky Industrial CyberSecurity for Networks в следующих случаях:

- при создании и изменении пользовательских типов событий;
- при настройке параметров передачи событий по электронной почте.

Вместо указанных переменных при регистрации или передаче события Сервер автоматически подставляет текущие значения параметров.

В параметрах пользовательских типов событий для полей ввода **Заголовок** и **Описание** вы можете использовать следующие переменные:

- `$communications` – строки описания сетевых взаимодействий (по одной строке на каждое сетевое взаимодействие) с указанием протокола и адресов отправителя и получателя сетевого пакета;
- `$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);
- `$event_type_id` – код типа события;
- `$monitoring_point` – имя точки мониторинга, трафик с которой вызвал регистрацию события;
- `$occurred` – дата и время регистрации события;
- `$protocol` – название протокола прикладного уровня, при отслеживании которого зарегистрировано событие;
- `$src_address` – адрес отправителя сетевого пакета (в зависимости от доступных в протоколе данных это могут быть IP-адрес, номер порта, MAC-адрес и / или другие адресные данные);
- `$tags` – список всех имен и значений тегов, участвующих в правиле контроля процесса;
- `$technology_rule` – имя правила контроля процесса, по которому регистрируется событие;
- `$top_level_protocol` – название протокола верхнего уровня;

- `$extra.<paramName>` – дополнительная переменная, добавленная с помощью функции AddEventParam для внешней системы или Lua-скрипта.

В параметрах адресата Электронная почта для поля ввода **Шаблон события** вы можете использовать следующие переменные:

- `$closed` – дата и время присвоения статуса *Обработано* или дата и время разрешения повтора события (для событий, не являющихся инцидентами), либо дата и время регистрации последнего события, включенного в инцидент (для инцидентов);
- `$communications` – строки описания сетевых взаимодействий (по одной строке на каждое сетевое взаимодействие) с указанием протокола и адресов отправителя и получателя сетевого пакета;
- `$count` – количество срабатываний события или инцидента;
- `$description` – описание события;
- `$event_id` – уникальный идентификатор зарегистрированного события;
- `$event_type_id` – код типа события;
- `$monitoring_point` – имя точки мониторинга, трафик с которой вызвал регистрацию события;
- `$occurred` – дата и время регистрации события;
- `$severity` – уровень важности события;
- `$technology` – технология, к которой относится событие;
- `$technology_rule` – имя правила, по которому регистрируется событие;
- `$title` – заголовок события.

В параметрах адресата Электронная почта для поля ввода **Текст уведомления** вы можете использовать только переменную `$events`. Переменная заменяется списком строк с информацией о событиях. Каждая строка будет соответствовать событию с текущими значениями переменных из поля **Шаблон события**.

Чтобы вставить переменную в поле ввода, выполните следующие действия:

1. Установите курсор в нужное место поля ввода, в котором вы хотите использовать переменную.
2. Нажмите на кнопку **Добавить переменную** или введите символ $ (от предыдущего слова символ $ нужно отделить пробелом).

   В поле ввода рядом с курсором отобразится раскрывающийся список с доступными переменными.
3. Выберите нужную переменную из раскрывающегося списка.

Переменная будет добавлена в поле ввода и выделена специальным шрифтом.

Контроль устройств

Kaspersky Industrial CyberSecurity for Networks позволяет контролировать устройства, подключенные к промышленной сети. Для контроля устройств в программе формируется таблица устройств.

Таблица устройств содержит сведения об устройствах, полученные автоматически при анализе трафика или указанные вручную.

Автоматическое получение и обновление поддерживается для сведений, которые можно определить при анализе трафика (например, адресная информация устройства). Для обнаружения активности устройств и автоматического обновления сведений должны быть включены соответствующие методы по технологии Контроль устройств. 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 требуется указать вручную, для них не предусмотрено автоматическое обновление. Такие сведения позволяют сохранить в таблице специфическую информацию об устройствах, 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.

Сведения из таблицы устройств хранятся на Сервере и не зависят от политики безопасности, которая загружена в Консоль или применена на Сервере. Однако устройства для контроля процесса, сохраненные в политике безопасности, после применения политики на Сервере автоматически добавляются в таблицу устройств (или обновляется адресная информация ранее добавленных устройств).

Вы можете просматривать и изменять сведения об устройствах в разделе **Устройства** 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 сети.

Методы и режимы контроля устройств

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 на основе полученных данных о взаимодействиях устройств.
- Контроль проектов ПЛК. Этот метод позволяет обнаруживать в трафике информацию о проектах ПЛК, сохранять эту информацию в программе и сравнивать с ранее полученной информацией.

Вы можете включать и выключать применение методов контроля устройств по отдельности.

Для методов контроля 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 методами обнаружения сведений об устройствах и контроля проектов ПЛК.
- 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 режиме обучения программа присваивает статус *Разрешенное* всем обнаруженным устройствам. Программа не регистрирует события при обнаружении активности устройств или при автоматическом обновлении сведений об устройствах.

Режим обучения контроля устройств 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.

В режиме наблюдения (при включенном методе обнаружения активности устройств) программа присваивает статус *Неразрешенное* всем устройствам, которые проявили активность и являются либо неизвестными программе, либо устройствами со статусом *Неиспользуемое*. Программа присваивает статус *Неиспользуемое* устройствам, которые длительное время не проявляли активность и сведения о которых не изменялись (30 дней и более).

При включенном методе обнаружения сведений об устройствах программа автоматически обновляет сведения об устройствах. Например, программа может автоматически обновлять название операционной системы, установленной на устройстве, по мере обнаружения уточняющих данных в трафике этого устройства. Обновляются те сведения, для которых включено автоматическое изменение в параметрах устройств.

Для автоматического получения сведений об устройствах программа анализирует трафик промышленной сети по *правилам определения сведений об устройствах и протоколов взаимодействия устройств*. Эти правила встроены в программу и применяются независимо от политики безопасности, которая загружена в Консоль или применена на Сервере.

После установки программы используются исходные правила определения сведений об устройствах и протоколов взаимодействия устройств. В большинстве случаев правила выдают верные результаты. Однако возможны ситуации с некорректным определением сведений из-за технических особенностей реализации устройств (например, определение категорий некоторых устройств). Для повышения точности определения специалисты "Лаборатории Касперского" регулярно обновляют базы с наборами правил. Вы можете обновлять правила, устанавливая обновления.

В режиме наблюдения программа регистрирует соответствующие события по технологии Контроль устройств. 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.

При включенном методе контроля проектов ПЛК программа может регистрировать большое количество событий, связанных с обнаружением операций чтения и записи проектов / 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.

О контроле 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:

- Schneider Electric серии Modicon: M580, M340;
- Siemens SIMATIC серий S7-300, S7-400.

Для контроля чтения и записи проектов ПЛК не требуется добавлять устройства в список устройств для контроля процесса. Контроль чтения и записи проектов ПЛК осуществляется для всех обнаруженных устройств указанных 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 устройств. 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 из 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 Консоли программы на закладке Настройка событий.

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-браузер.

Выбор применяемых методов и изменение режима контроля устройств

Управлять методами и режимами контроля устройств могут только пользователи с ролью Администратор.

Чтобы включить или выключить применение методов контроля устройств, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Параметры** и перейдите на закладку **Технологии**.
3. Включите или выключите применение методов контроля устройств, используя следующие переключатели:
   - **Обнаружение активности устройств**.
   - **Обнаружение сведений об устройствах**.
   - **Контроль проектов ПЛК**.
4. После включения или выключения метода дождитесь перевода переключателя в нужное состояние (*Включено* или *Выключено*).

   Процесс занимает некоторое время, переключатель при этом будет недоступен. Дождитесь включения или выключения метода.
5. Если включен метод обнаружения активности устройств, выберите нужный режим контроля устройств с применением метода. Для этого в раскрывающемся списке справа от названия метода выберите одно из следующих значений:

- **Обучение** – для применения метода в режиме обучения.
- **Наблюдение** – для применения метода в режиме наблюдения.

6. После выбора режима дождитесь появления названия этого режима в поле раскрывающегося списка.

   Процесс занимает некоторое время, при этом в раскрывающемся списке отображается статус *Изменение*. Дождитесь включения выбранного режима.

Таблица устройств

Для контроля устройств в программе формируется таблица устройств. Все устройства, присутствующие в таблице, считаются известными программе.

Для таблицы устройств действуют следующие ограничения по количеству элементов:

- Суммарное количество устройств со статусами *Разрешенное* и *Неразрешенное* – не более 1000.

  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 1000.

  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, вы можете указать MAC- и / или IP-адреса для сетевых интерфейсов устройства. Для устройства может быть указано до 64 сетевых интерфейсов.

- **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.
  - **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** – признак наличия событий, связанных с устройством. В зависимости от уровней важности событий, предусмотрены следующие состояния:
  - **Критические события**. Есть необработанные события с уровнем важности *Критические*.
  - **Важные события**. Есть необработанные события с уровнем важности *Важные* и при этом нет необработанных событий с уровнем важности *Критические*.
  - **ОК**. Нет необработанных событий или есть только события с уровнем важности *Информационные*.
- **Последнее появление** – дата и время последней зафиксированной активности устройства.
- **Последнее изменение** – дата и время последнего изменения сведений об устройстве.
- **Дата создания** – дата и время добавления устройства в таблицу устройств.
- **ОС** – название операционной системы, установленной на устройстве.
- **Производитель** – название производителя.
- **Модель** – информация о модели.
- **Сетевое имя** – имя, под которым устройство представлено в сети.
- **Метки** – список меток, назначенных устройству.

Просмотр таблицы устройств

Таблица устройств отображается в разделе **Устройства** веб-интерфейса программы. В таблице устройств представлены основные сведения об устройствах, известных программе.

При просмотре таблицы устройств вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице устройств

  Чтобы настроить список отображаемых в таблице граф, выполните следующие действия:

  1. В разделе **Устройства** веб-интерфейса программы нажмите на кнопку **Настроить таблицу**.

     Откроется окно для настройки отображения таблицы устройств.

  2. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр.

  3. Если вы хотите изменить порядок отображения граф, выделите название графы, которую требуется разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

  Выбранные графы отобразятся в указанном вами порядке в таблице устройств.

- Фильтрация по графам таблицы

*Чтобы отфильтровать устройства по графе **Статус**, **Категория** или **Состояние безопасности**, выполните следующие действия:*

1. В разделе **Устройства** нажмите на значок фильтрации в нужной графе таблицы.

   При фильтрации по состояниям безопасности устройств вы также можете воспользоваться соответствующими кнопками в панели инструментов.

   Откроется окно фильтрации.

2. Установите флажки напротив значений, по которым вы хотите выполнить фильтрацию. Вы можете снять или удалить все флажки по ссылке, которая отображается в верхней части окна фильтрации.

3. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать устройства по графе **ID устройства**, **ОС**, **Производитель**, **Модель** или **Сетевое имя**, выполните следующие действия:*

1. В разделе **Устройства** нажмите на значок фильтрации в нужной графе таблицы.

   Откроется окно фильтрации.

2. В полях **Включая** и **Исключая** введите значения для устройств, которые вы хотите включить в фильтрацию и / или исключить из фильтрации.

3. Если вы хотите применить несколько условий фильтрации, объединенных логическим оператором ИЛИ, в окне фильтрации выбранной графы нажмите на кнопку **Добавить условие** и введите условие в открывшемся поле.

4. Если вы хотите удалить одно из созданных условий фильтрации, в окне фильтрации выбранной графы нажмите на значок .

5. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать устройства по графе **Адресная информация**, выполните следующие действия:*

1. В разделе **Устройства** нажмите на значок фильтрации в графе **Адресная информация**.

   Откроется окно фильтрации.

2. В полях **Включая** и **Исключая** выберите в раскрывающихся списках типы адресов для устройств, которые вы хотите включить в фильтрацию и / или исключить из фильтрации. Вы можете выбрать следующие типы адресов:

   - IP-адрес.
   - MAC-адрес.
   - **Комплексный** – если вы хотите указать несколько адресов разных типов, объединенных логическим оператором И. Для добавления адресов разных типов используйте кнопку **Добавить условие (И)**.

3. Если вы хотите применить несколько условий фильтрации по типам адресов, объединенных логическим оператором ИЛИ, в окне фильтрации нажмите на кнопку **Добавить условие (ИЛИ)** и выберите нужные типы адресов.

4. Если вы хотите удалить одно из созданных условий фильтрации, в окне фильтрации нажмите на значок , который расположен справа от поля с раскрывающимся списком.

5. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать устройства по графе **Группа**, выполните следующие действия:*

1. В разделе **Устройства** нажмите на значок фильтрации в графе **Группа**.

   Откроется окно фильтрации.

2. Нажмите на значок в правой части поля для указания группы.

   Появится окно **Выбор группы в дереве**.

3. В дереве групп устройств выберите нужную группу и нажмите на кнопку **Выбрать**.

   Путь к выбранной группе появится в поле в окне фильтрации.

4. Если вы хотите применить несколько условий фильтрации, объединенных логическим оператором ИЛИ, в окне фильтрации нажмите на кнопку **Добавить условие** и укажите другую группу в открывшемся поле.

5. Если вы хотите удалить одно из созданных условий фильтрации, в окне фильтрации нажмите на значок .

6. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать устройства по графе **Последнее появление**, **Последнее изменение** или **Дата создания**, выполните следующие действия:*

1. В разделе **Устройства** нажмите на значок фильтрации в нужной графе таблицы.

   Откроется календарь.

2. В календаре задайте дату и время 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.ГГ чч:мм:сс.

3. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать устройства по графе **Метки**, выполните следующие действия:*

1. В разделе **Устройства** нажмите на значок фильтрации в графе **Метки**.

   Откроется окно фильтрации.

2. Введите одну или несколько меток, объединенных логическим оператором И.

3. Если вы хотите применить несколько условий фильтрации, объединенных логическим оператором ИЛИ, в окне фильтрации нажмите на кнопку **Добавить условие (ИЛИ)** и введите нужные метки (несколько меток в этом условии также будут объединены логическим оператором И).

4. Если вы хотите удалить лишние метки в окне фильтрации, вы можете:

   - удалить лишние метки с помощью значка ✕ рядом с названиями меток;
   - удалить одно из созданных условий фильтрации с помощью значка 🗑, который расположен справа от поля.

5. Нажмите на кнопку **ОК**.

- ## Поиск устройств

Чтобы найти нужные устройства,

в разделе **Устройства** введите поисковый запрос в поле **Поиск устройств**. Поиск инициируется во время ввода символов.

В таблице устройств отобразятся устройства, которые удовлетворяют условиям поиска.

Поиск выполняется по всем графам, кроме граф **ID устройств**, **Статус**, **Категория**, **Состояние безопасности**, **Последнее появление**, **Последнее изменение** и **Дата создания**. Поиск также выполняется по значениям пользовательских полей для устройств.

- ## Сброс заданных параметров фильтрации и поиска

Чтобы сбросить заданные параметры фильтрации и поиска в таблице устройств,

в панели инструментов в разделе **Устройства** нажмите на кнопку **Очистить фильтр** (кнопка отображается, если заданы параметры фильтрации или поиска).

- ## Сортировка устройств

Чтобы отсортировать устройства, выполните следующие действия:

1. В разделе **Устройства** нажмите на заголовок графы, по которой вы хотите выполнить сортировку.

2. При сортировке устройств по графе **Адресная информация** в раскрывающемся списке заголовка графы выберите параметр, по которому будет выполняться сортировка.

   В зависимости от выбранных значений для отображения в графе **Адресная информация**, вы можете выбрать один из следующих элементов:

   - IP-адрес.
   - MAC-адрес.

3. Если требуется отсортировать таблицу по нескольким графам, нажмите на клавишу **SHIFT** и, удерживая ее нажатой, нажмите на заголовки граф, по которым нужно выполнить сортировку.

Таблица будет отсортирована по выбранной графе. При сортировке по нескольким графам строки таблицы сортируются в соответствии с последовательностью выбора граф. Рядом с заголовками граф, по которым выполнена сортировка, отображаются значки, показывающие текущий порядок сортировки: по возрастанию или по убыванию значений.

- ## Обновление таблицы устройств

Сведения об устройствах могут быть изменены на Сервере в то время, когда вы просматриваете таблицу устройств (например, другим пользователем, который выполнил подключение к Серверу).

Для поддержания таблицы устройств в актуальном состоянии вы можете включить автоматическое обновление таблицы.

Чтобы включить или выключить автоматическое обновление таблицы устройств,

в панели инструментов в разделе **Устройства** используйте переключатель **Обновлять автоматически**.

Выбор устройств в таблице устройств

В таблице устройств вы можете выбирать устройства для просмотра сведений и для работы с этими устройствами. При выборе устройств в правой части окна веб-интерфейса появляется область деталей.

Чтобы выбрать нужные устройства в таблице, выполните одно из следующих действий:

- Если вы хотите выбрать одно устройство, установите флажок напротив этого устройства или выберите устройство с помощью мыши.
- Если вы хотите выбрать несколько устройств, установите флажки напротив нужных устройств или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**.
- Если вы хотите выбрать все устройства, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:
  - выберите любое устройств в таблице и нажмите комбинацию клавиш **CTRL+A**;
  - установите флажок в заголовке левой крайней графы таблицы.

При выборе более одного устройства в области деталей отображается количественное распределение выбранных устройств по категориям. Если среди выбранных устройств присутствуют устройства с различными категориями, вы можете исключить устройства одной из категорий. Для этого нужно снять флажок рядом с названием этой категории.

В заголовке левой крайней графы таблицы отображается флажок выбора устройств. В зависимости от количества выбранных устройств флажок может быть в одном из следующих состояний:

- ☐ – в таблице не выполнялся выбор всех устройств, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбрано одно устройство или несколько устройств с помощью флажков напротив устройств или с использованием клавиш **CTRL** или **SHIFT**.
- ☑ – в таблице выбраны все устройства, удовлетворяющие текущим параметрам фильтрации и поиска.
- ▣ – в таблице были выбраны все устройства, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых устройств были сняты флажки. Это состояние сохраняется и в случае, если флажки сняты для всех устройств, выбранных таким способом (из-за того, что количество выбранных устройств может измениться).

Если выбраны все устройства, удовлетворяющие параметрам фильтрации и поиска, количество выбранных устройств может автоматически изменяться. Например, состав устройств в таблице может быть изменен пользователем программы в другом сеансе подключения или при автоматическом добавлении устройств. Рекомендуется настраивать параметры фильтрации и поиска таким образом, чтобы в выборку попали только нужные устройства (например, перед выбором всех устройств вы можете отфильтровать устройства по идентификаторам).

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 устройств:

- 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 устройств.

- Обнаружение сведений об устройствах. При использовании этого метода программа обновляет сведения об известных устройствах на основе полученных данных из трафика.

При автоматическом добавлении для каждого нового устройства программа задает имя по шаблону: **Устройство <значение внутреннего счетчика устройств>**. При этом значение внутреннего счетчика в имени устройства может не совпадать с идентификатором устройства, который отображается в графе **ID устройства**. Если включено применение метода обнаружения сведений об устройствах, при получении сведений об устройстве программа может обновить его имя.

При обновлении имени устройства программа заменяет текущее имя устройства на полученное название модели устройства или его сетевое имя (под которым оно представлено в сети). Причем сетевое имя устройства имеет приоритет при актуализации.

Для актуализации имени устройства по изменениям в названии модели и / или в сетевом имени требуется включить автоматическое изменение этих сведений в параметрах устройства.

О дереве групп устройств

Дерево групп устройств предназначено для распределения устройств в соответствии с их назначением, размещением или по каким-либо другим произвольным признакам. Например, вы можете распределить устройства по группам, соответствующим местоположению устройств в производственной структуре предприятия.

Дерево групп устройств поддерживает до шести уровней вложенности. Вы можете добавлять устройства в группы на любом уровне иерархии. При этом каждое устройство может быть добавлено только в одну из групп дерева.

Для дерева действует ограничение по количеству групп – не более 1000.

Вы можете указывать группы для устройств при добавлении устройства вручную, при изменении сведений об устройстве или при выборе нескольких устройств в таблице. Если устройство не включено ни в одну из групп, это устройство считается относящимся к верхнему уровню иерархии в дереве. Устройства, автоматически добавленные в таблицу, по умолчанию не включаются в группы.

Узнать, в какие группы входят устройства, вы можете при просмотре таблицы устройств. Пути к группам указаны в графе **Группа**.

Формирование дерева групп устройств

Вы можете формировать дерево групп устройств при работе с таблицей устройств или с картой сети. Формирование дерева выполняется в окне **Формирование дерева групп** или **Выбор группы в дереве**.

Формировать дерево групп устройств могут только пользователи с ролью Администратор.

*Чтобы открыть окно **Формирование дерева групп**, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. В разделе **Устройства** или в разделе **Карта сети** нажмите на кнопку **Настроить группы**.

Изменения, сделанные в окне **Формирование дерева групп**, применяются сразу.

Для выбора группы при добавлении устройств в группы или при фильтрации по графе **Группа** открывается окно **Выбор группы в дереве**. В этом окне вам также доступны функции по формированию дерева групп устройств.

Для формирования дерева групп устройств вы можете использовать следующие функции:

- Добавление группы

  Чтобы добавить группу в дерево групп устройств, выполните следующие действия:

  1. В окне **Формирование дерева групп** или **Выбор группы в дереве** выберите группу, внутри которой или рядом с которой вы хотите добавить новую группу. Если дерево пустое или вы хотите добавить группу на верхнем уровне иерархии, пропустите это действие и перейдите к следующему.

  2. В зависимости от того, где вы хотите добавить новую группу, выполните соответствующие действия:

     - если вы хотите добавить дочернюю группу к текущей выбранной группе, нажмите на кнопку **Добавить** или на клавишу **INSERT**;
     - если вы хотите добавить группу на том же уровне, что и текущая выбранная группа, нажмите на клавишу **ENTER**;
     - если в дереве не выделена ни одна группа и вы хотите добавить группу на верхнем уровне иерархии, нажмите на кнопку **Добавить** или на любую из клавиш **INSERT** или **ENTER**.

  3. 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).

  4. Нажмите на значок ✓ справа от поля ввода.

- Переименование группы

  Чтобы переименовать группу в дереве групп устройств, выполните следующие действия:

  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 группы

При удалении группы не удаляются устройства, добавленные в эту группу и в ее дочерние группы. Эти устройства переводятся на верхний уровень иерархии дерева устройств (в сведениях об этих устройствах удаляется информация о включении в группы).

Чтобы удалить группу в дереве групп устройств, выполните следующие действия:

1. В окне **Формирование дерева групп** или **Выбор группы в дереве** выберите группу, которую вы хотите удалить.
2. Нажмите на значок .
   Откроется окно с запросом подтверждения.
3. В окне запроса подтвердите удаление группы.

Выбранная группа и ее дочерние группы будут удалены из дерева.

- Перемещение группы

Чтобы переместить группу в дереве групп устройств, выполните следующие действия:

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

Чтобы найти нужные группы в дереве групп устройств,

в окне **Формирование дерева групп** или **Выбор группы в дереве** введите поисковый запрос в поле **Поиск групп**. Поиск инициируется во время ввода символов.

