

kaspersky

Kaspersky Industrial CyberSecurity for Networks