В дереве групп устройств отобразятся группы, которые удовлетворяют условиям поиска. 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.

Чтобы обновить дерево групп устройств,

в окне **Формирование дерева групп** или **Выбор группы в дереве** нажмите на значок .

Добавление устройств вручную

Вы можете вручную добавить новое устройство в таблицу устройств. Для добавляемого устройства требуется указать уникальные MAC- и / или IP-адреса.

Добавлять устройства вручную могут только пользователи с ролью Администратор.

Добавлять устройств можно следующими способами:

- Добавление устройства при работе с таблицей устройств

Чтобы добавить устройство вручную при работе с таблицей устройств, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. В разделе **Устройства** нажмите на кнопку **Добавить устройство**.

   В правой части окна веб-интерфейса появится область деталей.

3. На закладке **Адреса** в области деталей укажите уникальные MAC- и / или IP-адреса устройства.

4. 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.

5. 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 кнопку **Удалить интерфейс**, которая расположена 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.

6. На закладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.

7. На закладках **Адреса** и **Параметры** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте переключатели **Обновлять автоматически**, расположенные над полями с возможностью автоматического изменения.

8. На закладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей.

9. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Закладка с параметрами, требующими ввода правильных значений, отмечена значком .

В таблице устройств появится новое устройство со статусом *Разрешенное*.

- Добавление устройства на основе узла карты сети

При работе с картой сети вы можете добавить новое устройство в таблицу устройств на основе узла, который представляет неизвестное программе устройство.

Чтобы добавить узел неизвестного устройства в таблицу устройств, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Устройства** и перейдите на закладку **Карта сети**.

3. Выберите нужный узел, представляющий неизвестное программе устройство.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Добавить в таблицу устройств**.

   В области деталей появятся закладки для настройки параметров нового устройства.

5. 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.

6. Нажмите на кнопку **Сохранить**.

В таблице устройств появится новое устройство со статусом *Разрешенное*. Узел на карте сети, который ранее представлял неизвестное программе устройство, будет представлять известное программе устройство.

Объединение 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. При этом, если возникают конфликты заданных значений в сведениях об устройствах, в объединенном устройстве сохранятся те значения, которые были заданы для устройства с IP-адресом. Поэтому 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.

При объединении узлов суммарное количество сетевых интерфейсов нового устройства должно быть не более 64.

Объединять устройства вручную может только пользователь с ролью Администратор.

Объединять устройств можно следующими способами:

- Объединение устройств при работе с таблицей устройств

  Чтобы объединить несколько устройств вручную при работе с таблицей устройств, выполните следующие действия:

  1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
  2. Выберите раздел **Устройства**.
  3. В таблице устройств выберите устройства, которые вы хотите объединить.

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

     В области деталей появятся закладки для настройки параметров нового устройства.
  5. Проверьте и при необходимости измените параметры нового устройства:
     - На закладке **Адреса** в области деталей MAC- и IP-адреса выбранных устройств распределяются по отдельным сетевым интерфейсам. При необходимости измените значения адресов и имена сетевых интерфейсов.
     - На закладке **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.
     - На закладке **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*.

- Объединение устройств при работе с картой сети

При работе с картой сети вы можете объединить несколько узлов на карте сети 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 карте сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. В разделе **Карта сети** 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.

3. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.

4. Нажмите на кнопку **Объединить устройства**.

   В области деталей появятся закладки для настройки параметров нового устройства.

5. Проверьте и при необходимости измените параметры нового устройства:

   - На закладке **Адреса** в области деталей MAC- и IP-адреса выбранных устройств распределяются по отдельным сетевым интерфейсам. При необходимости измените значения адресов и имена сетевых интерфейсов.
   - На закладке **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.
   - На закладке **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

Вы можете удалить одно или несколько устройств из таблицы устройств.

Удалять устройства может только пользователь 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 устройств).

Удалять устройства можно следующими способами:

- Удаление устройств при работе с таблицей устройств

Чтобы удалить устройства при работе с таблицей устройств, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Устройства**.
3. В таблице устройств выберите устройства, которые вы хотите удалить.
   В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить устройство** (если выбрано одно устройство) или **Удалить устройства** (если выбрано несколько устройств).
   Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.

- Удаление устройств при работе с картой сети

При работе с картой сети вы можете удалять устройства из таблицы устройств, используя узлы на карте сети, представляющие известные программе устройства.

Чтобы удалить устройство при работе с картой сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Карта сети** выберите один или несколько узлов, представляющих известные программе устройства.
   Для выбора нескольких узлов выполните одно из следующих действий:
   - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными узлами.
   - Удерживая нажатой клавишу **CTRL**, выберите нужные узлы с помощью мыши.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов с количественным распределением устройств по категориям.
3. Если среди выбранных узлов присутствуют устройства с различными категориями, вы можете исключить устройства одной из категорий. Для этого снимите флажок рядом с названием этой категории. Название категории исчезнет из списка.
4. Нажмите на кнопку **Удалить устройство** (если выбран один узел) или **Удалить устройства** (если выбрано несколько узлов).
   Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.

Автоматическое изменение статусов устройств

При отслеживании активности устройств в промышленной сети программа автоматически присваивает соответствующие статусы обнаруженным устройствам по полученным MAC- и / или IP-адресам устройств.

В режиме обучения всем обнаруженным устройствам присваивается статус *Разрешенное*.

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 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*.

Если устройство со статусом *Разрешенное* длительное время не проявляет активность и сведения об этом устройстве не изменялись (30 дней и более), этому устройству присваивается статус *Неиспользуемое*.

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).

Изменение статусов устройств вручную

Изменять статусы устройств может только пользователь с ролью Администратор.

Вы можете изменить статус для одного выбранного устройства или одновременно для нескольких выбранных устройств. Если выбрано одно устройство со статусом *Неиспользуемое*, изменение статуса этого устройства можно выполнить только при изменении сведений об устройстве. Если выбрано несколько устройств, вы можете присвоить этим устройствам любой статус независимо от их текущего статуса.

> После присвоения устройству статуса *Неиспользуемое* программа может автоматически изменить статус этого устройства, если оно проявит активность. В зависимости от текущего режима работы контроля устройств программа присвоит обнаруженному устройству статус *Разрешенное* или *Неразрешенное*.

Изменять статусы устройств можно следующими способами:

- Изменение статусов устройств при работе с таблицей устройств

Чтобы изменить статус устройств при работе с таблицей, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Устройства**.
3. В таблице устройств выберите устройства, статус которых вы хотите изменить.

   В правой части окна веб-интерфейса появится область деталей.
4. В зависимости от текущего статуса и количества выбранных устройств выполните одно из следующих действий:
   - Если выбрано несколько устройств, нажмите на кнопку с названием нужного статуса.
   - Если выбрано одно устройство со статусом *Разрешенное* или *Неразрешенное*, нажмите на кнопку с названием нужного статуса (кнопка с названием текущего статуса не отображается).

   Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.

- Изменение статусов устройств при работе с картой сети

При работе с картой сети вы можете изменять статусы известных программе устройств, представленных узлами на карте сети.

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 устройств при работе с картой сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Карта сети** выберите один или несколько объектов, представляющих 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.
3. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.
4. В зависимости от текущего статуса и количества выбранных узлов выполните одно из следующих действий:
   - Если выбрано несколько узлов, представляющих известные программе устройства, нажмите на кнопку с названием нужного статуса.
   - Если выбран один узел, представляющий устройство со статусом *Разрешенное* или *Неразрешенное*, и вы хотите присвоить этому устройству другой статус, нажмите на кнопку с названием нужного статуса (кнопка с названием текущего статуса не отображается).

   Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.

Просмотр сведений об устройстве

Подробные сведения об устройстве включают информацию из таблицы устройств, а также следующие поля:

- **Маршрут. устройство** – признак маршрутизирующего устройства.
- **Доп. сведения** – дополнительные сведения об устройстве, заданные пользователем программы.

- **Пользовательские поля** – набор пользовательских сведений, отсутствующих в стандартном наборе сведений. Для устройства может быть указано до 16 пользовательских полей.

Чтобы просмотреть сведения об устройстве,

в разделе **Устройства** выберите нужное устройство.

В правой части окна веб-интерфейса появится область деталей. В области деталей отображаются все сведения, для которых заданы значения. Сведения, для которых выключено автоматическое изменение, отмечены значком .

Управление размещением устройств в дереве групп

Вы можете управлять размещением устройств в дереве групп путем включения устройств в нужные группы или исключения устройств из групп.

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.

Управлять размещением устройств в дереве групп могут только пользователи с ролью Администратор.

Для управления размещением устройств в дереве групп вы можете использовать следующие функции:

- Включение одного устройства в группу

  Чтобы включить устройство в группу, выполните следующие действия:

  1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
  2. Выберите устройство в разделе **Устройства** или в разделе **Карта сети**.

     В правой части окна веб-интерфейса появится область деталей.
  3. Нажмите на кнопку **Изменить**.
  4. В области деталей перейдите на закладку **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. Закладка 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 сети вы можете включить в группу несколько известных программе устройств, представленных узлами на карте сети. 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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Устройства**.
3. В таблице устройств выберите устройства, которые вы хотите включить в группу.

   В правой части окна веб-интерфейса появится область деталей.
4. По правой клавише мыши откройте контекстное меню
5. В контекстном меню выберите пункт **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 графе **Группа**.

Чтобы включить несколько устройств в группу при работе с картой сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Карта сети** 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.
3. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.
4. По правой клавише мыши откройте контекстное меню
5. В контекстном меню выберите пункт **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**.

   Выбранные узлы, представляющие известные программе устройства, отобразятся внутри выбранной группы.

- Исключение одного устройства из группы

Чтобы исключить устройство из группы, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите устройство в разделе **Устройства** или в разделе **Карта сети**.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. В области деталей перейдите на закладку **Параметры**.
5. В поле **Группа** удалите путь к группе по ссылке **Очистить** над полем (ссылка отображается, если группа задана).
6. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Закладка 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 сети вы можете исключить из групп несколько известных программе устройств, представленных узлами на карте сети. 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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Устройства**.
3. В таблице устройств выберите устройства, которые вы хотите исключить из групп.

   В правой части окна веб-интерфейса появится область деталей.
4. По правой клавише мыши откройте контекстное меню
5. В контекстном меню выберите пункт **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 сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Карта сети** 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.
3. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.
4. По правой клавише мыши откройте контекстное меню
5. В контекстном меню выберите пункт **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 отобразятся вне групп.

Установка и удаление 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 графе **Метки**. Метки сортируются в ячейке в алфавитном порядке.

Устанавливать и удалять метки для устройств могут только пользователи с ролью Администратор.

Устанавливать и удалять метки можно следующими способами:

- Установка меток для одного устройства

  Чтобы установить метки для устройства, выполните следующие действия:

  1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

  2. Выберите устройство в разделе **Устройства** или в разделе **Карта сети**.

     В правой части окна веб-интерфейса появится область деталей.

  3. Нажмите на кнопку **Изменить**.

     В области деталей перейдите на закладку **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 по ссылке **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. Закладка 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 сети вы можете установить метки для известных программе устройств, представленных узлами на карте сети. 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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Устройства**.

3. В таблице устройств выберите устройства, для которых вы хотите установить метки.

   В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Установить метки**.

   Появится окно **Добавление меток**.

5. 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.

6. При необходимости скопируйте список меток по ссылке **Копировать метки**. Ссылка отображается, если список меток не пустой.

7. 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.

8. 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 картой сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. В разделе **Карта сети** 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.

3. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.

4. Нажмите на кнопку **Установить метки**.

   Появится окно **Добавление меток**.

5. 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.

6. При необходимости скопируйте список меток по ссылке **Копировать метки**. Ссылка отображается, если список меток не пустой.
7. 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.

8. 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**.

- Удаление меток для одного устройства

Чтобы очистить список меток устройства, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите устройство в разделе **Устройства** или в разделе **Карта сети**.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Изменить**.

   В области деталей перейдите на закладку **Параметры**.

4. В поле **Метки** удалите лишние метки:
   - с помощью значка ✕ рядом с названиями меток, если вы хотите удалить определенные метки;
   - по ссылке **Очистить** над списком меток, 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. Закладка с параметрами, требующими ввода правильных значений, отмечена значком ⚠.

- Очистка списков меток для нескольких устройств

Вы можете очистить списки метки для нескольких устройств при работе с таблицей устройств.

Также при работе с картой сети вы можете очистить списки меток для известных программе устройств, представленных узлами на карте сети. 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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Устройства**.
3. В таблице устройств выберите устройства, для которых вы хотите очистить списки меток.

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

   Появится окно **Добавление меток**.
5. Установите флажок **Удалить существующие**.
6. Нажмите на кнопку **ОК**.

Чтобы очистить списки меток для нескольких устройств при работе с картой сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Карта сети** 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.
3. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.
4. Нажмите на кнопку **Установить метки**.

   Появится окно **Добавление меток**.
5. Установите флажок **Удалить существующие**.
6. Нажмите на кнопку **ОК**.

Изменение сведений об устройстве

Изменять сведения об устройстве могут только пользователи с ролью Администратор.

Чтобы изменить сведения об устройстве вручную, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Устройства** выберите нужное устройство.

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

   В области деталей появятся закладки для просмотра и изменения сведений об устройстве: **Адреса**, **Параметры** и **Пользовательские поля**.

4. На закладке **Адреса** в области деталей укажите MAC- и / или IP-адреса устройства.

   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.

5. 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 кнопку **Удалить интерфейс**, которая расположена 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.

6. На закладке **Параметры** в области деталей укажите нужные значения в полях, определяющих сведения об устройстве.

   > Также на закладке **Параметры** вы можете изменить статус устройства (например, присвоить устройству со статусом *Неиспользуемое* любой другой статус).

7. На закладках **Адреса** и **Параметры** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте переключатели **Обновлять автоматически**, расположенные над полями с возможностью автоматического изменения.

8. На закладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей и их значений.

9. Нажмите на кнопку **Сохранить**.

   Кнопка недоступна, если в параметрах устройства указаны не все необходимые сведения или заданы недопустимые значения. Закладка с параметрами, требующими ввода правильных значений, отмечена значком .

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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Устройства** выберите нужное устройство.

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

   В области деталей появятся закладки для просмотра и изменения сведений об устройстве: **Адреса**, **Параметры** и **Пользовательские поля**.
4. Перейдите на закладку **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**.

Просмотр событий, связанных с устройствами

Вы можете просмотреть события, связанные с устройствами. Для загрузки событий автоматически применяется фильтрация по идентификаторам известных программе устройств с использованием значений MAC- и IP-адресов, которые указаны для устройств.

В таблице событий программа показывает события, в которых среди значений в графах **Отправитель** или **Получатель** присутствуют MAC- или IP-адреса выбранных устройств.

Возможность загрузки событий доступна, если выбрано не более 200 устройств.

Чтобы просмотреть события, связанные с устройствами, выполните следующие действия:

1. Выберите раздел **Устройства**.
2. В таблице устройств выберите устройства, для которых вы хотите просмотреть события.

   В правой части окна веб-интерфейса появится область деталей.

3. В зависимости от того, какие события вы хотите загрузить, нажмите на одну из следующих кнопок (кнопки недоступны, если выбрано более 200 устройств):

   - **Показать события** – если вы хотите просмотреть события с любым статусом.
   - **Показать необработанные события** – если вы хотите просмотреть события со статусами *Новое* или *В обработке*.

Откроется раздел **События**. В таблице событий будет применена фильтрация по идентификаторам устройств. Список идентификаторов устройств, заданных для фильтрации событий, отобразится в поле **ID устройств** в панели инструментов. Если вы загрузили события с помощью кнопки **Показать необработанные события**, события будут дополнительно отфильтрованы по графе **Статус**.

Контроль сети

Для контроля промышленной сети с помощью Kaspersky Industrial CyberSecurity for Networks вы можете настроить отслеживание взаимодействий между устройствами промышленной сети.

Программа отслеживает взаимодействия между устройствами промышленной сети по правилам контроля сети. *Правило контроля сети* описывает разрешенное взаимодействие для устройств.

Правило контроля сети может применять одну 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.

В общем случае правило контроля сети содержит следующую информацию о взаимодействии:

- стороны, принимающие участие в сетевом взаимодействии;
- разрешенный протокол или системные команды.

Правила контроля сети могут находиться в активном или неактивном состояниях.

По умолчанию после создания правило находится в активном состоянии и применяется для разрешения описанных взаимодействий. При обнаружении взаимодействий, описанных в активных правилах контроля сети, программа не регистрирует события.

Неактивные правила предназначены для описания нежелательных сетевых взаимодействий. В режиме обучения контроля сети неактивные правила предотвращают автоматическое создание новых активных правил для обнаруженных сетевых взаимодействий, описанных в неактивных правилах. В режиме наблюдения контроля сети неактивные правила не учитываются.

Программа обрабатывает правила контроля сети по технологии Контроль целостности сети и Контроль системных команд, если включено применение этих технологий.

Для создания списка правил контроля сети предусмотрены следующие способы:

- автоматическое формирование правил в режиме обучения;
- создание правил вручную.

Список правил контроля сети хранится на Сервере и не зависит от политики безопасности, которая загружена в Консоль или применена на Сервере.

Вы можете настраивать правила контроля сети в разделе **Контроль сети** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Настройка параметров регистрации событий контроля сети выполняется в Консоли программы на закладке Настройка событий. События, регистрируемые по технологиям Контроль целостности сети и Контроль системных команд, относятся к системным типам событий.

Вы можете просмотреть события контроля сети в таблице зарегистрированных событий. События, регистрируемые по технологии Контроль целостности сети, имеют уровень важности *Важные*. Событиям, регистрируемым по технологии Контроль системных команд, присваивается уровень важности в зависимости от заданного уровня важности для обнаруженной системной команды.

Режим обучения контроля сети

В режиме обучения контроля сети Kaspersky Industrial CyberSecurity for Networks выполняет следующие действия:

- Если включено применение технологии Контроль целостности сети, программа формирует правила по этой технологии. При обнаружении сетевых взаимодействий, которые удовлетворяют неактивным 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 неактивным 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 контроля сети 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 сети. Если обнаруженное взаимодействие не соответствует ни одному правилу, программа создает новое правило контроля сети. Событие обнаружения взаимодействия в этом случае не регистрируется. При создании нового правила программа устанавливает для него активное состояние и добавляет значения параметров на основании полученных данных о сетевом взаимодействии.

Если обнаруженное взаимодействие соответствует только неактивному правилу, программа регистрирует событие по технологии, соответствующей этому правилу. В этом случае новое активное правило не создается.

В процессе обучения программа может оптимизировать список правил контроля сети. 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 находятся в активном состоянии;

- 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 сети. 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.

Программа выполняет оптимизацию списка правил контроля сети периодически во время работы в режиме обучения. 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 списка правил после выключения режима обучения может выполняться с задержкой. Длительность задержки зависит от интенсивности поступления данных в программу и может составить до трех минут. В течение этого времени рекомендуется не вносить изменения в правила, созданные в режиме обучения.

Режим обучения контроля сети 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 контроля сети

В режиме наблюдения контроля сети Kaspersky Industrial CyberSecurity for Networks 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 активные 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 активные 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 списке правил контроля сети должны быть правила и для этой системной команды, и для сетевого пакета, в котором она передается.

Выбор применяемых технологий и изменение режима контроля сети

Управлять технологиями и режимами контроля сети могут только пользователи с ролью Администратор.

Чтобы включить или выключить применение технологий контроля сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры** и перейдите на закладку **Технологии**.

3. Включите или выключите применение технологий контроля сети, используя следующие переключатели:

   - **Контроль целостности сети**.
   - **Контроль системных команд**.

4. После включения или выключения технологии дождитесь перевода переключателя в нужное состояние (*Включено* или *Выключено*).

   Процесс занимает некоторое время, переключатель при этом будет недоступен. Дождитесь включения или выключения технологии.

5. Для каждой включенной технологии выберите нужный режим контроля сети. Для этого в раскрывающемся списке справа от названия технологии выберите одно из следующих значений:

   - **Обучение** – для применения технологии в режиме обучения.
   - **Наблюдение** – для применения технологии в режиме наблюдения.

6. После выбора режима дождитесь появления названия этого режима в поле раскрывающегося списка.

7. Процесс занимает некоторое время, при этом в раскрывающемся списке отображается статус *Изменение*. Дождитесь включения выбранного режима.

Автоматическое формирование правил контроля сети в режиме обучения

В режиме обучения Kaspersky Industrial CyberSecurity for Networks автоматически формирует правила контроля сети, анализируя сетевые взаимодействия устройств промышленной сети. Программа создает новое правило, если обнаруженное сетевое взаимодействие не соответствует ни одному правилу в списке правил контроля сети.

В режиме обучения программа может автоматически создавать правила контроля сети, разрешающие отправку системных команд для Kaspersky Industrial CyberSecurity for Nodes. Эти правила нужны для интеграции Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes 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 в этой же промышленной сети. Вы можете найти подробную информацию о включении компонентов Kaspersky Industrial CyberSecurity for Nodes в документе *Руководство администратора Kaspersky Industrial CyberSecurity for Nodes*.

Просмотр таблицы правил контроля сети

Таблица правил контроля сети отображается в разделе **Контроль сети** веб-интерфейса программы.

При просмотре таблицы правил контроля сети вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице правил

  Чтобы настроить список отображаемых в таблице граф, выполните следующие действия:

  1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер и выберите раздел **Контроль сети**.
  2. Нажмите на кнопку **Настроить таблицу**.

     Откроется окно для настройки отображения таблицы правил.
  3. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр.

     Для выбора доступны следующие параметры:

     - **ID правила**.

       Уникальный идентификатор правила.
     - **Состояние** (значок ◐).

       Текущее состояние правила (*Активное* или *Неактивное*).
     - **Технология**.

       Технология, к которой относится правило.
     - **Протоколы/Команды**.

       Для правил, относящихся к технологии Контроль целостности сети – набор используемых протоколов. Для правил, относящихся к технологии Контроль системных команд – протокол и системные команды. Протоколы, которые определяются программой по содержимому сетевых пакетов, выделены курсивом.
     - **Сторона 1**.

       Адресная информация одной из сторон сетевого взаимодействия:

       - **MAC-адрес**.
       - **IP-адрес**.
       - **Номер порта**.
     - **Сторона 2**.

       Адресная информация другой стороны сетевого взаимодействия:

       - **MAC-адрес**.
       - **IP-адрес**.
       - **Номер порта**.
     - **Комментарий**.

       Дополнительная информация о правиле.
     - **Дата создания**.

       Дата и время создания правила.
     - **Дата изменения**.

       Дата и время последнего изменения правила.
     - **Источник**.

       Сведения об источнике правила.
  4. Если вы хотите изменить порядок отображения граф, выделите название графы, которую требуется разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

     Для граф **Сторона 1** и **Сторона 2** вы также можете изменить порядок отображения адресной информации для сторон сетевого взаимодействия. Для этого выделите значение, которое вы хотите разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

  Выбранные графы отобразятся в указанном вами порядке в таблице правил контроля сети.

- Фильтрация по графам таблицы

*Чтобы отфильтровать правила по графе **ID правила**, выполните следующие действия:*

1. В разделе **Контроль сети** нажмите на значок фильтрации в графе **ID правила**.

   Откроется окно фильтрации.

2. В полях **Включая** и **Исключая** введите значения для правил, которые вы хотите включить в фильтрацию и / или исключить из фильтрации.

3. Если вы хотите применить несколько условий фильтрации, объединенных логическим оператором ИЛИ, в окне фильтрации графы нажмите на кнопку **Добавить условие** и введите условие в открывшемся поле.

4. Если вы хотите удалить одно из созданных условий фильтрации, в окне фильтрации графы нажмите на значок .

5. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать правила по графе **Состояние**, **Технология** или **Источник**, выполните следующие действия:*

1. В разделе **Контроль сети** нажмите на значок фильтрации в нужной графе.

   При фильтрации по состояниям, технологиям или источникам правил контроля сети вы также можете воспользоваться соответствующими кнопками в панели инструментов.

   Откроется окно фильтрации.

2. Установите флажки напротив значений, по которым вы хотите выполнить фильтрацию.

3. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать правила по графе **Протоколы/Команды**, выполните следующие действия:*

1. В разделе **Контроль сети** нажмите на значок фильтрации в графе **Протоколы/Команды**.

   > Фильтрация по графе **Протоколы/Команды** выполняется только по протоколам. Для фильтрации правил контроля сети по названиям системных команд вы можете использовать функцию поиска правил.

   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 графах 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 **ОК**.

*Чтобы отфильтровать правила по графам **Сторона 1** и **Сторона 2**, выполните следующие действия:*

1. В разделе **Контроль сети** откройте раскрывающийся список **Адресная информация**.

   Откроется окно фильтрации.

2. Укажите нужные значения в следующих полях:

   - **MAC-адрес**.
   - **IP-адрес**.
   - **Номер порта**.

3. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать правила по графе **Дата создания** или **Дата изменения**, выполните следующие действия:*

1. В разделе **Контроль сети** нажмите на значок фильтрации в нужной графе.

   Откроется календарь.

2. В календаре задайте дату и время 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.ГГ чч:мм:сс.

3. Нажмите на кнопку **ОК**.

- **Поиск правил**

Чтобы найти нужные правила,

в разделе **Контроль сети** введите поисковый запрос в поле **Поиск правил**. Поиск инициируется во время ввода символов.

В таблице правил контроля сети отобразятся правила, которые удовлетворяют условиям поиска.

Поиск выполняется по всем графам, кроме граф **Состояние**, **Технология**, **Дата создания**, **Дата изменения** и **Источник**.

- **Сброс заданных параметров фильтрации и поиска**

Чтобы сбросить заданные параметры фильтрации и поиска в таблице правил контроля сети,

в панели инструментов в разделе **Контроль сети** нажмите на кнопку **Очистить фильтр** (кнопка отображается, если заданы параметры фильтрации или поиска).

- **Сортировка правил**

Чтобы отсортировать правила контроля сети, выполните следующие действия:

1. В разделе **Контроль сети** нажмите на заголовок графы, по которой вы хотите выполнить сортировку.

   Вы можете отсортировать таблицу правил контроля сети по значениям любой графы, кроме графы **Комментарий**.

2. При сортировке правил по графе **Протоколы/Команды**, **Сторона 1** или **Сторона 2** в раскрывающемся списке заголовка графы выберите параметр, по которому будет выполняться сортировка:

   - В графе **Протоколы/Команды** выберите параметры сортировки: по протоколам или по системным командам.
   - В зависимости от значений, выбранных для отображения в графах **Сторона 1** или **Сторона 2**, выберите параметры сортировки: по MAC-адресам, по IP-адресам или по номерам портов.

3. Если требуется отсортировать таблицу по нескольким графам, нажмите на клавишу **SHIFT** и, удерживая ее нажатой, нажмите на заголовки граф, по которым нужно выполнить сортировку.

Таблица будет отсортирована по выбранной графе. При сортировке по нескольким графам строки таблицы сортируются в соответствии с последовательностью выбора граф. Рядом с заголовками граф, по которым выполнена сортировка, отображаются значки, показывающие текущий порядок сортировки: по возрастанию или по убыванию значений.

- **Обновление таблицы правил**

Правила контроля сети могут быть изменены на Сервере в то время, когда вы просматриваете таблицу правил. Например, таблица правил контроля сети становится неактуальной, если пользователь программы в другом сеансе подключения изменил правила или программа выполнила оптимизацию списка правил в режиме обучения.

Для поддержания таблицы правил контроля сети в актуальном состоянии вы можете включить автоматическое обновление правил или обновлять таблицу вручную. При обновлении все правила заново загружаются с Сервера.

Чтобы включить или выключить автоматическое обновление таблицы правил контроля сети,

в разделе **Контроль сети** используйте переключатель **Обновлять автоматически**.

При включенном автоматическом обновлении таблица правил контроля сети обновляется через каждые пять секунд.

Чтобы вручную обновить таблицу правил контроля сети, выполните следующие действия:

1. Выключите автоматическое обновление, если эта функция включена. Для этого в разделе **Контроль сети** переведите переключатель **Обновлять автоматически** в состояние *Выключено*.

2. Нажмите на кнопку **Обновить** (кнопка отображается справа от переключателя **Обновлять автоматически**, если переключатель выключен).

Таблица правил заново загрузится с Сервера.

Выбор правил контроля сети

В таблице правил контроля сети вы можете выбирать правила для просмотра сведений и для работы с этими правилами. При выборе правил в правой части окна веб-интерфейса появляется область деталей.

Чтобы выбрать нужные правила контроля сети, выполните одно из следующих действий:

- Если вы хотите выбрать одно правило, установите флажок напротив этого правила или выберите правило с помощью мыши.
- Если вы хотите выбрать несколько правил, установите флажки напротив нужных правил или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**. При выборе нескольких правил программа проверяет состояние выбранных правил и определяет наличие активных и неактивных правил среди выбранных.
- Если вы хотите выбрать все правила, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:
  - выберите любое правило в таблице и нажмите комбинацию клавиш **CTRL+A**;
  - установите флажок в заголовке левой крайней графы таблицы.

При выборе нескольких правил в области деталей отображается общее количество выбранных правил. Если вы выбрали все правила, удовлетворяющие текущим параметрам фильтрации и поиска, в области деталей отображается одно из следующих значений:

- Если выбрано до 1000 правил включительно, отображается точное количество. В этом случае программа проверяет состояние выбранных правил, как и при других способах выбора нескольких правил.
- Если выбрано более 1000 правил, отображается **1000+**. В этом случае программа не проверяет состояние выбранных правил.

В заголовке левой крайней графы таблицы отображается флажок выбора правил. В зависимости от количества выбранных правил флажок может быть в одном из следующих состояний:

- ☐ – в таблице не выполнялся выбор всех правил, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбрано одно правило или несколько правил с помощью флажков напротив правил или с использованием клавиш **CTRL** или **SHIFT**.
- ☑ – в таблице выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска.
- ▣ – в таблице были выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых правил были сняты флажки. Это состояние сохраняется и в случае, если флажки сняты для всех правил, выбранных таким способом (из-за того, что количество выбранных правил может измениться).

Если выбраны все правила, удовлетворяющие параметрам фильтрации и поиска, количество выбранных правил может автоматически изменяться. Например, состав правил в таблице может быть изменен пользователем программы в другом сеансе подключения или при оптимизации списка правил в режиме обучения. Рекомендуется настраивать параметры фильтрации и поиска таким образом, чтобы в выборку попали только нужные правила (например, перед выбором всех правил вы можете отфильтровать правила по идентификаторам).

Создание правил контроля сети вручную

Для создания правил контроля сети вручную предусмотрены следующие варианты:

- с изначально пустыми значениями параметров;
- на основе имеющегося правила;
- на основе событий, зарегистрированных по технологии Контроль целостности сети или Контроль системных команд.

Чтобы создать правило с изначально пустыми значениями параметров, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Контроль сети** нажмите на кнопку **Добавить правило**.

   В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила.
3. Выберите технологию для правила:

   - 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**.
4. 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 левой графе 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 **ОК**.

Если выбран протокол, который программа может определять по содержимому сетевых пакетов, ниже поля **Протокол** появится пояснение об этом.

5. 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 **ОК**.

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 следующие значения:

   - MAC-адрес;
   - IP-адрес;
   - номер порта.

8. Нажмите на кнопку **Сохранить**.

   Программа проверит таблицу правил контроля сети.

9. Если в таблице правил присутствует активное правило, в котором совпадают все параметры, отобразится предупреждение о наличии совпадающего правила. В этом случае закройте предупреждение и измените параметры создаваемого правила.

10. Если в таблице правил присутствует активное 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 список правил контроля сети.

11. Если в таблице правил присутствуют активные 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 неактивные правила с более частными или совпадающими параметрами, программа удаляет эти правила из списка. При удалении этих правил программа не отображает запрос.

12. Если для нового правила, относящегося к технологии Контроль системных команд, отсутствует активное правило, которое разрешает сетевое взаимодействие между устройствами, отобразится запрос на создание соответствующего правила, относящегося к 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, относящегося к технологии Контроль целостности сети.

Чтобы создать новое правило контроля сети на основе имеющегося правила, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. В разделе **Контроль сети** выберите правило, на основе которого вы хотите создать новое правило.

3. По правой клавише мыши откройте контекстное меню.

4. В контекстном меню выберите пункт **Создать правило на основе выбранного правила**.

   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 3–8, описанные в процедуре создания правила с изначально пустыми значениями параметров.

Чтобы создать новое правило контроля сети на основе зарегистрированного события, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **События**.

3. В таблице зарегистрированных событий выберите событие, на основе которого вы хотите создать правило контроля сети. Вы можете выбрать событие, зарегистрированное по технологии *Контроль целостности сети* или *Контроль системных команд*. При этом событие должно содержать сведения только об одном сетевом взаимодействии.

   В правой части окна веб-интерфейса появится область деталей.

4. В области деталей нажмите на кнопку **Создать правило контроля сети**.

   В окне веб-браузера откроется раздел **Контроль сети**. 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 4–8, 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 сети

Вы можете изменить параметры активного правила контроля сети. Для неактивных правил возможность изменения недоступна.

Чтобы изменить параметры правила контроля сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Контроль сети** выберите нужное правило для изменения параметров.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Изменить**.
4. Измените нужные параметры. Описание действий для настройки параметров см. в процедуре создания правила с изначально пустыми значениями параметров в разделе Создание правил контроля сети вручную.

Изменение состояния правил контроля сети

Правила контроля сети могут находиться в активном или неактивном состояниях. По умолчанию каждое правило после создания находится в активном состоянии.

Вы можете перевести правила в неактивное состояние, чтобы выключить их использование при контроле сети в режиме наблюдения.

Чтобы перевести правила контроля сети в неактивное состояние, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Контроль сети** выберите одно или несколько активных правил, для которых вы хотите изменить состояние.

   В правой части окна веб-интерфейса появится область деталей.
3. В зависимости от количества выбранных правил, нажмите на кнопку **Выключить правило** или **Выключить правила**. Кнопка не отображается, если вы выбрали только неактивные правила. При этом если выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000 программа не проверяет состояние правил. В этом случае кнопка **Выключить правила** отображается независимо от состояния выбранных правил.

Чтобы перевести правила контроля сети в активное состояние, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Контроль сети** выберите одно или несколько неактивных правил, для которых вы хотите изменить состояние.

   В правой части окна веб-интерфейса появится область деталей.

3. В зависимости от количества выбранных правил, нажмите на кнопку **Активировать правило** или **Активировать правила**. Кнопка не отображается, если вы выбрали только активные правила. При этом если выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000, программа не проверяет состояние правил. В этом случае кнопка **Активировать правила** отображается независимо от состояния выбранных правил.

Удаление правил контроля сети

Вы можете выборочно удалить одно или несколько правил контроля сети. Удаленные правила перестают действовать при контроле сети как в режиме наблюдения, так и в режиме обучения.

Чтобы удалить правила контроля сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Контроль сети**.

3. В таблице правил выберите правила, которые вы хотите удалить.

   В правой части окна веб-интерфейса появится область деталей.

4. В зависимости от количества выбранных правил, нажмите на кнопку **Удалить правило** или **Удалить правила**.

   Откроется окно с запросом подтверждения. В зависимости от состояния выбранных правил, в запросе будут предложены следующие варианты действий:

   - Если все выбранные правила находятся в активном состоянии, программа предлагает удалить выбранные правила, перевести их в неактивное состояние 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 неактивные 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.

Обнаружение 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.

Правила обнаружения вторжений и дополнительные методы обнаружения вторжений по встроенным алгоритмам применяются независимо от политики безопасности, которая загружена в Консоль или применена на Сервере.

Вы можете настраивать правила обнаружения вторжений в Консоли Kaspersky Industrial CyberSecurity for Networks на закладке Обнаружение вторжений.

Изменять состояния методов обнаружения вторжений вы можете при подключении к Серверу через веб-браузер.

Настройка параметров регистрации событий обнаружения вторжений выполняется в Консоли программы на закладке Настройка 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.

Правила обнаружения вторжений входят в наборы правил. Набор правил включает правила обнаружения вторжений, сгруппированные по произвольным признакам (например, правила, которые содержат взаимозависимые условия для анализа трафика). В программе могут использоваться 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. Названия пользовательских наборов правил совпадают с именами файлов, из которых были загружены эти наборы правил (без указания расширений файлов).

Наборы правил обнаружения вторжений могут находиться в активном или неактивном состояниях. Активное состояние означает, что правила из набора применяются при анализе трафика, если включен метод обнаружения вторжений по правилам. Если набор правил переведен в неактивное состояние, правила из этого набора перестают применяться.

При загрузке набора правил программа выполняет проверку правил, содержащихся в наборе. Если в результате проверки набора правил возникли ошибки (например, обнаружены дублирующиеся правила), программа отображает сведения о количестве обнаруженных ошибок для этого набора. Наборы правил с обнаруженными ошибками игнорируются в программе (правила из этих наборов не применяются, даже если наборы находятся в активном состоянии).

При обнаружении в трафике условий, заданных в активном правиле обнаружения вторжений, 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.

Уровни важности событий Kaspersky Industrial CyberSecurity for Networks соответствуют значениям приоритетов в правилах обнаружения вторжений (см. таблицу ниже).

Соответствие приоритетов правил и уровней важности событий

Значения приоритетов в правилах обнаружения вторжений	Уровни важности событий Kaspersky Industrial CyberSecurity for Networks
4 и более	Информационные
2 или 3	Важные
1	Критические

Дополнительные методы обнаружения вторжений

Для обнаружения вторжений вы можете применять следующие дополнительные методы:

- **Обнаружение признаков подмены адресов в ARP-пакетах**

  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).

Вы можете применять дополнительные методы обнаружения вторжений независимо от наличия и состояния правил обнаружения вторжений. Для проверки по дополнительным методам используются встроенные алгоритмы.

Включение и выключение обнаружения вторжений по правилам

Вы можете включать и выключать применение метода обнаружения вторжений по правилам при подключении к Серверу через веб-браузер.

Включать и выключать метод обнаружения вторжений по правилам могут только пользователи с ролью Администратор.

Чтобы включить или выключить метод обнаружения вторжений по правилам, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры** и перейдите на закладку **Технологии**.

3. С помощью переключателя **Обнаружение вторжений по правилам** включите или выключите обнаружение вторжений по правилам.

4. После включения или выключения метода дождитесь перевода переключателя в нужное состояние (*Включено* или *Выключено*).

   Процесс занимает некоторое время. Переключатель при этом будет недоступен.

Включение и выключение дополнительных методов обнаружения вторжений

Вы можете включать и выключать применение дополнительных методов обнаружения вторжений при подключении к Серверу через веб-браузер.

Включать и выключать дополнительные методы обнаружения вторжений могут только пользователи с ролью Администратор.

Чтобы включить или выключить дополнительные методы обнаружения вторжений, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. Выберите раздел **Параметры** и перейдите на закладку **Технологии**.

3. Включите или выключите применение дополнительных методов обнаружения вторжений, используя следующие переключатели:

   - **Обнаружение ARP-спуфинга** – включает или выключает обнаружение признаков подмены адресов в ARP-пакетах.

   - **Обнаружение аномалий в протоколе TCP** – включает или выключает обнаружение аномалий в протоколе TCP.

   - **Обнаружение аномалий в протоколе IP** – включает или выключает обнаружение аномалий в протоколе IP.

4. После включения или выключения метода дождитесь перевода переключателя в нужное состояние (*Включено* или *Выключено*).

   Процесс занимает некоторое время. Переключатель при этом будет недоступен.

Просмотр таблицы с наборами правил обнаружения вторжений

При просмотре таблицы с наборами правил обнаружения вторжений вы можете использовать следующие функции:

- Фильтрация таблицы

  Чтобы отфильтровать таблицу с наборами правил обнаружения вторжений, выполните следующие действия:

  1. На закладке **Обнаружение вторжений** нажмите на значок фильтрации в графе, по которой вы хотите выполнить фильтрацию.

     Вы можете использовать для фильтрации любую графу, кроме графы **Название набора правил**.

  2. В раскрывающемся списке выберите параметр фильтрации наборов правил.

     В таблице с наборами правил обнаружения вторжений будут отображены только те наборы, которые удовлетворяют выбранному параметру фильтрации.

- Поиск наборов правил

  Чтобы найти наборы правил обнаружения вторжений,

  на закладке **Обнаружение вторжений** введите поисковый запрос в поле **Поиск**. Поиск инициируется во время ввода символов.

  В таблице с наборами правил обнаружения вторжений отобразятся наборы, которые удовлетворяют условиям поиска.

  Поиск выполняется по графе **Название набора правил**.

- Сортировка наборов правил

  Чтобы отсортировать наборы правил обнаружения вторжений по значениям графы, выполните следующие действия:

  1. На закладке **Обнаружение вторжений** нажмите на значок стрелки в правой части заголовка графы, по которой вы хотите выполнить сортировку.

     Таблица будет отсортирована по выбранной графе. При этом значок стрелки примет вид, соответствующий текущему порядку сортировки.

  2. Если вы хотите изменить порядок сортировки на обратный, нажмите на значок стрелки еще раз.

Изменение состояния наборов правил обнаружения вторжений

Наборы правил обнаружения вторжений могут находиться в активном или неактивном состояниях. Если набор правил переведен в неактивное состояние, все правила этого набора не используются при обнаружении вторжений.

Изменять состояния наборов правил обнаружения вторжений могут только пользователи с ролью Администратор.

Чтобы изменить состояние наборов правил обнаружения вторжений, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. Выберите закладку **Обнаружение вторжений** в окне Консоли программы.
3. В таблице с наборами правил обнаружения вторжений установите или снимите флажки в графе **Активно** для тех наборов, состояние которых вы хотите изменить.

   Строки с наборами правил, для которых будет изменено состояние, выделяются цветом.
4. Нажмите на кнопку **Применить**.

Состояние правил изменится согласно установленным и снятым флажкам. После перевода набора правил в неактивное состояние строка, соответствующая набору правил, выделяется курсивом.

Загрузка и замена пользовательских наборов правил обнаружения вторжений

Вы можете загрузить в программу наборы правил обнаружения вторжений из файлов. Файлы с описаниями правил обнаружения вторжений должны находиться в одной директории 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. Название набора правил будет совпадать с именем файла без расширения rules.

При загрузке наборов правил из файлов текущие пользовательские наборы правил удаляются из таблицы и заменяются новыми. При этом системные наборы правил (для которых в графе **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, выполните следующие действия:

1. Убедитесь, что у вас есть права на чтение файлов в директории с файлами правил обнаружения вторжений, которые вы хотите использовать.

2. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.

3. Выберите закладку **Обнаружение вторжений** в окне Консоли программы.

4. В панели инструментов откройте меню **Пользовательские правила** и выберите пункт **Заменить пользовательские правила**.

   Откроется окно **Директория с файлами правил обнаружения вторжений**.

5. Укажите директорию с файлами правил обнаружения вторжений.

6. Нажмите на кнопку **Выбрать**.

   В таблице с наборами правил отобразятся новые пользовательские наборы правил. Для этих наборов правил в графе **Источник** будет указано значение **Пользователь**. Все наборы правил будут в активном состоянии.

7. Проверьте наличие ошибок в загруженных наборах правил. Сведения об обнаруженных ошибках отображаются в графе **Ошибки**. Если набор правил содержит ошибки, вы можете просмотреть подробные сведения о них по ссылке **Подробнее**.

8. Если вы не хотите использовать некоторые из наборов правил при обнаружении вторжений, измените их состояние.

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.

При удалении пользовательских наборов правил не удаляются файлы, из которых были загружены эти наборы правил. Файлы можно будет использовать для новой загрузки правил (например, если вы хотите загрузить файлы выборочно).

Удалять пользовательские наборы правил обнаружения вторжений могут только пользователи с ролью Администратор.

Чтобы удалить пользовательские наборы правил обнаружения вторжений, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. Выберите закладку **Обнаружение вторжений** в окне Консоли программы.
3. В панели инструментов откройте меню **Пользовательские правила** и выберите пункт **Удалить пользовательские правила**.

   Пункт меню **Удалить пользовательские правила** доступен, если в таблице есть пользовательские наборы правил обнаружения вторжений.

   Откроется окно с запросом подтверждения.
4. Нажмите на кнопку **Да**.

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 записей журналов в базе данных

Вы можете изменить параметры хранения записей журналов в базе данных.

Чтобы изменить параметры хранения записей программы, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Параметры** окна Консоли программы выберите пункт **Журналы**.

   Откроется окно **Управление журналами**.
3. На закладке **Параметры хранения записей** в блоках параметров **Аудит**, **История событий** и **Сообщения программы** настройте следующие параметры:

   - **Максимальное время хранения записей (в днях)**.

Значение параметра по умолчанию – 365 дней.

- **Максимальное количество записей**.

  Значение параметра по умолчанию – 100 000 записей. При изменении значения параметра обратите внимание на оцениваемый объем заполнения дискового пространства для указанного количества записей.

4. Нажмите на кнопку **Применить**.

Управление параметрами сохранения трафика в базе данных

Программа может сохранять в базе данных трафик на момент регистрации событий. 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 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, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Параметры** окна Консоли программы выберите пункт **Журналы**.

   Откроется окно **Управление журналами**.
3. Выберите закладку **Сохранение трафика**.
4. Настройте следующие параметры хранения трафика в базе данных:

   - **Максимальное количество сохраняемых пакетов**.

     Значение параметра по умолчанию – 100 000 000 пакетов.

   - **Максимальное время хранения пакетов (в днях)**.

     Значение параметра по умолчанию – 365 дней.

   - **Максимальный объем сохраненного трафика в базе данных (МБ)**.

     Значение параметра по умолчанию – 15 000 МБ.
5. Нажмите на кнопку **Применить**.

Включение и выключение аудита действий пользователей

Вы можете включать и выключать аудит действий пользователей при подключении к Серверу через веб-браузер или в Консоли программы.

По умолчанию аудит действий пользователей включен.

Чтобы включить или выключить аудит действий пользователей при подключении к Серверу через веб-браузер, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Параметры** и перейдите на закладку **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.

Чтобы включить или выключить аудит действий пользователей в Консоли программы, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Параметры** окна Консоли программы выберите пункт **Журналы**.

   Откроется окно **Управление журналами**.
3. На закладке **Параметры хранения записей** выполните нужное действие:
   - Если вы хотите включить аудит, установите флажок **Включить** в блоке **Аудит**.
   - Если вы хотите выключить аудит, снимите флажок **Включить** в блоке **Аудит**.
4. Нажмите на кнопку **Применить**.

Изменение уровней ведения журналов работы процессов

Вы можете управлять сохранением данных в журналах работы следующих процессов программы:

- ProductFacade.
- ProductServer.
- KisClient.
- Filter.
- NetworkDumper.
- EntityManager.
- Watchdog.

Для каждого процесса вы можете задать один из следующих уровней ведения журнала:

- **Критический**. В журнале сохраняются данные о нарушениях в работе процесса, которые могут оказать критическое влияние на работу программы.

- **Ошибка**. В журнале сохраняются данные уровня **Критический** и информация об ошибках, возникших в работе процесса.
- **Предупреждение**. В журнале сохраняются данные уровня **Ошибка** и данные, на которые нужно обратить внимание.
- **Информационный**. В журнале сохраняются данные уровня **Предупреждение** и информация справочного характера.
- **Отладочный**. В журнале сохраняются данные уровня **Информационный** и все данные о работе процесса, которые могут потребоваться в процессе отладки программы (например, вспомогательные сообщения, сведения о производительности процесса).

Необходимость изменить уровни ведения журналов может возникнуть, например, при обращении в Службу технической поддержки.

Чтобы изменить уровень ведения журнала процесса Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:

1. Запустите Консоль программы и укажите учетные данные пользователя с ролью Администратор.
2. В меню **Параметры** окна Консоли программы выберите пункт **Сервер и сенсоры**.

   Откроется окно **Параметры Сервера и сенсоров**.
3. На закладке **Режим работы** раскройте список процессов нужного узла в графе **Узел**.
4. Если процесс, для которого нужно изменить уровень ведения журнала, относится к определенному компоненту (Серверу или сенсору), раскройте список процессов этого компонента.
5. В раскрывающемся списке графы **Уровень ведения журнала** для нужного процесса задайте уровень ведения журнала.
6. Нажмите на кнопку **Применить**.

Управление технологиями

В веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks вы можете включать и выключать использование технологий, а также изменять режим работы технологий. Управлять технологиями могут только пользователи с ролью Администратор

Включение и выключение поддерживается для следующих технологий и методов:

- Технологии контроля сети:
  - Контроль целостности сети.
  - Контроль системных команд.
- Методы контроля устройств:
  - Обнаружение активности устройств.
  - Обнаружение сведений об устройствах.

    - Контроль проектов ПЛК.
- Обнаружение неизвестных тегов по технологии контроля процесса.
- Методы обнаружения вторжений:
    - Обнаружение вторжений по правилам.
    - Обнаружение ARP-спуфинга.
    - Обнаружение аномалий в протоколе IP.
    - Обнаружение аномалий в протоколе TCP.

Если технология или метод выключены, программа не контролирует взаимодействия устройств по этой технологии или по этому методу. При этом вы можете настраивать параметры выключенных технологий и методов (например, добавлять или изменять правила).

Изменение режима поддерживается для следующих технологий и методов:

- Контроль целостности сети.
- Контроль системных команд.
- Обнаружение активности устройств.

По умолчанию после установки программы включены все технологии и методы, за исключением методов контроля проектов ПЛК и обнаружения неизвестных тегов. Для технологий и методов, поддерживающих изменение режима, по умолчанию включен режим обучения.

Чтобы изменить состояние и / или режим работы технологий и методов, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. Выберите раздел **Параметры** и перейдите на закладку **Технологии**.

   Отобразится список технологий и методов, доступных для изменения состояний и режимов работы.

   > Если изменение состояний и режимов работы технологий и методов невозможно в текущий момент, переключатели в списке недоступны (при этом в полях для выбора режимов отображается значение **Нет данных**). В этом случае рекомендуется проверить статус сервиса kics4net на компьютере Сервера. Если сервис не активен, требуется его запустить.

3. Включите или выключите применение нужных технологий и / или методов с помощью переключателей слева. Чтобы включить или выключить все технологии и методы одновременно, используйте кнопку **Включить все** или **Выключить все**.
4. После включения или выключения технологии или метода дождитесь применения изменений. До завершения перевода в другое состояние переключатель недоступен.
5. Если включены технологии Контроль целостности сети, Контроль системных команд или метод обнаружения активности устройств, выберите нужный режим. Для этого в раскрывающемся списке справа от названия технологии или метода выберите один из следующих элементов:

- **Обучение** – для применения технологии или метода в режиме обучения.
- **Наблюдение** – для применения технологии или метода в режиме наблюдения.

Чтобы изменить режим всех включенных технологий и методов одновременно, используйте раскрывающийся список **Режим**.

6. После выбора режима дождитесь применения изменений. До завершения изменения режима в раскрывающемся списке отображается статус *Изменение*.

   Если вы выбрали разные режимы для включенных технологий и методов, в раскрывающемся списке **Режим** отображается значение **Смешанный**.

Использование Kaspersky Industrial CyberSecurity for Networks API

В Kaspersky Industrial CyberSecurity for Networks реализован интерфейс прикладного программирования (Application Programming Interface, далее API), который содержит набор функций для использования в сторонних программах. Kaspersky Industrial CyberSecurity for Networks API предоставляет gRPC-методы для получения данных из Kaspersky Industrial CyberSecurity for Networks и отправки данных в программу.

Методы API для Kaspersky Industrial CyberSecurity for Networks позволяют выполнять следующие действия:

- получать данные об устройствах из таблицы устройств;
- получать данные о событиях Kaspersky Industrial CyberSecurity for Networks;
- отправлять события в Kaspersky Industrial CyberSecurity for Networks;
- получать данные о тегах;
- подписываться на уведомления о чтении и записи значений тегов;
- получать данные о текущей политике безопасности.

Kaspersky Industrial CyberSecurity for Networks API поставляется в виде пакета с набором proto-файлов. Этот пакет включен в комплект поставки программы. Proto-файлы могут быть скомпилированы в исходный код, позволяющий выполнять RPC-запросы к Kaspersky Industrial CyberSecurity for Networks.

Документация для Kaspersky Industrial CyberSecurity for Networks API публикуется в виде онлайн-справки на странице Kaspersky Online Help. Документация представляет собой руководство разработчика на английском языке. Руководство разработчика описывает программный интерфейс, используемый для RPC-запросов к Kaspersky Industrial CyberSecurity for Networks. В руководстве разработчика также представлены примеры кода и подробные описания вызываемых элементов, которые доступны в Kaspersky Industrial CyberSecurity for Networks API. Руководство разработчика Kaspersky Industrial CyberSecurity for Networks API адресовано специалистам, знакомым с языком программирования Python и с принципами разработки программ с использованием API.

Kaspersky Industrial CyberSecurity for Networks API использует протокол сетевого взаимодействия Google™ RPC. Библиотека Google RPC поддерживает широкий набор языков программирования.

Сертификаты для безопасного соединения через API

Клиентские приложения, подключающиеся к Серверу Kaspersky Industrial CyberSecurity for Networks через API, устанавливают безопасное соединение с использованием клиентских сертификатов и сертификата gRPC-сервера.

В процессе установки программы создаются следующие ключи и сертификаты:

- Сертификат gRPC-сервера (файл product_facade_grpc_server.crt).

  Этот сертификат используется клиентскими приложениями для аутентификации Сервера. Сервер использует этот сертификат для установки соединения с клиентскими узлами.

- Корневой сертификат gRPC-сервера (файл product_facade_grpc_ca.crt).

  Этот сертификат используется администратором для создания клиентских сертификатов. Клиентские приложения используют этот сертификат для подтверждения достоверности своих сертификатов (как часть цепочки сертификатов).

- Закрытый ключ gRPC-сервера (файл product_facade_grpc_ca.key).

  Этот закрытый ключ используется администратором для создания клиентских сертификатов.

По умолчанию указанные файлы расположены в директории /var/opt/kaspersky/kics4net/public_certs/. Доступ к этой директории предоставлен пользователю с root-правами, а также пользователям группы kics4net.

Для соединения с gRPC-сервером клиентское приложение должно использовать следующие сертификаты и ключи:

- Сертификат gRPC-сервера (файл product_facade_grpc_server.crt).

  Этот сертификат, созданный при установке программы, требуется для аутентификации Сервера.

- Цепочка сертификатов (файл client.crt).

  Эта цепочка сертификатов используется клиентским приложением для аутентификации. Цепочка сертификатов включает в себя клиентский сертификат, заверенный корневым сертификатом gRPC-сервера, и цепочку сертификатов до корневого сертификата gRPC-сервера.

- Закрытый ключ клиента (файл client.key).

  Этот закрытый ключ используется клиентским приложением при аутентификации.

Администратору требуется создать сертификаты и ключи для использования клиентскими приложениями (далее также "клиентские сертификаты"). Каждый клиентский сертификат должен быть создан на имя того компьютера, который будет подключаться к Серверу Kaspersky Industrial CyberSecurity for Networks через API.

Сведения об использовании клиентских сертификатов для установки соединения с Сервером Kaspersky Industrial CyberSecurity for Networks через API см. в документации для Kaspersky Industrial CyberSecurity for Networks API.

Создание клиентских сертификатов для подключения через API

Чтобы создать клиентские сертификаты, выполните следующие действия:

1. Получите от пользователя имя компьютера, для которого требуется создать клиентский сертификат.

2. Получите от пользователя запрос на подпись сертификата (Certificate Signing Request, далее CSR) для клиентского компьютера.

   Если требуется самостоятельно создать закрытый ключ клиента и CSR, вы можете использовать утилиту OpenSSL. Для этого введите команды:

   ```
   openssl genrsa -des3 -out client.key 4096
   openssl req -new -key client.key -out client.csr
   ```

3. Создайте сертификат на основе полученного CSR, используя корневой сертификат и закрытый ключ gRPC-сервера. Сертификат должен быть создан на имя клиентского компьютера, который будет использоваться для установки соединения (см. пункт 1).

   Для создаваемого сертификата укажите в параметрах утилиты OpenSSL срок действия сертификата в днях (параметр `days`) и серийный номер сертификата (параметр `set_serial`). Пример команды создания сертификата:

   ```
   openssl x509 -req -days 365 -in client.csr \
   -CA product_facade_grpc_ca.crt \
   -CAkey product_facade_grpc_ca.key \
   -set_serial 01 -out client.crt
   ```

4. Создайте цепочку сертификатов, включив корневой сертификат gRPC-сервера в итоговый клиентский сертификат.

   Если вы используете промежуточные сертификаты, они также должны быть включены в цепочку. Для создания цепочки сертификатов введите команду:

   ```
   cat product_facade_grpc_ca.crt >> client.crt
   ```

5. Передайте пользователю клиентского приложения следующие сертификаты и ключи:

   - Сертификат gRPC-сервера (файл product_facade_grpc_server.crt).

   - Закрытый ключ клиента (файл client.key).

     Этот файл нужно передавать только в том случае, когда закрытый ключ клиента был создан администратором.

   - Цепочка сертификатов или клиентский сертификат (файл client.crt).

     Этот файл включает в себя цепочку сертификатов, начиная от подписанного сертификата клиента и заканчивая корневым сертификатом gRPC-сервера.

   - Если требуется передавать клиентский сертификат отдельно, передайте также корневой сертификат gRPC-сервера (файл product_facade_grpc_ca.crt) и все промежуточные сертификаты, если они используются.

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.

Просматривая данные в блоках **Устройства** и **События**, вы можете контролировать наиболее значимые изменения в системе. Если вам нужно просмотреть более подробную информацию (например, об устройствах, требующих внимания), вы можете перейти к другим разделам веб-интерфейса программы или открыть всплывающую подсказку.

Для просмотра данных в онлайн-режиме вы также можете использовать раздел Теги, который позволяет просматривать теги со значениями параметров технологического процесса и контролировать текущее состояние Kaspersky Industrial CyberSecurity for Networks.

Информация в блоке Устройства

В блоке **Устройства** раздела **Мониторинг** отображается информация об устройствах, входящих в список известных программе устройств.

В блоке представлена следующая информация:

- Данные о количественном распределении известных программе устройств по категориям. Эти данные отображаются в верхней части блока **Устройства** 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 блока **Устройства** при наличии таких устройств. Пространство для отображения графических элементов ограничено размером блока **Устройства**.

Программа считает, что устройство требует внимания, в любом из следующих случаев:

- устройство имеет статус *Разрешенное* и состояние безопасности устройства отличается от *ОК*;

- 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 блоке **Устройства**. Количество графических элементов в

строке зависит от текущего размера окна веб-браузера. Если устройств, требующих внимания, больше, чем отображаемых графических элементов в строке, то справа отображается количество скрытых устройств в формате +<количество 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 *ОК*, *Важные события* или *Критические события*.

Графические элементы отображаются в следующем порядке:

1. Устройства с присвоенным статусом *Неразрешенное*.
2. Устройства, имеющие состояние безопасности *Критические события*.
3. Устройства, имеющие состояние безопасности *Важные события*.

Просмотр подробных сведений об устройствах

Для просмотра подробных сведений об устройствах вы можете перейти к таблице устройств с помощью элементов управления в блоке **Устройства** раздела **Мониторинг**. Предусмотрены следующие варианты:

- получение сведений о всех устройствах выбранной категории;
- получение сведений об устройствах, требующих внимания и относящихся к определенной категории;
- получение сведений об устройстве, требующем внимания;
- получение сведений о всех устройствах, известных программе.

Чтобы перейти к таблице устройств и просмотреть сведения о всех устройствах выбранной категории,

в верхней части блока **Устройства** нажмите на значок нужной категории.

В окне веб-браузера откроется раздел **Устройства**. В таблице устройств 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, нажмите на ссылку с количеством устройств нужной категории (ссылка отображается в конце строки со значком категории и текстовым комментарием **требующие внимания**).

В окне веб-браузера откроется раздел **Устройства**. В таблице устройств 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 блоке **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 блоке **Устройства** нажмите на графический элемент, представляющий нужное устройство.

В окне веб-браузера откроется раздел **Устройства**. В таблице устройств будет применена фильтрация по идентификатору устройства.

Чтобы перейти к таблице устройств и просмотреть сведения обо всех устройствах, известных программе,

в блоке **Устройства** нажмите на кнопку **Показать все устройства**.

В окне веб-браузера откроется раздел **Устройства**. В таблице устройств отобразятся устройства, удовлетворяющие параметрам фильтрации, которые были заданы ранее в таблице устройств.

Поиск устройств с переходом в раздел Устройства

При просмотре сведений в блоке **Устройства** раздела **Мониторинг** вы можете выполнять поиск устройств в таблице известных программе устройств.

Чтобы найти нужные устройства, выполните следующие действия:

1. В блоке **Устройства** введите поисковый запрос в поле **Поиск устройств**.
2. Нажмите на кнопку **Поиск**.

   В окне веб-браузера откроется раздел **Устройства**. В таблице устройств отобразятся устройства, которые удовлетворяют условиям поиска.

Информация в блоке События

В блоке **События** раздела **Мониторинг** отображается общая информация о событиях и инцидентах, имеющих наиболее поздние значения даты и времени последнего появления.

В блоке отображаются следующие элементы:

- Гистограмма событий и инцидентов за выбранный период. Эти данные отображаются в верхней части блока **События**. Гистограмма отображает распределение событий и инцидентов по уровням важности.
- Список с информацией о зарегистрированных событиях и инцидентах, отсортированный по дате и времени последнего появления. Эти данные отображаются в средней части блока **События**.

Статистика событий и инцидентов

На гистограмме распределения событий и инцидентов столбцы соответствуют суммарному количеству событий за каждый интервал времени. Внутри столбцов цветом обозначены уровни важности событий и инцидентов. Уровням важности соответствуют следующие цвета:

- Синий цвет. Этот цвет используется для событий и инцидентов с уровнем важности *Информационные*.
- Желтый цвет. Этот цвет используется для событий и инцидентов с уровнем важности *Важные*.
- Красный цвет. Этот цвет используется для событий и инцидентов с уровнем важности *Критические*.

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 важности.

Длительность интервалов времени зависит от выбранного периода для отображения. Для построения гистограммы предусмотрены следующие периоды:

- 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 одному дню.

Список событий и инцидентов

Список событий и инцидентов в блоке **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 блока **События**.

Для каждого события или инцидента в списке представлены следующие сведения:

- заголовок события или инцидента;
- дата и время последнего появления;
- значок, обозначающий уровень важности события или инцидента: *Информационные*, *Важные*, или *Критические*.

Инциденты в списке обозначаются значком .

Выбор периода для отображения гистограммы

Вы можете выбрать нужный период для построения гистограммы зарегистрированных событий и инцидентов в блоке **События** в разделе **Мониторинг**.

Чтобы построить гистограмму за нужный период,

в блоке **События** нажмите на одну из следующих кнопок:

- **1ч** – если вы хотите построить гистограмму за последний час;

- **12ч** – если вы хотите построить гистограмму за последние 12 часов;
- **24ч** – если вы хотите построить гистограмму за последние 24 часа;
- **7д** – если вы хотите построить гистограмму за последние семь дней.

На гистограмме распределения событий и инцидентов отобразятся сведения за выбранный период.

Просмотр подробных сведений о событиях и инцидентах

Для просмотра подробных сведений о событиях и инцидентах вы можете перейти к таблице событий с помощью элементов управления в блоке **События** раздела **Мониторинг**. Предусмотрены следующие варианты:

- получение сведений о событии или инциденте из числа отображаемых в блоке **События**;
- получение сведений обо всех событиях и инцидентах.

*Чтобы просмотреть подробные сведения о событии или инциденте, отображаемом в списке блока **События**,*

в блоке **События** нажмите на нужное событие или инцидент.

В окне веб-браузера откроется раздел **События**. В таблице событий будет применена фильтрация 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).

Чтобы просмотреть подробные сведения обо всех событиях и инцидентах,

в блоке **События** нажмите на кнопку **Показать все события**.

В окне веб-браузера откроется раздел **События**. В таблице событий отобразятся события и инциденты, удовлетворяющие параметрам фильтрации, которые были заданы ранее в таблице событий.

Поиск событий и инцидентов с переходом в разделу События

При просмотре сведений в блоке **События** раздела **Мониторинг** вы можете выполнять поиск событий и инцидентов в таблице событий.

Чтобы найти нужные события и инциденты, выполните следующие действия:

1. В блоке **События** введите поисковый запрос в поле **Поиск событий**.
2. Нажмите на кнопку **Поиск**.

   В окне веб-браузера откроется раздел **События**. В таблице событий отобразятся события и инциденты, которые удовлетворяют условиям поиска.

Работа с картой сети

Карта сети – это визуальное отображение обнаруженных взаимодействий между устройствами промышленной сети. С помощью карты сети вы можете просматривать сведения о взаимодействиях устройств в различные периоды времени.

На карте сети могут отображаться следующие объекты:

- Узлы. Эти объекты обозначают отправителей и получателей сетевых пакетов в обнаруженных взаимодействиях.
- 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 сети на основании данных, полученных из трафика за определенный промежуток времени. Группы устройств отображаются постоянно.

При необходимости вы можете использовать фильтрацию узлов и соединений. По умолчанию на карте сети в онлайн-режиме отображаются объекты с заданным периодом для фильтрации длительностью один час.

Объекты, требующие внимания, визуально выделяются на карте сети. Программа считает требующими внимания следующие объекты:

- Узел, если с этим узлом связаны необработанные события с уровнем важности *Важные* или *Критические*, либо если этот узел представляет устройство со статусом *Неразрешенное*.
- Соединение, если к нему относятся события с уровнем важности *Важные* или *Критические*. 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 сети

Узлы на карте сети 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 сети, 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 сети) 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.

Отображаемая информация на узлах, представляющих известные программе устройства

Для узлов, представляющих известные программе устройства, при максимальном масштабе карты сети отображается следующее:

- Заданное имя устройства.
- Значок категории устройства.
- IP-адрес устройства (если IP-адрес не задан, отображается MAC-адрес).
- Значок статуса устройства:
  - – устройство имеет статус *Разрешенное*;
  - – устройство имеет статус *Неразрешенное*;
  - – устройство имеет статус *Неиспользуемое*.
- Утолщенная линия на левой границе узла одного из следующих цветов в зависимости от состояния безопасности устройства:
  - зеленый цвет – состояние безопасности *ОК*;
  - желтый цвет – состояние безопасности *Важные события*;
  - красный цвет – состояние безопасности *Критические события*.
- Значок , если для устройства задан признак маршрутизирующего устройства.

Если устройство имеет статус *Неразрешенное* или состояние безопасности устройства отличается от состояния *ОК*, фон узла закрашен красным цветом.

Отображаемая информация на узлах, представляющих неизвестные программе устройства

Для узлов, представляющих неизвестные программе устройства, при максимальном масштабе карты сети 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 неизвестных устройств .
- Значок статуса неизвестных устройств .

Узлы, представляющие неизвестные программе устройства, фон узла закрашен серым цветом.

Отображаемая информация на узлах WAN

Для узлов WAN при максимальном масштабе карты сети отображается следующее:

- Имя узла: **WAN**.
- Значок узла WAN .

Группы устройств на карте сети

Группы из дерева групп устройств могут отображаться на карте сети в свернутом или развернутом состояниях.

Отображаемая информация на свернутых группах

Если группа свернута, при максимальном масштабе карты сети отображается следующее:

- Имя группы.
- Количество устройств, удовлетворяющих текущим параметрам фильтрации на карте сети. 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 сети.

Если группа содержит устройства или соединения, требующие внимания, (в том числе в дочерних группах любого уровня вложенности), окно закрашено красным фоном.

Соединения на карте сети

Соединения на карте сети 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 сети:

- узел, представляющий одно устройство;
- свернутая группа, если соединение показывает взаимодействие с одним или несколькими устройствами в этой группе;
- общий узел неизвестных устройств, если соединение показывает взаимодействие с одним или несколькими неизвестными устройствами этого узла.

В зависимости от уровней важности событий, зарегистрированных при обнаружении взаимодействий, линия соединения может быть окрашена следующими цветами:

- Серый цвет – взаимодействие не вызвало регистрацию событий или зарегистрированы только события с уровнем важности *Информационные.*

- Красный цвет – взаимодействие вызвало регистрацию событий с уровнем важности *Важные* или *Критические*.

Для соединений учитываются события, зарегистрированные в течение заданного периода для фильтрации объектов. При этом текущий статус событий не учитывается.

Просмотр подробных сведений об объектах

Подробные сведения об объектах, представленных на карте сети, 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.
- 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. Раздел отображается, если среди узлов неизвестных устройств есть узлы с IP-адресами.
  - **MAC-адреса** – количество MAC-адресов неизвестных устройств и первые 100 MAC-адресов. 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 масок подсетей, по которым определяются устройства внешней сети.

Для групп отображаются следующие сведения:

- Количество устройств и групп в выбранной группе и в ее дочерних группах всех уровней вложенности.
- Путь к группе в дереве групп устройств. Если группа относится к верхнему уровню иерархии, отображается **Группа верхнего уровня**.
- Сведения о количестве объектов, требующих внимания, в выбранной группе и в ее дочерних группах всех уровней вложенности. Если таких объектов нет, отображается состояние безопасности *ОК*.

Для соединений отображаются следующие сведения:

- **Уровень важности** – значок, соответствующий максимальному уровню важности событий, связанных с соединением. Если с соединением не связано ни одно событие, отображается **Без**

событий. Учитываются события, зарегистрированные в течение заданного периода 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).
  - 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.
- Если одной из сторон взаимодействия является свернутая группа, отображаются сведения о количестве соединений, обозначенных выбранным соединением:
  - **Всего соединений** – общее количество соединений с устройствами свернутой группы.
  - Список с количественным распределением соединений по уровням важности связанных с ними событий (в том числе указывается количество соединений, с которыми не связано ни одно событие). Рядом с элементами списка отображаются ссылки для просмотра подробных сведений об элементах. По ссылке **К устройствам** вы можете перейти в раздел **Устройства** и отфильтровать устройства, относящиеся к соединениям. По ссылке **К событиям** вы можете перейти в раздел **События** и отфильтровать события, с которыми связаны соединения.
- **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 и позиционирование карты сети

Карта сети может отображаться в масштабе 1–100%. Текущее значение масштаба отображается в панели инструментов, которая расположена в левой части области отображения карты сети.

Позиционирование карты сети можно изменять, перемещая ее по экрану.

При работе с картой сети вы можете использовать следующие функции:

- Изменение масштаба карты сети

Чтобы изменить масштаб карты сети,

используйте колесико мыши или кнопки + и –, расположенные в панели инструментов рядом с текущим значением масштаба.

При уменьшении масштаба карты сети 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.

- Изменение позиционирования карты сети

При необходимости вы можете изменить позиционирование карты сети вручную или автоматически. Автоматическое позиционирование позволяет переместить карту сети и изменить ее масштаб таким образом, чтобы на экране отображались все узлы, удовлетворяющие заданным параметрам фильтрации, а также все развернутые группы.

Чтобы позиционировать карту сети вручную, выполните следующие действия:

1. Наведите курсор мыши на любое место карты сети, не занятое объектами.
2. Удерживая нажатой левую клавишу мыши, перетащите изображение карты сети.

Чтобы автоматически позиционировать карту сети,

нажмите на кнопку  в панели инструментов, которая расположена в левой части области отображения карты сети.

Позиционирование и масштаб карты сети изменятся для отображения всех узлов и развернутых групп.

Сворачивание и разворачивание групп

Вы можете сворачивать и разворачивать группы устройств на карте сети. Свернутые группы отображаются в виде значков, аналогичных узлам. Развернутые группы отображаются в виде окон с включенными в них узлами и другими группами.

Чтобы развернуть группы на карте сети, выполните следующие действия:

1. На карте сети выберите одну или несколько свернутых групп.

   Для выбора нескольких свернутых групп выполните 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 сети (кнопка доступна, если выбрана хотя бы одна свернутая группа).

Чтобы свернуть развернутые группы на карте сети, выполните одно из следующих действий:

- Если вы хотите свернуть одну развернутую группу, нажмите на кнопку в заголовке окна этой группы.

- Если вы хотите свернуть все развернутые группы на карте сети, нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения карты сети (кнопка доступна, если развернута хотя бы одна группа).

Перемещение узлов и групп в другие группы на карте сети

Вы можете изменять размещение узлов и групп в дереве групп устройств, перетаскивая объекты на карте сети. 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, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.

2. В разделе **Карта сети** 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.

3. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.

4. Наведите курсор на один из выбранных объектов (группу или узел, представляющий известное программе устройство).

5. 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.

6. В окне запроса подтвердите перемещение выбранных объектов.

Закрепление и открепление узлов и групп

По умолчанию на карте сети не зафиксировано местоположение узлов и свернутых групп. До того как местоположение узлов и свернутых групп будет закреплено, они могут автоматически перемещаться для оптимального отображения остальных объектов.

Объекты, включенные в группы, могут перемещаться только в пределах групп, в которые они включены. Остальные объекты могут занимать любое место на карте сети, исключая пространства, занятые развернутыми группами.

Закрепление узлов и групп происходит при изменении их местоположения вручную или автоматически. Также вы можете закрепить текущее местоположение отображаемых узлов и свернутых групп в пределах одной группы или на всей карте сети.

После того, как местоположение узла или свернутой группы закреплено, в правом верхнем углу этого элемента отображается значок . Значок перестает отображаться при уменьшении масштаба карты сети до 25% и менее.

Местоположение закрепленного узла или закрепленной группы сохраняется. Если закрепленный узел перестал отображаться на карте сети (например, после применения фильтрации), при следующем появлении этот узел отобразится на том же месте.

Чтобы закрепить местоположение отображаемых узлов и свернутых групп, выполните одно из следующих действий:

- Если вы хотите закрепить местоположение всех отображаемых узлов и свернутых групп на карте сети, нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения карты сети (кнопка доступна, если на карте сети есть незакрепленные объекты).

- Если вы хотите закрепить местоположение отображаемых узлов и свернутых групп в окне развернутой группы, нажмите на кнопку в заголовке окна развернутой группы (кнопка доступна, если в окне группы есть незакрепленные объекты).

Чтобы открепить отображаемые узлы и свернутые группы, выполните одно из следующих действий:

- Если вы хотите открепить один узел или одну свернутую группу, нажмите на значок в правом верхнем углу узла или свернутой группы.

- Если вы хотите открепить все отображаемые узлы и свернутые группы на карте сети, нажмите на кнопку в панели инструментов, которая расположена в левой части области отображения карты сети (кнопка доступна, если на карте сети есть закрепленные объекты).

- Если вы хотите открепить отображаемые узлы и свернутые группы в окне развернутой группы, нажмите на кнопку в заголовке окна развернутой группы (кнопка доступна, если в окне группы есть закрепленные объекты).

Изменение местоположения узлов и групп вручную

Вы можете вручную изменять местоположение узлов и групп на карте сети, распределяя их наиболее удобным для вас способом.

После перемещения узлы и группы закрепляются на новом местоположении. При необходимости вы можете открeплять эти объекты.

Объекты, включенные в группы, можно перемещать только в пределах окон этих групп.

Чтобы изменить местоположение узлов и / или свернутых групп, выполните следующие действия:

1. На карте сети 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 клавишу мыши и перетащите окно в нужное место.

Автоматическое распределение узлов и групп

Для оптимального размещения объектов на карте сети 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 автоматически распределять следующие объекты:

- все отображаемые узлы и группы, относящиеся к верхнему уровню иерархии в дереве групп;
- все отображаемые узлы и группы, относящиеся к раскрытой группе;
- выбранные узлы и свернутые группы.

После автоматического распределения узлы и группы закрепляются на новом месте. В этих объектах появляется значок . При необходимости вы можете открепить эти объекты.

Чтобы автоматически распределить все отображаемые узлы и группы, относящиеся к верхнему уровню иерархии в дереве групп, выполните следующие действия:

1. В панели инструментов, которая расположена в левой части области отображения карты сети, нажмите на одну из следующих кнопок (кнопки доступны, если на карте сети есть отображаемые узлы или группы):

   - Если вы хотите распределить объекты по радиальному принципу, нажмите на кнопку .
   - Если вы хотите выровнять объекты по сетке, нажмите на кнопку .

   Откроется окно с запросом подтверждения.

2. В окне запроса подтвердите изменение местоположения объектов.

Чтобы автоматически распределить все отображаемые узлы и группы внутри развернутой группы, выполните следующие действия:

1. На карте сети разверните нужную группу.

2. В заголовке окна развернутой группы нажмите на одну из следующих кнопок (кнопки доступны, если в группе есть отображаемые узлы или группы):

   - Если вы хотите распределить объекты по радиальному принципу, нажмите на кнопку .
   - Если вы хотите выровнять объекты по сетке, нажмите на кнопку .

   Откроется окно с запросом подтверждения.

3. В окне запроса подтвердите изменение местоположения объектов.

Чтобы автоматически распределить только выбранные узлы и свернутые группы, выполните следующие действия:

1. На карте сети выберите несколько узлов и / или свернутых групп, выполнив одно из следующих действий:

   - Удерживая нажатой клавишу **SHIFT**, вы можете выделить мышью прямоугольную область с нужными объектами.
   - Удерживая нажатой клавишу **CTRL**, вы можете выбрать нужные объекты с помощью мыши.

2. В панели инструментов, которая расположена в левой части области отображения карты сети, нажмите на одну из следующих кнопок (кнопки доступны, если выбрано не менее трех объектов, имеющих общие соединения):

   - Если вы хотите распределить объекты по радиальному принципу, нажмите на кнопку .
   - Если вы хотите выровнять объекты по сетке, нажмите на кнопку .

   Откроется окно с запросом подтверждения.

3. В окне запроса подтвердите изменение местоположения объектов.

Фильтрация узлов и соединений по времени взаимодействий

Вы можете настроить фильтрацию узлов и соединений для отображения только тех из них, которым соответствуют взаимодействия в заданный период времени.

Выбор периода для фильтрации выполняется с помощью временной шкалы, которая отображается в нижней части раздела **Карта сети**. На временной шкале отображаются следующие элементы:

- Дата и время начала временной шкалы.
- Периоды, когда были зарегистрированы события с уровнями важности *Критические* и *Важные*. 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 окончанием временной шкалы.

- 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, выполните следующие действия:

1. Нажмите на кнопку **Сейчас** справа от временной шкалы.

   Вы также можете переместить период к правой части временной шкалы с помощью мыши.

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 для выбора длительности периода с помощью кнопки с текущей длительностью периода над желтой полосой периода, выберите нужный вариант (**Час**, **День**, **7 дней**) и нажмите на кнопку **ОК**.

   На карте сети 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, выполните следующие действия:

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**.

      - **Месяц**.

      - **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 одну или обе границы желтой полосы периода в нужную часть временной шкалы (максимальная длительность периода – 7 дней).
- Откройте окно для выбора длительности периода с помощью графического элемента над желтой полосой периода, выберите нужный вариант (**Час**, **День**, **7 дней**) и нажмите на кнопку **ОК**.

Вы также можете переместить период в нужную часть временной шкалы с помощью мыши.

На карте сети отобразятся только те узлы и соединения, для которых были обнаружены взаимодействия в течение времени заданного периода.

Фильтрация узлов на карте сети

По умолчанию на карте сети отображаются все узлы, между которыми были обнаружены взаимодействия в течение заданного периода времени. Для ограничения количества отображаемых узлов на карте сети вы можете использовать следующие функции:

- Фильтрация по статусам устройств

  Чтобы отфильтровать узлы на карте сети по статусам устройств, выполните следующие действия:

  1. В панели инструментов, которая расположена над картой сети, 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 сети.

  3. Нажмите на кнопку **ОК**.

  На карте сети отобразятся только те узлы, которые представляют устройства с выбранными статусами.

- Фильтрация по состояниям безопасности устройств

  Чтобы отфильтровать узлы на карте сети по состояниям безопасности устройств, выполните следующие действия:

  1. В панели инструментов, которая расположена над картой сети, откройте раскрывающийся список **Состояния устройств**.

     Появится список, содержащий названия состояний безопасности для устройств (**ОК**, **Важные события**, **Критические события**).

  2. В раскрывающемся списке установите флажки для тех состояний безопасности, узлы с которыми нужно отобразить на карте сети.

  3. Нажмите на кнопку **ОК**.

  На карте сети отобразятся только те узлы, которые представляют устройства с выбранными состояниями безопасности.

- Фильтрация по категориям устройств

Чтобы отфильтровать узлы на карте сети по категориям устройств, выполните следующие действия:

1. В панели инструментов, которая расположена над картой сети, 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 сети.

3. Нажмите на кнопку **ОК**.

   На карте сети отобразятся только те узлы, которые представляют устройства выбранных категорий.

После фильтрации на карте сети отображаются только те узлы, которые удовлетворяют заданным параметрам фильтрации. При этом для отображения узла на карте сети требуется, чтобы этот узел имел соединение с другим отображаемым узлом. Если по заданным параметрам фильтрации на карте сети не отображаются все узлы, с которыми были обнаружены взаимодействия узла, этот узел также не отображается на карте сети. 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 сети всех узлов, связанных с отфильтрованными узлами. Вместе с узлами, удовлетворяющими заданным параметрам фильтрации узлов, на карте сети 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 сети отобразятся все узлы, с которыми взаимодействовали устройства категории **ПЛК**. Если отображение связанных узлов выключено, на карте сети 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 сети.

Фильтрация соединений на карте сети

По умолчанию на карте сети отображаются все соединения, для которых были обнаружены взаимодействия в течение заданного периода времени. Для ограничения количества отображаемых соединений на карте сети вы можете использовать следующие функции:

- Фильтрация по уровням важности событий

  Чтобы отфильтровать соединения на карте сети по уровням важности событий, выполните следующие действия:

  1. В панели инструментов, которая расположена над картой сети, откройте раскрывающийся список **Важность соединений**.

     Появится список, содержащий названия уровней важности событий (**Информационные события**, **Важные события**, **Критические события**), а также элемент **Без событий**, позволяющий выполнить фильтрацию соединений, для которых не зарегистрированы события.

  2. В раскрывающемся списке установите флажки для тех уровней важности, по которым вы хотите выполнить фильтрацию.

  3. Нажмите на кнопку **ОК**.

     На карте сети отобразятся только те соединения, с которыми связаны события с выбранными уровнями важности.

- Фильтрация по протоколам взаимодействий

Чтобы отфильтровать соединения на карте сети по протоколам взаимодействий, выполните следующие действия:

1. В панели инструментов, которая расположена над картой сети, 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 графах 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 **ОК**.

На карте сети отобразятся только те соединения, в которых использовались выбранные протоколы.

- Фильтрация 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 сети по уровням сетевой модели OSI, выполните следующие действия:

1. В панели инструментов, которая расположена над картой сети, 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 сети.

3. Нажмите на кнопку **ОК**.

На карте сети отобразятся только те соединения, которые относятся к выбранному уровню модели OSI.

Сохранение и загрузка параметров отображения карты сети

Программа позволяет сохранить текущие параметры отображения карты сети. Набор сохраняемых параметров отображения называется *видом*. Вы можете использовать виды для применения сохраненных в них параметров на карте сети (например, чтобы быстро восстановить параметры отображения после каких-либо изменений или для работы с картой сети на другом компьютере).

При сохранении вида карты сети сохраняются следующие параметры отображения:

- местоположение закрепленных узлов и групп;
- масштаб и позиционирование карты сети;
- фильтрация узлов;
- фильтрация соединений.

В программе можно сохранить и использовать не более 10 наборов параметров, представляющих различные виды карты сети.

Управлять списком видов карты сети (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.

Для работы с видами карты сети вы можете использовать следующие функции:

- Добавление нового вида с сохранением текущих параметров отображения карты сети

  Чтобы добавить новый вид и сохранить в нем текущие параметры отображения карты сети, выполните следующие действия:

  1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
  2. В разделе **Карта сети** настройте параметры отображения карты сети.
  3. Нажмите на кнопку **Настроить виды**.
     Появится окно **Настройка видов карты сети**.
  4. Нажмите на кнопку **Добавить текущий**.
  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 сети

  Чтобы обновить вид и сохранить в нем текущие параметры отображения карты сети, выполните следующие действия:

  1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
  2. В разделе **Карта сети** настройте параметры отображения карты сети.
  3. Нажмите на кнопку **Настроить виды**.
     Появится окно **Настройка видов карты сети**.
  4. Выберите вид, в котором вы хотите сохранить текущие параметры отображения карты сети.
  5. Нажмите на кнопку **Перезаписать**.
     Откроется окно с запросом подтверждения.
  6. В окне запроса подтвердите сохранение текущих параметров в выбранном виде.

- Переименование вида карты сети

Чтобы переименовать вид, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Карта сети** нажмите на кнопку **Настроить виды**.
   Появится окно **Настройка видов карты сети**.
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 сети

Чтобы удалить вид, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер с учетными данными пользователя с ролью Администратор.
2. В разделе **Карта сети** нажмите на кнопку **Настроить виды**.
   Появится окно **Настройка видов карты сети**.
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 сети параметров, сохраненных в виде

Чтобы применить на карте сети параметры, сохраненные в виде, выполните следующие действия:

1. В разделе **Карта сети** нажмите на кнопку **Настроить виды**.
   Появится окно **Настройка видов карты сети**.
2. Выберите нужный вид в списке.
3. Нажмите на кнопку **Применить**.
   Откроется окно с запросом подтверждения.
4. В окне запроса подтвердите применение вида.

Сброс заданных параметров фильтрации на карте сети

Вы можете сбросить заданные параметры фильтрации узлов и соединений в состояние по умолчанию.

Чтобы сбросить заданные параметры фильтрации на карте сети,

в панели инструментов, которая расположена над картой сети, нажмите на кнопку **Очистить фильтр** (кнопка отображается, если заданы параметры фильтрации).

На карте сети отобразятся все узлы и соединения, для которых были обнаружены взаимодействия в течение времени заданного периода.

Поиск узлов на карте сети

Вы можете выполнять поиск узлов на карте сети 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 сети.

Для узлов, представляющих известные программе устройства, поиск выполняется по всем графам таблицы устройств, кроме граф **Статус**, **Состояние безопасности**, **Последнее появление**, **Последнее изменение** и **Дата создания**. Поиск также выполняется по значениям пользовательских полей для устройств.

Чтобы найти нужные узлы на карте сети, выполните следующие действия:

1. 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 сведения:

   - 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.

2. Для переходов между найденными объектами используйте кнопки в виде стрелок в правой части поля **Поиск узлов**. Переходы выполняются в алфавитном порядке имен найденных объектов. При переходе к очередному объекту карта сети автоматически позиционируется для отображения этого объекта.

Просмотр событий, связанных с узлами известных программе устройств

Для узлов на карте сети, представляющих известные программе устройства, вы можете просмотреть связанные с ними события. При загрузке событий автоматически применяется фильтрация по идентификаторам известных программе устройств с использованием значений MAC- и IP-адресов, которые указаны для устройств.

Возможность загрузки событий доступна, если выбрано не более 200 узлов на карте сети. 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 просмотреть события, связанные с устройствами, выполните следующие действия:

1. На карте сети выберите один или несколько объектов, представляющих 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.

2. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.

3. В зависимости от того, какие события вы хотите загрузить, нажмите на одну из следующих кнопок (кнопки недоступны, если общее количество известных программе устройств в выборке превышает 200):

   - **Показать события** – если вы хотите просмотреть события с любым статусом.
   - **Показать необработанные события** – если вы хотите просмотреть события со статусами *Новое* или *В обработке*.

   Откроется раздел **События**. В таблице событий будет применена фильтрация по идентификаторам устройств, которым соответствуют выбранные узлы на карте сети (появится поле **ID устройств** в панели инструментов). Если вы загрузили события с помощью кнопки **Показать необработанные события**, события дополнительно отфильтруются по графе **Статус**.

Просмотр событий, связанных с соединением

Для соединений на карте сети вы можете просмотреть связанные с ними события. При загрузке событий применяется фильтрация по идентификаторам событий, связанных с соединением, и по периоду времени.

Для загрузки событий, связанных с соединениями, вы можете использовать следующие способы:

- Загрузка событий, связанных с выбранным соединением. Этот способ можно использовать для любых соединений, кроме соединений с общим узлом неизвестных устройств.
- Загрузка событий, связанных с соединениями с узлами в свернутой группе.

Программа загружает для просмотра не более 200 событий, связанных с соединением. Если событий больше, в первую очередь отбираются события с наиболее высокими уровнями важности и с наиболее поздним временем появления событий.

Чтобы просмотреть события, связанные с соединением, выполните следующие действия:

1. На карте сети выберите соединение (кроме соединения, в котором одной из сторон взаимодействия является общий узел неизвестных устройств).

   В правой части окна веб-интерфейса появится область деталей.

2. В зависимости от того, какие события вы хотите загрузить, нажмите на одну из следующих кнопок (кнопки доступны, если есть события, связанные с соединением):

   - **Показать события** – если вы хотите просмотреть события с любым статусом.

   - **Показать необработанные события** – если вы хотите просмотреть события со статусами *Новое* или *В обработке*.

3. Если в течение периода времени, заданного на карте сети, было зарегистрировано более 200 событий, связанных с соединением, отобразится предупреждение о большом количестве событий. Для загрузки событий с наиболее высокими уровнями важности подтвердите решение в окне запроса.

Откроется раздел **События**. В таблице событий будет применена фильтрация по идентификаторам событий и по периоду времени, заданному на карте сети. Если вы загрузили события с помощью кнопки **Показать необработанные события**, события дополнительно отфильтруются по графе **Статус**.

Чтобы просмотреть события, связанные с соединениями узлов в свернутых группах, выполните следующие действия:

1. На карте сети выберите соединение, показывающее взаимодействия с узлами в свернутой группе.

   В правой части окна веб-интерфейса появится область деталей. Блок параметров **Всего соединений: <количество>** содержит список максимальных уровней важности событий в соединениях с узлами свернутой группы. Для каждого уровня важности отображается количество соединений с этим уровнем важности. Отображаются только те уровни важности, с которыми есть соединения с узлами свернутой группы. Если есть соединения, с которыми не связано ни одно событие, отображается **Без событий** с количеством таких соединений.

2. Загрузите события по ссылке **К событиям** в строке с нужным уровнем важности.

   Вы можете загрузить следующие события:

   - для уровня **Критические** – загружаются события, связанные с соединениями с уровнем важности **Критические**;

   - для уровня **Важные** – загружаются события, связанные с соединениями с уровнями важности **Важные** и **Критические**;

   - для уровня **Информационные** – загружаются события, связанные с соединениями с уровнями важности **Информационные**, **Важные** и **Критические**.

3. Если в течение периода времени, заданного на карте сети, было зарегистрировано более 200 событий, связанных с соединениями выбранных уровней важности, отобразится предупреждение о большом количестве событий. Для загрузки событий с наиболее высокими уровнями важности подтвердите решение в окне запроса.

Откроется раздел **События**. В таблице событий будет применена фильтрация по идентификаторам событий и по периоду времени, заданному на карте сети.

Просмотр сведений в таблице устройств по выбранным узлам

Для узлов на карте сети, представляющих известные программе устройства, вы можете просмотреть сведения в таблице устройств. В таблице устройств автоматически применяется фильтрация по идентификаторам известных программе устройств.

Возможность загрузки сведений доступна, если выбрано не более 200 узлов, представляющих известные программе устройства. 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 просмотреть сведения об устройствах в таблице устройств, выполните следующие действия:

1. На карте сети выберите один или несколько объектов, представляющих 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.

   В правой части окна веб-интерфейса появится область деталей. В области деталей отобразится общее количество выбранных узлов и групп с количественным распределением выбранных объектов по типам.

2. Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программе устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.

3. В зависимости от количества выбранных объектов нажмите на кнопку **Показать устройство** или **Показать устройства** (кнопка **Показать устройства** недоступна, если общее количество известных программе устройств в выборке превышает 200).

   Откроется раздел **Устройства**. В таблице устройств будет применена фильтрация по идентификаторам устройств, которым соответствуют выбранные узлы на карте сети.

Просмотр сведений в таблице устройств по выбранному соединению

Для соединений на карте сети вы можете просмотреть сведения об известных программе устройствах, участвовавших во взаимодействиях. Для загрузки сведений выполняется переход к таблице устройств. В таблице устройств автоматически применяется фильтрация по идентификаторам известных программе устройств.

Вы можете просматривать сведения в таблице устройств только для соединений с узлами в свернутых группах.

Программа загружает для просмотра не более 200 устройств, относящихся к соединениям с узлами в свернутых группах. Если устройств больше, в первую очередь отбираются устройства, относящиеся к соединениям с наиболее высокими уровнями важности.

Чтобы просмотреть сведения об устройствах, относящихся к соединениям с узлами в свернутых группах, выполните следующие действия:

1. На карте сети выберите соединение, показывающее взаимодействия с узлами в свернутой группе.

   В правой части окна веб-интерфейса появится область деталей. Блок параметров **Всего соединений: <количество>** содержит список максимальных уровней важности событий в соединениях с узлами свернутой группы. Для каждого уровня важности отображается количество соединений с этим уровнем важности. Отображаются только те уровни важности, с которыми есть соединения с узлами свернутой группы. Если есть соединения, с которыми не связано ни одно событие, отображается **Без событий** с количеством таких соединений.

2. Загрузите сведения об устройствах по ссылке **К устройствам** в строке с нужным уровнем важности.

   Вы можете загрузить следующие сведения об устройствах:

   - для уровня **Критические** – загружаются сведения об устройствах, относящихся к соединениям с уровнем важности **Критические**;
   - для уровня **Важные** – загружаются сведения об устройствах, относящихся к соединениям с уровнями важности **Важные** и **Критические**;
   - для уровня **Информационные** – загружаются сведения об устройствах, относящихся к соединениям с уровнями важности **Информационные**, **Важные** и **Критические**;
   - для уровня **Без событий** – загружаются сведения об устройствах, относящихся к соединениям со всеми уровнями важности.

3. Если общее количество известных программе устройств в выборке превысило 200, отобразится предупреждение о большом количестве устройств. Для загрузки устройств, относящиеся к соединениям с наиболее высокими уровнями важности, подтвердите решение в окне запроса.

Откроется раздел **Устройства**. В таблице устройств будет применена фильтрация по идентификаторам устройств.

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 используются системные типы событий, которым присвоены коды 8000000000, 8000000001, 8000000002 и 8000000003.

Правила корреляции событий встроены в программу и применяются независимо от политики безопасности, которая загружена в Консоль или применена на Сервере.

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 и передает сведения о них в сторонние системы в соответствии с параметрами, заданными для регистрации типов событий. Вы можете настроить эти параметры в Консоли программы на закладке **Настройка событий**. Сведения о настройке см. в разделе Настройка событий.

Параметры хранения событий и инцидентов настраиваются в окне Управление журналами Консоли программы. По умолчанию база данных хранит 100 000 записей в течение 365 дней. Если количество записей или период хранения превышают предельные значения, самые старые записи удаляются. При необходимости вы можете изменить количество хранимых записей, а также время их хранения.

Программа сохраняет события и инциденты в базе данных на Сервере.

Удаление или изменение любого файла в директориях СУБД 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.
- Раздел События – отображает подробную информацию о событиях и инцидентах и предоставляет возможность загрузки информации из базы данных Сервера за любой период.

Уровни важности событий

События и инциденты в Kaspersky Industrial CyberSecurity for Networks классифицируются по следующим уровням важности:

- *Информационные* (обозначаются значком).

  Информационные события и инциденты содержат сведения справочного характера. Эти события обычно не требуют немедленной реакции.

- *Важные* (обозначаются значком).

  Важные события и инциденты содержат сведения, на которые нужно обратить внимание. Эти события могут требовать реакции.

- *Критические* (обозначаются значком).

  Критические события и инциденты содержат сведения, которые могут оказать критическое влияние на технологический процесс. Эти события требуют немедленной реакции.

Вы можете задать уровни важности для пользовательских типов событий. Уровни важности для системных типов событий (включая события инцидентов) присваиваются программой автоматически.

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 внешних систем с использованием методов Kaspersky Industrial CyberSecurity for Networks API.

- *Контроль устройств* (AM).

  По этой технологии регистрируются события, связанные с обнаружением в трафике информации об устройствах (например, событие при обнаружении нового IP-адреса у устройства).

Вы можете задать технологию *Контроль технологического процесса* или *Внешние системы* для пользовательских типов событий. Технологии для системных типов событий присваиваются программой автоматически.

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* (обозначается значком).

  Этот статус присваивается всем событиям и инцидентам при их регистрации в Kaspersky Industrial CyberSecurity for Networks.

- *В обработке* (обозначается значком).

Этот статус вы можете присвоить событиям и инцидентам, которые находятся в обработке (например, во время расследования причин регистрации этих событий и инцидентов).

- *Обработано* (обозначается значком ☑).

  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 сети.

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** веб-интерфейса программы.

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 графе **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.

При работе с таблицей событий и инцидентов вы можете выполнять следующие действия:

- управлять отображением событий в инцидентах;
- фильтровать события;
- осуществлять поиск событий;
- сортировать события;
- настраивать таблицу зарегистрированных событий;
- просматривать подробные данные о событии;
- изменять статусы событий;
- просматривать в таблице устройств сведения по событиям;
- устанавливать метки;
- копировать события в текстовый редактор;

- экспортировать события в файл;
- загружать трафик событий.

Параметры отображения таблицы событий (например, параметры фильтрации) автоматически сохраняются для текущего пользователя программы. Сохраненные параметры применяются при следующем подключении этого пользователя к Серверу, если для подключения используются те же компьютер, веб-браузер и учетная запись операционной системы.

Выбор событий в таблице событий

В таблице событий вы можете выбирать события и инциденты для просмотра сведений и для работы с этими событиями и инцидентами. При выборе событий и инцидентов в правой части окна веб-интерфейса появляется область деталей.

Чтобы выбрать нужные события и / или инциденты, выполните одно из следующих действий:

- Если вы хотите выбрать одно событие или инцидент, установите флажок напротив этого события или инцидента или выберите его с помощью мыши.
- Если вы хотите выбрать несколько событий и / или инцидентов, установите флажки напротив нужных событий и / или инцидентов или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**. При выборе нескольких событий и / или инцидентов программа проверяет их статус и определяет наличие событий и / или инцидентов со статусами *Новое*, *В обработке* и *Обработано* среди выбранных.
- Если вы хотите выбрать все события и инциденты, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:
  - выберите любое событие или инцидент в таблице и нажмите комбинацию клавиш **CTRL+A**;
  - установите флажок в заголовке левой крайней графы таблицы.

При выборе нескольких событий и / или инцидентов в области деталей отображается общее количество выбранных элементов. При этом вложенные элементы свернутых инцидентов (события и другие инциденты) не учитываются.

Если вы выбрали все события и инциденты, удовлетворяющие текущим параметрам фильтрации и поиска, вложенные элементы свернутых инцидентов учитываются в общем количестве выбранных элементов. В области деталей отображается одно из следующих значений:

- Если выбрано до 1000 событий и инцидентов включительно, отображается точное количество. В этом случае программа проверяет статусы выбранных событий и инцидентов, как и при других способах выбора нескольких элементов.
- Если выбрано более 1000 событий и инцидентов, отображается **1000+**. В этом случае программа не проверяет статусы выбранных событий и инцидентов.

В заголовке левой крайней графы таблицы отображается флажок выбора событий и инцидентов. В зависимости от количества выбранных элементов в таблице флажок может быть в одном из следующих состояний:

- ▢ – в таблице не выполнялся выбор всех событий и инцидентов, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбрано одно событие / инцидент или выбрано несколько событий и / или инцидентов с помощью флажков напротив событий и инцидентов или с использованием клавиш **CTRL** или **SHIFT**.

- ☑ – в таблице выбраны все события и инциденты, удовлетворяющие текущим параметрам фильтрации и поиска.

- ▣ – в таблице были выбраны все события и инциденты, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых из них были сняты флажки. Это состояние сохраняется и в случае, если флажки сняты для всех событий и инцидентов, выбранных таким способом (из-за того, что количество выбранных событий и инцидентов может измениться).

Если выбраны все события и инциденты, удовлетворяющие параметрам фильтрации и поиска, количество выбранных элементов может автоматически изменяться. Например, если зарегистрированы новые события или инциденты. Рекомендуется настраивать параметры фильтрации и поиска таким образом, чтобы в выборку попали только нужные элементы (например, перед выбором всех событий и инцидентов вы можете отфильтровать события по идентификаторам).

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 включают вложенные события и могут быть свернуты или развернуты в таблице событий.

Вы можете изменить режим отображения при настройке таблицы событий.

Чтобы развернуть или свернуть строки с информацией о вложенных элементах инцидента в режиме отображения структур,

нажмите кнопку ⊞ или ⊟ в ячейке с заголовком инцидента.

Фильтрация событий

Для ограничения количества событий и инцидентов, отображаемых в таблице событий, вы можете использовать следующие функции:

- Фильтрация по стандартным периодам

При фильтрации по стандартному периоду таблица событий обновляется в онлайн-режиме.

Чтобы настроить фильтрацию событий и инцидентов по стандартному периоду, выполните следующие действия:

1. В разделе **События** выполните одно из следующих действий:
   - откройте раскрывающийся список **Период**;
   - нажмите на значок фильтрации в графе **Последнее появление**.
2. В раскрывающемся списке выберите один из стандартных периодов:
   - **Последний час**.
   - **Последние 12 часов**.
   - **Последние 24 часа**.
   - **Последние 48 часов**.
3. Если обновление таблицы выключено, в открывшемся окне подтвердите, что вы согласны возобновить обновление таблицы.

В таблице отобразятся события и инциденты за указанный вами период.

- Фильтрация по заданному периоду

При фильтрации по заданному периоду таблица перестает обновляться. В таблице отображаются только те события и инциденты, у которых дата и время последнего появления входят в указанный период.

Чтобы настроить фильтрацию событий и инцидентов по заданному периоду, выполните следующие действия:

1. В разделе **События** выполните одно из следующих действий:
   - откройте раскрывающийся список **Период**;
   - нажмите на значок фильтрации в графе **Последнее появление**.
2. В раскрывающемся списке выберите **Задать период**.
3. Если обновление таблицы включено, в открывшемся окне подтвердите, что вы согласны приостановить обновление таблицы.

   Справа появятся дополнительные кнопки, с помощью которых вы можете задать период фильтрации вручную.
4. Нажмите на любую из кнопок со значением даты и времени в полях **От** и **до**.

   Откроется календарь.
5. В поле под календарем слева укажите дату и время начальной границы периода фильтрации. В поле под календарем справа укажите дату и время конечной границы периода фильтрации. Если вы хотите снять ограничение для конечной границы периода, удалите значение в поле под календарем справа.

   Для ввода значения в поле вы можете выбрать дату в календаре (при этом для выбранной даты будет указано текущее время) или ввести нужное значение вручную. При вводе даты и времени вручную требуется ввести значение в формате ДД.ММ.ГГГГ чч:мм:сс.
6. Нажмите на кнопку **ОК**.

В таблице событий отобразятся события и инциденты за указанный вами период.

- Фильтрация по графам таблицы

Вы можете настроить фильтрацию событий и инцидентов по значениям во всех графах, кроме граф **Завершение**, **Заголовок** и **Описание**.

*Чтобы отфильтровать таблицу событий по графе **Начало**, выполните следующие действия:*

1. В разделе **События** нажмите на значок фильтрации в графе **Начало**.

   Откроется календарь.

2. В календаре задайте дату и время 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 вы хотите снять ограничение для одной из границ периода, удалите значение в поле под календарем.

3. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать таблицу событий по графе **Важность**, **Технология**, **Статус**, **Точка мониторинга** или **Метка**, выполните следующие действия:*

1. В разделе **События** нажмите на значок фильтрации в нужной графе.

   При фильтрации по уровням важности или по технологиям вы также можете воспользоваться соответствующими кнопками в панели инструментов.

   Откроется окно фильтрации.

2. Установите флажки напротив значений, по которым вы хотите выполнить фильтрацию. Для выбора всех значений в графах **Метка** и **Технология** вы можете установить флажок **Все**.

3. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать таблицу событий по графе **Отправитель** или **Получатель**, выполните следующие действия:*

1. В разделе **События** нажмите на значок фильтрации в нужной графе.

   Откроется окно фильтрации.

2. В полях **Включая** и **Исключая** выберите в раскрывающихся списках типы адресных блоков, которые вы хотите включить в фильтрацию и / или исключить из фильтрации. Вы можете выбрать следующие типы адресных блоков:

   - **IP-адрес**.
   - **Номер порта**.
   - **MAC-адрес**.
   - **Адрес прикладного уровня**.
   - VLAN ID.
   - **Комплексный** – если вы хотите указать несколько адресных блоков разных типов, объединенных логическим оператором И. Для добавления адресных блоков разных типов используйте кнопку **Добавить условие (И)**.

3. Если вы хотите применить несколько условий фильтрации по типам адресных блоков, объединенных логическим оператором ИЛИ, в окне фильтрации нажмите на кнопку **Добавить условие (ИЛИ)** и выберите нужные типы адресов.

4. Если вы хотите удалить одно из созданных условий фильтрации, в окне фильтрации нажмите на значок ✕, который расположен справа от поля с раскрывающимся списком.

5. Нажмите на кнопку **ОК**.

*Чтобы отфильтровать таблицу событий по графе **Протокол**, выполните следующие действия:*

1. В разделе **События** нажмите на значок фильтрации в графе **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.

   В графах 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 **ОК**.

*Чтобы отфильтровать таблицу событий по графе **Всего появлений**, **ID**, **Сработавшее правило** или **Тип события**, выполните следующие действия:*

1. В разделе **События** нажмите на значок фильтрации в нужной графе.

   Откроется окно фильтрации.

2. В полях **Включая** и **Исключая** введите значения для событий и инцидентов, которые вы хотите включить в фильтрацию и / или исключить из фильтрации.

3. Если вы хотите применить несколько условий фильтрации, объединенных логическим оператором ИЛИ, в окне фильтрации выбранной графы нажмите на кнопку **Добавить условие** и введите условие в открывшемся поле.

4. Если вы хотите удалить одно из созданных условий фильтрации, в окне фильтрации выбранной графы нажмите на значок .

5. Нажмите на кнопку **ОК**.

- Фильтрация по значениям в ячейках таблицы

Вы можете отфильтровать таблицу событий по значениям в ячейках любой графы, кроме граф **Начало**, **Последнее появление**, **Заголовок**, **Описание** и **Завершение**.

Чтобы отфильтровать таблицу по значениям параметров в ячейках таблицы, выполните следующие действия:

1. Выберите раздел **События**.

2. В таблице событий установите флажок напротив события или инцидента, по параметру которого вы хотите выполнить фильтрацию.

   Если вы хотите выбрать несколько событий и / или инцидентов, установите флажки напротив событий и / или инцидентов, по параметрам которых вы хотите выполнить фильтрацию. Вы также можете выбрать несколько событий и / или инцидентов, удерживая нажатой клавишу **CTRL** или **SHIFT**.

   В правой части окна веб-интерфейса появится область деталей. Если выбрано несколько событий и / или инцидентов, в области деталей отобразится общее количество выбранных элементов.

3. В таблице событий наведите курсор мыши на ячейку нужной графы одного из выбранных событий или инцидентов.

4. По правой клавише мыши откройте контекстное меню.

5. В контекстном меню выберите один из следующих пунктов:

   - **Показать все события с данным значением параметра**, если выбрано одно событие или инцидент.
   - **Показать все события с данными значениями параметра**, если выбрано несколько событий и / или инцидентов.

   Пункт **Показать все события с данным значением параметра** или **Показать все события с данными значениями параметра** недоступен для выбора, если невозможно выполнить фильтрацию по значениям графы.

В таблице зарегистрированных событий отобразятся события и инциденты, у которых в этой же графе содержатся значения, совпадающие со значениями выбранных событий и / или инцидентов.

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 событий

Вы можете выполнять поиск событий и инцидентов в таблице событий.

Поиск выполняется по графам, содержащим символьные значения (буквы и / или цифры), кроме граф **Начало**, **Последнее появление**, **Завершение** и **Всего появлений**.

Чтобы найти нужные события и инциденты,

в разделе **События** введите поисковый запрос в поле **Поиск событий**. Поиск инициируется по мере ввода символов в строку поиска.

В таблице отобразятся события и инциденты, которые удовлетворяют условиям поиска.

При поиске 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 условиям поиска.

Вы можете выбрать нужный вариант представления инцидентов с помощью флажка **Показывать вложенные при фильтрации** при настройке таблицы.

Сброс заданных параметров фильтрации и поиска в таблице событий

Вы можете сбросить заданные параметры фильтрации и поиска в таблице событий в состояние по умолчанию.

Чтобы сбросить заданные параметры фильтрации и поиска в таблице событий,

в панели инструментов в разделе **События** нажмите на кнопку **Очистить фильтр** (кнопка отображается, если заданы параметры фильтрации и / или поиска).

Сортировка событий

Вы можете отсортировать события и инциденты, отображаемые в разделе **События** веб-интерфейса программы. Сортировку можно выполнить по значениям любой графы, кроме графы **Описание**.

По умолчанию строки таблицы отсортированы по графе **Последнее появление** в порядке убывания значений даты и времени последнего появления событий. При изменении сортировки по умолчанию программа перестает обновлять события в таблице.

Чтобы отсортировать события и инциденты, выполните следующие действия:

1. В разделе **События** нажмите на заголовок графы, по которой вы хотите выполнить сортировку.
2. При сортировке событий по графе **Получатель** или **Отправитель** в раскрывающемся списке заголовка графы выберите адрес получателя или отправителя, по которому будет выполняться сортировка.

   В зависимости от выбранных значений для отображения в этих графах, вы можете выбрать один из следующих элементов:

   - IP-адрес.
   - Номер порта.
   - MAC-адрес.
   - VLAN ID.

- **Адрес прикладного уровня**.

3. Если требуется отсортировать таблицу по нескольким графам, нажмите на клавишу **SHIFT** и, удерживая ее нажатой, нажмите на заголовки граф, по которым нужно выполнить сортировку.

4. Если обновление таблицы включено, в открывшемся окне подтвердите, что вы согласны приостановить обновление таблицы.

Таблица будет отсортирована по выбранной графе. При сортировке по нескольким графам строки таблицы сортируются в соответствии с последовательностью выбора граф. Рядом с заголовками граф, по которым выполнена сортировка, появляются значки, показывающие текущий порядок сортировки: по возрастанию или по убыванию значений.

Настройка таблицы зарегистрированных событий

Вы можете настраивать следующие параметры отображения таблицы событий:

- отображение информационной панели;
- отображение событий, включенных в инциденты;
- состав и порядок граф, отображаемых в таблице.

Чтобы настроить параметры отображения таблицы событий, выполните следующие действия:

1. В разделе **События** нажмите на кнопку **Настроить таблицу**.

   Откроется окно для настройки отображения таблицы событий.

2. Если вы хотите включить отображение информационной панели, показывающей количество событий со статусами *Новое* и *В обработке*, установите флажок **Отображать информационную панель**.

3. В блоке параметров **Отображение вложенных списков** выберите нужный режим отображения событий, включенных в инциденты:

   - **Простой вид**. В этом режиме в таблице событий отображаются все события без учета вложенности событий в инциденты.
   - **Структурное представление**. В этом режиме инциденты отображаются в виде дерева вложенных событий и других инцидентов. Если вы хотите, чтобы вложенные элементы инцидентов отображались независимо от текущих параметров фильтрации и поиска, установите флажок **Показывать вложенные при фильтрации**.

4. В блоке параметров **Отображаемые графы таблицы** установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Необходимо выбрать хотя бы один параметр.

   Для просмотра доступны следующие параметры:

   - **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 графе **Всего появлений**. Для инцидента – самые поздние дата и время последнего появления событий, входящих в инцидент. Аналогично графе **Начало**, вы можете просматривать в таблице дату совместно со временем, либо только дату или только время.

- **Заголовок**.

  Заголовок, заданный для типа события.

- **Важность**.

  Значок, соответствующий уровню важности события или инцидента.

- **Отправитель**.

  Адрес отправителя сетевых пакетов (в скобках указаны сокращенные названия для отображения в ячейках таблицы):

  - **IP-адрес**.
  - **Номер порта (P)**.
  - **MAC-адрес**.
  - **VLAN ID (VID)**.
  - **Адрес прикладного уровня**.

- **Получатель**.

  Адрес получателя сетевых пакетов (в скобках указаны сокращенные названия для отображения в ячейках таблицы):

  - **IP-адрес**.
  - **Номер порта (P)**.
  - **MAC-адрес**.
  - **VLAN ID (VID)**.
  - **Адрес прикладного уровня**.

- **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 этой графе отображается значение 1.

- ID.

  Уникальный идентификатор зарегистрированного события или инцидента.

- 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 графе **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.

5. Если вы хотите изменить порядок отображения граф, выделите название графы, которую вы хотите разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

   Для граф **Начало**, **Последнее появление** и **Завершение** вы также можете изменить порядок отображения даты и времени, а для граф **Отправитель** и **Получатель** – адресов отправителей и получателей сетевых пакетов. Для этого выделите значение, которое вы хотите разместить левее или правее в таблице, и используйте кнопки с изображением стрелок вверх и вниз.

Выбранные графы отобразятся в указанном вами порядке в таблице в разделе **События**.

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** выберите нужное событие или инцидент.

В правой части окна веб-интерфейса появится область деталей, в которой отобразятся подробные сведения о выбранном событии или инциденте.

Просмотр сведений об устройствах, связанных с событиями

Вы можете просмотреть сведения об устройствах, с которыми связаны события, в таблице устройств. В таблице устройств автоматически применяется фильтрация по идентификаторам известных программе устройств с использованием значений MAC- и IP-адресов, которые указаны в событиях.

Возможность загружать сведения доступна, если выбрано не более 200 событий, не включая инциденты (если выбраны инциденты, то загрузка сведений выполняется для первых выбранных 200 событий, включая события выбранных инцидентов). В таблице устройств показываются сведения не более чем для 200 устройств, с которыми связаны события.

Чтобы просмотреть сведения об устройствах в таблице устройств, выполните следующие действия:

1. Выберите раздел **События**.
2. В таблице событий выберите события и / или инциденты, для которых вы хотите просмотреть сведения об устройствах.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Показать устройства**.

   Кнопка **Показать устройства** недоступна, если среди выбранных событий нет инцидентов и количество выбранных событий превышает 200.

Откроется раздел **Устройства**. В таблице устройств будет применена фильтрация по идентификаторам устройств, которые соответствуют выбранным событиям.

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.

Чтобы присвоить событиям или инцидентам статус В обработке, выполните следующие действия:

1. Выберите раздел **События**.
2. В таблице событий выберите события и / или инциденты, статус которых вы хотите изменить. Выбранные события и / или инциденты должны быть со статусом *Новое*.

   В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку с названием статуса *В обработке*. Кнопка недоступна, если выбранным событиям и инцидентам уже присвоен статус *В обработке* или *Обработано.* При этом 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 кнопка с названием статуса *В обработке* доступна.

   Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **ОК**.

Чтобы присвоить событиям или инцидентам статус Обработано, выполните следующие действия:

1. Выберите раздел **События**.

2. В таблице событий выберите события и / или инциденты, статус которых вы хотите изменить. Выбранные события и / или инциденты должны быть со статусом *Новое* или со статусом *В обработке*.

   В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку с названием статуса *Обработано*. Кнопка недоступна, если выбранным событиям и инцидентам уже присвоен статус *Обработано*. При этом 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 кнопка с названием статуса *Обработано* доступна.

   Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **ОК**.

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, выполните следующие действия:

1. В разделе **События** откройте контекстное меню по левой клавише мыши в ячейке графы **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 граф, отображаемых в таблице в текущий момент.

Возможность копировать события доступна, если выбрано не более 200 событий (в том числе в составе выбранных инцидентов).

Чтобы скопировать события в текстовый редактор, выполните следующие действия:

1. Выберите раздел **События**.
2. В таблице событий выберите события и / или инциденты, информацию о которых вы хотите скопировать в текстовый редактор.

   В правой части окна веб-интерфейса появится область деталей.
3. По правой клавише мыши откройте контекстное меню одного из выбранных событий.
4. В контекстном меню выберите один из следующих пунктов:
   - **Копировать детали события**, если вы копируете одно событие или инцидент.
   - **Копировать детали выбранных событий**, если вы копируете 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.

Экспорт событий в файл

Вы можете экспортировать информацию о событиях и / или инцидентах в файл формата CSV. Информация экспортируется из граф, отображаемых в таблице в текущий момент.

Чтобы экспортировать информацию о событиях и / или инцидентах, выполните следующие действия:

1. Выберите раздел **События**.
2. В таблице событий выберите события и / или инциденты, информацию о которых вы хотите экспортировать в файл.

   Для экспорта информации о всех событиях и инцидентах, удовлетворяющих текущим параметрам фильтрации и поиска, вы можете выбрать все события и инциденты в таблице или использовать кнопку **Экспорт** в панели инструментов раздела **События**. При нажатии на кнопку **Экспорт** сразу запускается процесс формирования файла формата CSV.

   После выбора событий и / или инцидентов в правой части окна веб-интерфейса появится область деталей.
3. В зависимости от количества выбранных элементов, нажмите на кнопку **Экспортировать событие** или **Экспортировать выбранные события**.
4. 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 **Загрузить файл**.

Откроется стандартное окно используемого веб-браузера для сохранения файла.

5. В открывшемся окне укажите имя файла и директорию, в которую нужно сохранить файл.

6. Сохраните файл.

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). 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, выполните следующие действия:

1. Выберите раздел **События**.

2. В таблице событий выберите события и / или инциденты, для которых вы хотите загрузить трафик.

   В правой части окна веб-интерфейса появится область деталей.

3. В зависимости от количества выбранных элементов, нажмите на кнопку **Загрузить трафик для события** или **Загрузить трафик для выбранных событий**.

4. 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 **Загрузить файл**.

   Откроется стандартное окно используемого веб-браузера для сохранения файла.

5. В открывшемся окне укажите имя файла и директорию, в которую нужно сохранить файл.

6. Сохраните файл.

Мониторинг параметров технологического процесса

Kaspersky Industrial CyberSecurity for Networks отображает параметры технологического процесса в онлайн-режиме.

Набор отображаемых параметров технологического процесса определяется тегами для контроля процесса. Отображаются только те теги, для которых есть правила контроля процесса. Вы можете сформировать списки тегов и правил контроля процесса в Консоли программы на закладке **Контроль процесса**. Сведения о настройке контроля процесса см. в разделе Контроль 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.

Вы можете просматривать теги со значениями параметров технологического процесса в разделе **Теги** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Просмотр параметров технологического процесса

Чтобы просмотреть таблицу с тегами и значениями параметров технологического процесса,

подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер и выберите раздел **Теги**.

В окне веб-браузера отобразится таблица с тегами и их текущими значениями. Текущая скорость обработки тегов выводится в строке **Теги** в верхней части окна.

Сортировка тегов при просмотре параметров технологического процесса

Вы можете сортировать теги в разделе **Теги** веб-интерфейса программы. Сортировка выполняется по графам **Имя тега**, **Идентификатор** и **Описание**.

Чтобы отсортировать теги,

в таблице тегов нажмите на заголовок графы, по которой вы хотите выполнить сортировку.

Таблица будет отсортирована по выбранной графе. Рядом с заголовком графы появится значок, показывающий текущий порядок сортировки: по возрастанию или по убыванию значений.

Взаимодействие программы с Kaspersky Security Center

Этот раздел содержит информацию о настройке взаимодействия программы с Kaspersky Security Center и об использовании функций Kaspersky Security Center для получения лицензионного ключа, загрузки обновлений баз и программных модулей, мониторинга событий и контроля состояния безопасности АСУ ТП.

Для взаимодействия Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center должны быть выполнены следующие условия:

- При установке Сервера добавлена функциональность взаимодействия программы с Kaspersky Security Center. Если функциональность не добавлена, добавьте ее.
- В Kaspersky Security Center установлен плагин управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center.
- 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). Подробную информацию о перемещении управляемых устройств в группы администрирования см. в справочной системе для Kaspersky Security Center.

Подключение к Консоли из Kaspersky Security Center

Вы можете удаленно подключаться к Консоли Kaspersky Industrial CyberSecurity for Networks из Консоли администрирования Kaspersky Security Center. 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 Консоли Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center, выполните следующие действия:

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 закладке **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. Если Консоль программы не запущена, запустите ее.

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 Консоли программы.

Для распространения лицензионного ключа вам нужно добавить его в хранилище Сервера администрирования Kaspersky Security Center. Вы можете добавить лицензионный ключ в хранилище Сервера администрирования из файла лицензионного ключа.

Автоматическое распространение лицензионного ключа работает, если компьютер Сервера Kaspersky Industrial CyberSecurity for Networks входит в группу администрирования в папке **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center. Если компьютер Сервера Kaspersky Industrial CyberSecurity for Networks отсутствует в группе администрирования, вам нужно добавить его.

Подробную информацию о лицензировании управляемых программ в Kaspersky Security Center и описания действий для автоматического распространения ключей см. в справочной системе Kaspersky Security Center.

Использование Сервера администрирования Kaspersky Security Center в качестве источника обновлений

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.

Чтобы использовать Сервер администрирования Kaspersky Security Center в качестве источника обновлений баз и программных модулей Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center создайте и настройте задачу Загрузка обновлений в хранилище Сервера администрирования.

   Подробную информацию о создании и использовании задачи Загрузка обновлений в хранилище Сервера администрирования см. в справочной системе Kaspersky Security Center.

2. В Консоли Kaspersky Industrial CyberSecurity for Networks выберите в качестве источника обновлений Сервер администрирования Kaspersky Security Center.

3. Выберите режим запуска обновления или, если обновления уже загружены на Сервер администрирования, запустите обновление вручную.

Мониторинг событий через Kaspersky Security Center

В Kaspersky Security Center сведения о событиях Kaspersky Industrial CyberSecurity for Networks отображаются в следующих графах таблицы событий:

- **Время** – 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** – 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** – уровень важности события в соответствии с типизацией Kaspersky Security Center.
- **Зарегистрировано** – время регистрации события в базе данных Kaspersky Security Center.

Вы можете настроить состав полей, отображаемых в таблице событий. Описания действий для добавления и удаления полей в таблицах см. в справочной системе 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, выполните следующие действия:

1. Убедитесь, что в Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center установлены необходимые компоненты.

2. В плагине управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center настройте получение событий нужных типов для всех уровней важности событий. Подробную информацию о настройке получения событий Kaspersky Security Center см. в справочной системе для Kaspersky Security Center.

3. В Консоли Kaspersky Industrial CyberSecurity for Networks выберите закладку Настройка событий.

4. Добавьте Kaspersky Security Center как адресата событий. Этот адресат добавляется автоматически, если на момент создания политики безопасности в Kaspersky Industrial CyberSecurity for Networks включена возможность передачи событий в Kaspersky Security Center.

5. Укажите в списке типы событий, которые вы хотите отправлять в Kaspersky Security Center. Если адресат для Kaspersky Security Center был добавлен автоматически, для этого адресата по умолчанию включена передача всех системных типов событий, имеющих уровень важности *Критические*.

6. В меню **Управление политикой безопасности** в окне Консоли программы примените политику безопасности.

   Если включен межсетевой экран на компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks, вам нужно проверить заданные параметры межсетевого экрана. Для передачи событий в межсетевом экране должен быть открыт SSL-порт, указанный для подключения к компьютеру с Kaspersky Security Center при установке Сервера Kaspersky Industrial CyberSecurity for Networks.

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	Регистрация в качестве инцидента	Соответствующий код типа события в Kaspersky Industrial CyberSecurity for Networks

	Kaspersky Security Center	
Тестовое событие (DPI)	нет	4000000001
Тестовое событие (NIC)	нет	4000000002
Тестовое событие (IDS)	нет	4000000003
Тестовое событие (AM)	нет	4000000004
Обнаружено неразрешенное сетевое взаимодействие	нет	4000002601
Обнаружена системная команда	только события с уровнем важности *Критические*	4000002602
Отсутствует трафик на точке мониторинга	нет	4000002700
Обнаружена аномалия в протоколе TCP: подмена содержимого в перекрывающихся TCP-сегментах	да	4000002701
Нарушено правило контроля процесса	только события с уровнем важности *Критические*	4000002900
Сработало правило обнаружения вторжений из системного набора правил	нет	4000003000
Сработало правило обнаружения вторжений из пользовательского набора правил	нет	4000003001
Обнаружены признаки ARP-спуфинга в ARP-ответах	да	4000004001
Обнаружены признаки ARP-спуфинга в ARP-запросах	да	4000004002
Обнаружено новое устройство в сети	да	4000005003
Обнаружены новые параметры устройства	нет	4000005004
Обнаружен конфликт IP-адреса	да	4000005005
Обнаружена активность устройства со статусом Неиспользуемое	нет	4000005006
Обнаружен новый IP-адрес устройства	да	4000005007
Обнаружен новый MAC-адрес устройства	да	4000005010
Добавлен IP-адрес устройству	нет	4000005009
Добавлен MAC-адрес устройству	нет	4000005008
Обнаружена аномалия в протоколе IP: конфликт данных при сборке IP-пакета	да	4000005100
Обнаружена аномалия в протоколе IP: превышение размера фрагментированного IP-пакета	да	4000005101

Обнаружена аномалия в протоколе IP: размер начального фрагмента IP-пакета меньше ожидаемого	да	4000005102
Обнаружена аномалия в протоколе IP: несоответствие фрагментов IP-пакета (mis-associated fragments)	да	4000005103
Контроль проектов ПЛК: обнаружено чтение неизвестного блока из ПЛК	нет	4000005200
Контроль проектов ПЛК: обнаружено чтение известного блока из ПЛК	нет	4000005201
Контроль проектов ПЛК: обнаружена запись нового блока в ПЛК	нет	4000005202
Контроль проектов ПЛК: обнаружена запись известного блока в ПЛК	нет	4000005203
Контроль проектов ПЛК: обнаружено чтение неизвестного проекта из ПЛК	нет	4000005204
Контроль проектов ПЛК: обнаружено чтение известного проекта из ПЛК	нет	4000005205
Контроль проектов ПЛК: обнаружена запись нового проекта в ПЛК	нет	4000005206
Контроль проектов ПЛК: обнаружена запись известного проекта в ПЛК	нет	4000005207
Зарегистрировано событие по правилу корреляции	только события с уровнем важности *Критические*	8000000000, 8000000001, 8000000002, 8000000003
Достигнуто максимальное количество переданных событий	да	–
Пользовательское событие по технологии Контроль технологического процесса	только события с уровнем важности *Критические*	–
Пользовательское событие по технологии Внешние системы	да	–

Соответствие уровней важности событий в Kaspersky Security Center

Уровни важности событий в Kaspersky Security Center соответствуют уровням важности событий Kaspersky Industrial CyberSecurity for Networks (см. таблицу ниже).

Соответствие уровней важности событий

Уровни важности событий Kaspersky Security Center	Уровни важности событий Kaspersky Industrial CyberSecurity for Networks
Информационное сообщение	Информационные
Предупреждение	Важные
Критическое событие	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.

Просмотр состояния безопасности АСУ ТП в Kaspersky Security Center

Чтобы просмотреть состояние безопасности АСУ ТП в Kaspersky Security Center, выполните следующие действия:

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.

   Информация о статусе компьютера отобразится в блоке работы с выбранным объектом, который появляется справа в рабочей области выбранной группы.

3. Если блок работы с выбранным объектом не отображается, откройте его с помощью правой границы таблицы со списком управляемых устройств.

Статус компьютера Сервера Kaspersky Industrial CyberSecurity for Networks соответствует состоянию безопасности АСУ ТП. Состояние безопасности АСУ ТП определяется по наличию необработанных инцидентов Kaspersky Security Center. Инциденты Kaspersky Security Center регистрируются при получении определенных типов событий Kaspersky Industrial CyberSecurity for Networks.

Цвет значка компьютера Сервера Kaspersky Industrial CyberSecurity for Networks соответствует одному из следующих состояний безопасности АСУ ТП:

- Красный цвет: статус *Критический*. Есть необработанные инциденты Kaspersky Security Center. Этот статус отображается, если для выбранной группы администрирования включено условие **Есть необработанные инциденты** в списке условий статуса *Критический* (включено по умолчанию).

- Желтый цвет: статус *Предупреждение*. Есть необработанные инциденты Kaspersky Security Center. Этот статус отображается, если для выбранной группы администрирования включено условие **Есть необработанные инциденты** в списке условий статуса *Предупреждение* (и при этом такое условие выключено для статуса *Критический*).

- Зеленый цвет: статус *ОК*. Отсутствуют необработанные инциденты Kaspersky Security Center.

  Зеленый цвет значка со статусом *ОК* может отображаться и при наличии необработанных инцидентов Kaspersky Security Center. Это возможно, если для выбранной группы администрирования выключено условие **Есть необработанные инциденты** в списках условий статусов *Предупреждение* и *Критический*. Для правильного отображения состояния безопасности АСУ ТП требуется включить указанное условие в списке условий хотя бы одного из статусов *Предупреждение* или *Критический*.

Просмотр состояния безопасности АСУ ТП через SCADA-систему

Чтобы настроить получение и отображение состояния безопасности АСУ ТП в SCADA-системе, выполните следующие действия:

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*.

Устранение неисправностей

Этот раздел содержит описание возможных неисправностей в работе Kaspersky Industrial CyberSecurity for Networks и способов их устранения.

Не выполняется установка компонента программы на выбранном узле

Проблема

При установке программы выводится сообщение о недоступности узла для установки компонента из-за невозможности подключения по протоколу SSH. Установка компонента на этом узле не выполняется.

Решение

Установка компонента программы невозможна, если после настройки доступа по протоколу SSH на узле для установки компонента изменилась адресная информация или сетевое имя компьютера. Для установки компонента программы требуется восстановить доступ по протоколу SSH к удаленному компьютеру.

Чтобы восстановить доступ по протоколу SSH и установить компонент программы, выполните следующие действия:

1. На компьютере, с которого выполняется 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

В зависимости от способа подключения к Серверу программа информирует о проблемах в работе следующими способами:

- При подключении через веб-интерфейс – в верхней части меню веб-интерфейса программы отображается значок красного цвета рядом с кнопкой  .
- При подключении через Консоль программы – в строке состояния Консоли отображается значок красного цвета и сообщение об ошибке.

Решение

Такое состояние Kaspersky Industrial CyberSecurity for Networks означает, что работа одного из процессов программы нарушена.

Чтобы восстановить работу программы, выполните следующие действия:

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 разделе Директории для хранения данных программы. Для доступа к журналам нужно иметь root-права в операционной системе.

Новое сообщение программы

Проблема

Появилось новое сообщение программы на закладке **Сообщения программы** в разделе **Параметры** (при подключении к Серверу через веб-интерфейс).

> 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 на закладку **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 на закладке **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.

- *Состояние неизвестно*, *Сбой* – если сообщение появилось только что, подождите 20–30 секунд и проверьте текущее состояние программы. Вы можете просматривать информацию о текущем состоянии программы в окне Консоли.

- *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 разделе 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, выполните следующие действия:

1. Освободите на жестком диске компьютера достаточный объем пространства, соответствующий минимальным требованиям к объему свободного пространства.

2. Перезапустите сервисы, обеспечивающие работу компонентов программы.

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 текущее состояние *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 на закладке 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).

Неизвестно состояние программы

Проблема

В строке состояния Консоли отображается значок серого цвета и текстовое сообщение с описанием проблемы (например, о неизвестном состоянии узла с установленными компонентами программы).

Решение

Такое состояние Kaspersky Industrial CyberSecurity for Networks означает, что программе не удалось установить связь с компонентом или процессом программы.

Подождите 20–30 секунд. Состояние программы изменится. Возможны следующие варианты:

- Если проблема не воспроизведена, значок серого цвета и сообщение перестанут отображаться в строке состояния Консоли.
- Если проблема сохраняется, программа проинформирует о проблемах в работе.

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 **Загрузить трафик для события** 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.

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.

Для типов событий, которые регистрируются в качестве инцидентов (коды типов событий: 8000000000, 8000000001, 8000000002 и 8000000003), невозможно включить сохранение трафика. Чтобы сохранять трафик, связанный с инцидентами, вам нужно включить сохранение трафика для типов событий, которые приводят к регистрации инцидентов.

Для регистрации инцидентов могут использоваться различные типы событий. Используемые типы событий определяются правилами корреляции событий. При этом сами правила корреляции событий могут изменяться при установке обновлений программы.

Вы можете определить примерный состав типов событий, используемых для инцидентов, просмотрев события в ранее зарегистрированных инцидентах. Однако полученный таким образом список типов событий не будет полным. В следующих регистрируемых инцидентах могут использоваться другие типы событий (например, из-за изменений в правилах корреляции после установки обновлений). Если вы хотите, чтобы программа всегда сохраняла трафик для всех событий в инцидентах, вы можете включить сохранение трафика для всех системных типов событий (для которых возможно включить сохранение трафика).

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.

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 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, 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, для возобновления контроля защищаемой АСУ ТП вам нужно снова включить точки мониторинга 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 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 сети и контроля устройств.

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 разделе Директории для хранения данных программы. Для доступа к журналам нужно иметь root-права в операционной системе.

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, выполните следующие действия:

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-браузер

Проблема

При попытке подключения к Серверу через веб-браузер 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 веб-браузера введены неправильные данные. Введите IP-адрес или имя компьютера Сервера, которое было указано при установке Веб-сервера. Номер порта можно не указывать, если задан порт по умолчанию 443. Если задан другой номер порта, введите в адресной строке полный адрес `https://<имя Сервера>:<порт>`

- В веб-браузере выключено выполнение сценариев JavaScript. Сообщение об этом выводится на странице предупреждения о невозможности подключения. В параметрах веб-браузера включите

выполнение JavaScript и обновите страницу.

- Доступ к компьютеру Сервера заблокирован межсетевым экраном. Выполните настройку используемого межсетевого экрана.

При подключении к Серверу веб-браузер выводит предупреждение о сертификате

Проблема

При попытке подключения к Серверу веб-браузер выводит предупреждение о том, что сертификат безопасности или устанавливаемое соединение не является доверенным. Содержание предупреждения зависит от используемого веб-браузера.

Решение

Предупреждение означает, что на Веб-сервере используется самоподписанный сертификат. Для 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 веб-браузера выберите вариант, позволяющий продолжить подключение. После подключения к Серверу в окне веб-браузера будет отображаться предупреждающее сообщение о сертификате. Текст сообщения зависит от используемого веб-браузера.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского".

> Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;

- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

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 разделе 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 установки программы kics4net-deploy-<номер версии программы>.bundle.sh.

Чтобы получить данные о компонентах программы, выполните следующие действия:

1. На компьютере, с которого выполнялась установка, перейдите в директорию с сохраненными файлами из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.
2. Введите команду запуска скрипта установки программы с параметром `gather-artefacts`:

   ```
   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 `SUDO 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.

Источники информации о программе

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Industrial CyberSecurity for Networks:

- страница Kaspersky Industrial CyberSecurity for Networks на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Industrial CyberSecurity for Networks на веб-сайте Службы технической поддержки (База знаний);
- онлайн-справка.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Industrial CyberSecurity for Networks на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Industrial CyberSecurity for Networks вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Industrial CyberSecurity for Networks в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Industrial CyberSecurity for Networks в Базе знаний вы найдете статьи, которые содержат полезную информацию и рекомендации по использованию программы.

Онлайн-справка

Онлайн-справка располагается на веб-ресурсе "Лаборатории Касперского".

В онлайн-справке вы можете найти информацию для выполнения следующих задач:

- подготовка к установке, установка и удаление Kaspersky Industrial CyberSecurity for Networks;
- настройка и использование Kaspersky Industrial CyberSecurity for Networks;
- взаимодействие Kaspersky Industrial CyberSecurity for Networks с Kaspersky Security Center.

В онлайн-справке также содержится информация о типовых задачах, которые пользователь может выполнять с помощью программы, с учетом имеющихся прав в Kaspersky Industrial CyberSecurity for Networks.

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;

- удаленный вызов процедур для получения данных из Kaspersky Industrial CyberSecurity for Networks и отправки данных в программу.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа примерами, а также справочными и дополнительными сведениями.

Пример установки Сервера и сенсора

В этом разделе описан пример последовательности действий для установки Kaspersky Industrial CyberSecurity for Networks в варианте установки Сервера и одного сенсора. Компьютер, на который устанавливается Сервер, обозначен в примере как "компьютер 1". Компьютер, на который устанавливается сенсор, обозначен как "компьютер 2". В качестве компьютера, с которого выполняется установка, используется компьютер 1.

Чтобы установить Сервер и сенсор на компьютере 1 и компьютере 2, выполните следующие действия:

1. На компьютере 1 и компьютере 2 назначьте одинаковый пароль для учетной записи root (от имени этого пользователя будет выполняться установка компонентов программы).

   Для назначения пароля вы можете ввести в командной строке команду `sudo passwd root`.

2. На компьютере 1 создайте учетную запись kics4net_startuser. Эта учетная запись будет использоваться для запуска скрипта установки программы. Также после установки программы этой учетной записи будет разрешено выполнять запуск Консоли программы.

   Учетной записи kics4net_startuser не требуется исполнять команды с root-правами. Для создания учетной записи вы можете ввести в командной строке команду `sudo useradd kics4net_startuser`. После создания учетной записи вы можете назначить для нее пароль с помощью команды `sudo passwd kics4net_startuser`.

3. Выясните и сохраните следующие данные о компьютерах:

   - имя и IP-адрес компьютера 1;
   - IP-адрес компьютера 2;
   - 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`).

4. На компьютере 1 проверьте доступ по протоколу SSH к компьютеру 2.

   Для подключения выполните следующие действия:

   a. Введите в командной строке команду:

      ```
      ssh root@<IP-адрес компьютера 2>
      ```

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

   c. Для завершения сеанса подключения используйте команду:

      ```
      exit
      ```

5. На компьютере 1 войдите в систему под учетной записью kics4net_startuser и создайте директорию /home/kics4net_startuser/kics4net_install/.

6. В созданную директорию скопируйте следующие файлы из комплекта поставки Kaspersky Industrial CyberSecurity for Networks:

   - скрипт установки программы kics4net-deploy-<номер версии программы>.bundle.sh;
   - пакет для установки Сервера и сенсоров: kics4net-<номер версии программы>.x86_64.rpm;
   - пакет для установки Консоли: kics4net-utm-<номер версии программы>.x86_64.rpm;
   - пакет для установки СУБД: kics4net-postgresql-<номер версии СУБД>.x86_64.rpm;
   - пакет для установки системы обнаружения вторжений: kics4net-suricata-<номер версии системы>.x86_64.rpm;
   - пакет для установки Веб-сервера: kics4net-webserver-<номер версии программы>.x86_64.rpm;
   - пакет для установки Агента администрирования из состава комплекта поставки Kaspersky Security Center: klnagent64-<номер версии Агента администрирования>.x86_64.rpm.

7. Перейдите в директорию /home/kics4net_startuser/kics4net_install/.

8. Введите команду запуска скрипта установки программы:

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

   На экране отобразится предложение выбрать язык для меню установки.

9. Выберите язык, который вы хотите использовать в меню установки.

10. После выбора языка для меню установки выполняется проверка контрольных сумм пакетов в директории с сохраненными файлами из комплекта поставки. Дождитесь завершения проверки контрольных сумм пакетов.

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

    На экране отобразится главное меню установки.

12. Выберите пункт меню **Добавить Сервер** и укажите основные параметры Сервера в следующих запросах:

    - **Введите IP-адрес узла для установки** – введите IP-адрес компьютера 1.
    - **Введите IP-адрес для подключений к Серверу** – повторно введите IP-адрес компьютера 1.
    - **Введите имя Сервера** – введите произвольное уникальное имя Сервера в составе решения Kaspersky Industrial CyberSecurity (например, `Server_1`).
    - **Добавить функциональность взаимодействия программы с Kaspersky Security Center** – введите символ `y` и в следующих запросах введите IP-адрес / имя компьютера с Kaspersky Security Center и SSL-порт для подключения.
    - **Включить синхронизацию времени между Сервером и сенсорами** – введите символ `y`.
    - **Введите IP-адрес или имя компьютера с Веб-сервером** – введите IP-адрес / имя компьютера 1.
    - **Введите номер порта Веб-сервера** – введите номер порта 443.
    - **Введите имя пользователя программы** – введите имя пользователя программы `kics4net_admin`.

- **Использовать самоподписанные сертификаты для соединения с Веб-сервером** – введите символ `y` для подтверждения использования самоподписанного сертификата Веб-сервера. Если у вас есть сертификат, изданный доверенным центром сертификации, для использования этого сертификата введите символ `n` в этом запросе и затем символ `y` в запросе **Использовать доверенные сертификаты для соединения с Веб-сервером**. Для использования доверенного сертификата требуется указать путь к файлу доверенного сертификата.

  > Если вы хотите использовать в программе доверенный сертификат, он должен быть выдан на тот IP-адрес или на то имя компьютера, которые будут указывать пользователи программы при подключении через веб-интерфейс. Для загрузки доверенного сертификата вы можете использовать файл формата PFX с сохраненным доверенным сертификатом и закрытым ключом. Файл должен быть создан без заданного пароля для доступа к содержимому.

- **Введите имя пользователя операционной системы для запуска Консоли** – введите имя пользователя `kics4net_startuser`. Этому пользователю будет разрешено запускать Консоль программы.

- **Указать имя еще одного пользователя** – введите символ `n`.

13. Выберите пункт меню **Добавить сенсор** и укажите основные параметры сенсора в следующих запросах:

    - **Введите IP-адрес узла для установки** – введите IP-адрес компьютера 2.

    - **Введите имя сенсора** – введите произвольное уникальное имя сенсора в составе решения Kaspersky Industrial CyberSecurity (например, `Sensor_1`).

14. Выберите пункт меню **Изменить язык интерфейса** и в появившемся меню выберите язык локализации компонентов Kaspersky Industrial CyberSecurity for Networks.

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

16. При появлении на экране сообщения о необходимости ознакомиться с условиями Лицензионного соглашения и Политики конфиденциальности нажмите на клавишу **ENTER**.

    На экране отобразится текст Лицензионного соглашения.

17. Внимательно прочитайте Лицензионное соглашение.

    После того, как вы завершили просмотр текста Лицензионного соглашения, на экране отобразится меню для выбора дальнейших действий.

18. Выберите пункт **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.

19. При появлении сообщения о просмотре Политики конфиденциальности нажмите на клавишу **ENTER**.

    На экране отобразится текст Политики конфиденциальности.

20. Внимательно прочитайте Политику конфиденциальности.

    После того, как вы завершили просмотр текста Политики конфиденциальности, на экране отобразится меню для выбора дальнейших действий.

21. Выберите пункт **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**.

После принятия условий Политики конфиденциальности на экране отобразится приглашение для ввода пароля пользователя, от имени которого выполняется установка.

22. Введите пароль пользователя root. Пароль требуется ввести дважды: сначала в приглашении `SSH password` и затем в приглашении `SUDO password`.

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

23. При появлении запроса для ввода пароля пользователя kics4net_admin введите новый пароль для этого пользователя.

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

После завершения установки Kaspersky Industrial CyberSecurity for Networks не выполняет функции по контролю промышленной сети (на сетевые интерфейсы узлов с установленными компонентами программы не добавлены точки мониторинга). Чтобы использовать программу, вам нужно выполнить действия для подготовки программы к работе.

Системные типы событий в Kaspersky Industrial CyberSecurity for Networks

При регистрации событий в Kaspersky Industrial CyberSecurity for Networks используются типы событий. Список типов событий содержит системные типы событий, автоматически созданные при установке программы. Также вы можете создавать дополнительные типы событий и добавлять их в список в качестве пользовательских типов событий.

Каждый тип события относится к определенной технологии регистрации событий.

Системные типы событий по технологии Контроль технологического процесса

В этом разделе приведено описание системных типов событий, относящихся к технологии Контроль технологического процесса (см. таблицу ниже).

Системные типы событий по технологии Контроль технологического процесса (DPI)

Код типа события	Заголовок события	Уровень важности	Условия для регистрации
4000002900	Нарушение правила контроля процесса: $ruleName	*Критические*	Сработало правило контроля процесса, для которого указан этот тип события. В заголовке и в описании типа события используются следующие переменные: • $ruleName – название правила; • $tags – полученные значения тегов, для которых заданы условия в правиле.

4000000001	Тестовое событие (DPI)	*Информационные*	Обнаружен тестовый сетевой пакет.

Системные типы событий по технологии Контроль системных команд

В этом разделе приведено описание системного типа события, относящегося к технологии Контроль системных команд (см. таблицу ниже).

Системный тип события по технологии Контроль системных команд (CC)

Код типа события	Заголовок события	Уровень важности	Условия для регистрации
4000002602	$systemCommandShort	Определяется по уровню важности системной команды	Обнаружена системная команда, выбранная для отслеживания (при этом для системной команды не создано активное правило контроля сети). В заголовке и в описании типа события используются следующие переменные: • $systemCommandShort – краткое описание обнаруженной системной команды; • $systemCommandFull – подробное описание обнаруженной системной команды.

Системные типы событий по технологии Контроль целостности сети

В этом разделе приведено описание системных типов событий, относящихся к технологии Контроль целостности сети (см. таблицу ниже).

Системные типы событий по технологии Контроль целостности сети (NIC)

Код типа события	Заголовок события	Уровень важности	Условия для регистрации
4000002601	Обнаружено неразрешенное сетевое взаимодействие ($top_level_protocol)	*Важные*	Обнаружено сетевое взаимодействие, не указанное в активном правиле контроля сети. 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	*Важные*	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)	*Информационные*	Обнаружен тестовый сетевой пакет (при включенной технологии Контроль целостности сети).

Системные типы событий по технологии Обнаружение вторжений

В этом разделе приведено описание системных типов событий, относящихся к технологии Обнаружение вторжений (см. таблицу ниже).

Системные типы событий по технологии Обнаружение вторжений (IDS)

Код типа события	Заголовок события	Уровень важности	Условия для регистрации
4000003000	Сработало правило из набора $fileName (системный набор правил)	Определяется по приоритету правила	Сработало правило обнаружения вторжений, входящее в системный набор правил (набор правил находится в активном состоянии). В заголовке и в описании типа события используются следующие переменные: • $fileName – название набора правил; • $category – класс правила; • $ruleName – название правила; • $severity – приоритет правила.

4000003001	Сработало правило из набора $fileName (пользовательский набор правил)	Определяется по приоритету правила	Сработало правило обнаружения вторжений, входящее в пользовательский набор правил (набор правил находится в активном состоянии). В заголовке и в описании типа события используются следующие переменные: • $fileName – название набора правил; • $category – класс правила; • $ruleName – название правила; • $severity – приоритет правила.
4000004001	Обнаружены признаки ARP-спуфинга в ARP-ответах	*Критические*	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	*Критические*	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	*Критические*	Обнаружена аномалия в протоколе IP: при наложении фрагментов IP-пакета данные не совпадают.
4000005101	Обнаружена аномалия в протоколе IP: превышение размера фрагментированного IP-пакета	*Критические*	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	*Критические*	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)	*Важные*	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	*Критические*	Обнаружена аномалия в протоколе TCP: пакеты содержат перекрывающиеся TCP-сегменты с различающимся содержимым.
4000000003	Тестовое событие (IDS)	*Информационные*	Обнаружен тестовый сетевой пакет (при включенном методе обнаружения вторжений по правилам).

Системные типы событий по технологии Контроль устройств

В этом разделе приведено описание системных типов событий, относящихся к технологии Контроль устройств (см. таблицу ниже).

Системные типы событий по технологии Контроль устройств (AM)

Код типа события	Заголовок события	Уровень важности	Условия для регистрации
4000005003	Обнаружено новое устройство с адресом $owner_ip_or_mac	*Критические*	В режиме наблюдения контроля устройств автоматически добавлено новое устройство по обнаруженному IP- или MAC-адресу, который не указан для других устройств в таблице. 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	*Информационные*	В режиме наблюдения контроля устройств 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	*Критические*	В режиме наблюдения контроля устройств 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	*Критические*	В режиме наблюдения контроля устройств обнаружена активность устройства, которому был присвоен статус *Неиспользуемое*. 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.
4000005007	Обнаружен новый IP-адрес $new_ip_addr у устройства с MAC-адресом $owner_mac	*Критические*	В режиме наблюдения контроля устройств 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	*Информационные*	В режиме наблюдения контроля устройств автоматически добавлен MAC-адрес для сетевого интерфейса,

	устройству с IP-адресом $owner_ip		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	*Информационные*	В режиме наблюдения контроля устройств 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	*Критические*	В режиме наблюдения контроля устройств 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.
4000005200	Контроль проектов ПЛК: обнаружено чтение неизвестного блока из ПЛК $asset_name	*Критические*	При контроле чтения и записи проектов ПЛК обнаружена операция чтения неизвестного блока проекта из ПЛК (если отсутствует сохраненная информация об этом блоке). 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	*Критические*	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). 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.
4000005202	Контроль проектов ПЛК: обнаружена запись нового блока в ПЛК $asset_name	*Критические*	При контроле чтения и записи проектов ПЛК обнаружена операция записи неизвестного блока проекта из ПЛК (если отсутствует сохраненная информация об этом блоке). 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	*Критические*	При контроле чтения и записи проектов ПЛК обнаружена операция

	запись известного блока в ПЛК $asset_name		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). 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	*Критические*	При контроле чтения и записи проектов ПЛК обнаружена операция чтения неизвестного проекта из ПЛК (если отсутствует сохраненная информация об этом проекте). 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	*Критические*	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). 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	*Критические*	При контроле чтения и записи проектов ПЛК обнаружена операция записи нового проекта в ПЛК (если отсутствует сохраненная информация об этом проекте). 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	*Критические*	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). В заголовке и в описании типа события используются следующие переменные: • $asset_name – имя устройства; • $saved_date_time – дата и время сохранения проекта в программе.
4000000004	Тестовое событие (AM)	*Информационные*	Обнаружен тестовый сетевой пакет (при включенном методе обнаружения активности устройств).

Системные типы событий по технологии Внешние системы

В этом разделе приведено описание системных типов событий, относящихся к технологии Внешние системы (см. таблицу ниже).

Системные типы событий по технологии Внешние системы (EXT)

Код типа события	Заголовок события	Уровень важности	Условия для регистрации
8000000000	Инцидент	Определяется по уровню важности правила корреляции	Обнаружена последовательность событий, удовлетворяющих условиям правила корреляции (если в правиле не заданы заголовок и описание инцидента).
8000000001	$customTitle	Определяется по уровню важности правила корреляции	Обнаружена последовательность событий, удовлетворяющих условиям правила корреляции (если в правиле задан заголовок, но не задано описание инцидента). В заголовке типа события используется переменная $customTitle, которая при регистрации события заменяется на заголовок инцидента.
8000000002	Инцидент	Определяется по уровню важности правила корреляции	Обнаружена последовательность событий, удовлетворяющих условиям правила корреляции (если в правиле задано описание, но не задан заголовок инцидента).

			В описании типа события используется переменная $customDescription, которая при регистрации события заменяется на описание инцидента.
8000000003	$customTitle	Определяется по уровню важности правила корреляции	Обнаружена последовательность событий, удовлетворяющих условиям правила корреляции (если в правиле заданы заголовок и описание инцидента). В заголовке и в описании типа события используются следующие переменные: • $customTitle – заголовок инцидента; • $customDescription – описание инцидента.

Файлы для импорта пользовательских тегов и конфигураций устройств

Вы можете импортировать описания пользовательских тегов и конфигураций устройств в Kaspersky Industrial CyberSecurity for Networks. Импорт 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). В этом разделе приведено описание типовых структур файлов данных.

Для импорта тегов и устройств в Kaspersky Industrial CyberSecurity for Networks требуется следующий набор файлов данных:

- devices.csv. Содержит описания устройств и соединений.

  Соединение – это именованная связь между устройством, набором протоколов устройства и набором тегов устройства, передаваемых через эти протоколы.

- connections.csv. Содержит описания протоколов для соединений.
- 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.
- iec61850_sv_messages.csv. Содержит описания сообщений для протокола IEC 61850: Sampled Values.

При использовании файлов данных учитывайте следующие особенности:

- Файлы данных должны быть в кодировке UTF-8.
- Все файлы данных должны находиться в одной директории.
- 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.

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 находиться в директории импорта.

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.

Файл описания устройств: devices.csv

Файл описания устройств содержит перечисление устройств, их типов и идентификаторов соединений. Идентификатор соединения, указанный в файле описания устройств, используется в файле описания соединений и протоколов для связи с тегами и протоколами.

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 AFV series;
- 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.

- `Connection` – идентификатор соединения из файла описания соединений и протоколов 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 и протоколов: connections.csv

Файл описания протоколов содержит описание протоколов для каждого соединения.

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.
- `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 – EMERSON CONTROLWAVE DATA EXCHANGE;
- 27 – HONEYWELL CONTROLEDGE 900 INTERACTION.

- `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 использовать 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=S`
  `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"`

- 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"`
- EMERSON CONTROLWAVE DATA EXCHANGE:
  `"IP-Address=192.168.0.7;Port=1234"`
- HONEYWELL CONTROLEDGE 900 INTERACTION:
  `"IP-Address=192.168.1.99;Port=41103"`

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;EngUnit
```

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.
- `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;EngUnit
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
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.

- EMERSON CONTROLWAVE DATA EXCHANGE: 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.

Пример строки адреса тега для протоколов MMS и GOOSE приведен ниже.

Пример:
```
DOMAIN=IED009PROT1;LN=LLN0;CO=DC;DA=NamPlt.configRev;CDC=LPL;LNCDC=LLN0
```

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";"Unbuffer
```

Файл описания сообщений протокола Sampled Values: iec61850_sv_messages.csv

Файл описания сообщений протокола Sampled Values содержит параметры для сообщений протокола IEC 61850: Sampled Values.

В начале файла должны быть указаны заголовочные строки, которые содержат данные для обработки файла. Пример заголовочных строк файла iec61850_sv_messages.csv приведен ниже.

Пример:

```
'SVMessages
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;SVControlBlockName;SampledValuesId;ConfRev;DataSetName;IsMulticast;OptionalF
```

Первые три заголовочные строки аналогичны заголовочным строкам в файле devices.csv.

Строка `Connection;SVControlBlockName;SampledValuesId;ConfRev;DataSetName;IsMulticast;OptionalFiel` содержит наименования столбцов с данными:

- `Connection` – идентификатор соединения, к которому относится строка настроек в файле iec61850_sv_messages.csv.

- `SVControlBlockName` – имя блока управления для этого сообщения.
- `SampledValuesId` – идентификатор сообщения.
- `ConfRev` – ревизия конфигурации.
- `DataSetName` – имя набора данных, связанного с этим сообщением.
- `IsMulticast` – тип рассылки. Принимает значения `Multicast` или `Unicast`.
- `OptionalFields` – список дополнительных (необязательных) полей, включенных в тело сообщения при рассылке.

После заголовочных строк следует тело файла, содержащее значения параметров (идентификатор соединения, имя блока управления, идентификатор сообщения, ревизия конфигурации, имя набора данных для сообщения, тип рассылки, дополнительные поля). Пример файла iec61850_sv_messages.csv приведен ниже.

Пример:

```
'SVMessages
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;SVControlBlockName;SampledValuesId;ConfRev;DataSetName;IsMulticast;OptionalF
"IED_TRANSFORMER1";"IED_TRANSFORMER1/LLN0$MS$SMV_Control_Block1";"SMV_ID_1";"0";"IED_TRA
```

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).

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.

АСУ ТП

Аббревиатура от "автоматизированная система управления технологическим процессом". Группа технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Веб-сервер Kaspersky Industrial CyberSecurity for Networks

Компонент Kaspersky Industrial CyberSecurity for Networks. Предоставляет интерфейс для подключения к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-браузер.

Внешние системы

Технология регистрации инцидентов, а также событий, которые поступают в Kaspersky Industrial CyberSecurity for Networks от внешних 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.

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 сети

Модель для визуального отображения обнаруженных взаимодействий между устройствами промышленной сети. Карта сети содержит следующие объекты: узлы, представляющие устройства, группы устройств и соединения между узлами / группами устройств.

Консоль Kaspersky Industrial CyberSecurity for Networks

Компонент Kaspersky Industrial CyberSecurity for Networks. Реализует графический интерфейс для подключения к Серверу и позволяет настраивать функциональность, которая недоступна для управления при подключении через веб-браузер.

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 устройств

Технология регистрации событий, связанных с обнаружением в трафике активности устройств (например, событие при обнаружении активности ранее неизвестного устройства).

Контроль целостности сети

Технология регистрации событий, связанных с целостностью промышленной сети или с безопасностью взаимодействий (например, обнаружено взаимодействие устройств по неразрешенному протоколу).

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 контроля процесса и параметры регистрации для типов событий.

Правило контроля процесса

Набор условий для значений тегов. При выполнении условий правила контроля процесса Kaspersky Industrial CyberSecurity for Networks регистрирует событие.

Правило контроля сети

Описание разрешенного взаимодействия для устройств промышленной сети. При обнаружении сетевого взаимодействия, которое удовлетворяет активному правилу контроля сети, Kaspersky Industrial CyberSecurity for Networks не 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.

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 копию трафика промышленной сети от точек мониторинга, обрабатывает полученные данные и передает их на Сервер.

Сервер Kaspersky Industrial CyberSecurity for Networks

Компонент Kaspersky Industrial CyberSecurity for Networks. Сервер обрабатывает информацию о трафике промышленной сети, сохраняет и предоставляет данные (например, события и сведения об устройствах). Сервер может принимать информацию о трафике промышленной сети от точек мониторинга на сенсорах или от собственных точек мониторинга.

Системная команда

Блок данных в трафике промышленной сети, содержащий команду управления устройством (например, START PLC) или системное сообщение, связанное с функционированием устройства (например, REQUEST NOT FOUND).

Событие

Запись, содержащая информацию об обнаружении в трафике промышленной сети данных, которые требуют 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, который обозначает взаимодействие узлов в виде линии связи между узлами.

Тег

Переменная, которая содержит значение какого-либо параметра технологического процесса (например, температуры).

Тип события

Заданный набор параметров для регистрации событий в Kaspersky Industrial CyberSecurity for Networks. Каждому типу события присваивается уникальный номер (код типа события). В Kaspersky Industrial CyberSecurity for Networks используются системные и пользовательские типы событий. Системные типы событий создаются программой при установке и не могут быть удалены. Пользовательские типы событий можно создавать, изменять и удалять вручную.

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).

Уведомление

Сообщение с информацией о событии (событиях), которое программа отправляет через системы доставки сообщений (например, по электронной почте) на указанные адреса.

Узел

Компьютер, на котором установлен Сервер или сенсор Kaspersky Industrial CyberSecurity for Networks, либо объект на карте сети, представляющий одно или несколько устройств.

Устройство

Устройство промышленной сети, используемое для автоматизации технологического процесса на предприятии (например, программируемый логический контроллер, удаленный терминал, интеллектуальное электронное устройство).

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/

Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Flash – товарный знак или зарегистрированный в Соединенных Штатах Америки и/или в других странах товарный знак Adobe Systems Incorporated.

Antaira – зарегистрированный товарный знак Antaira Technologies, LLC.

Apple, iPad, iPhone, Mac, macOS, Mac OS и OS X – товарные знаки Apple Inc., зарегистрированные в США и других странах.

AXIS и AXIS COMMUNICATIONS – зарегистрированные товарные знаки или заявки на регистрацию товарных знаков Axis AB в различных юрисдикциях.

BitTorrent – товарный знак BitTorrent, Inc.

Cisco и IOS – зарегистрированные в Соединенных Штатах Америки и в других странах товарные знаки Cisco Systems, Inc. и / или ее аффилированных компаний.

Dell – товарный знак Dell, Inc. или дочерних компаний.

Radmin – зарегистрированный товарный знак Famatech.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

General Electric и MULTILIN – зарегистрированные товарные знаки компании General Electric.

Android, Google и Google Chrome – товарные знаки Google, Inc.

Intel и Core – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

IBM и DB2 – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, SQL Server, Windows, Windows Server и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

MOXA – зарегистрированный товарный знак Moxa Inc.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

IPX – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

JavaScript и Oracle – зарегистрированные товарные знаки компании Oracle и/или ее аффилированных компаний.

Pilz – зарегистрированный товарный знак Pilz GmbH & Co. KG.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Realtek – товарный знак Realtek Semiconductor Corporation.

CentOS – товарный знак компании Red Hat, Inc.

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.

Dameware – товарный знак SolarWinds Worldwide, LLC, зарегистрированный в США и других странах.

Texas Instruments – товарный знак Texas Instruments.

Tor – товарный знак The Tor Project, регистрация в США № 3 465 432.

SecureCRT – товарный знак VanDyke Software, Inc.

VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.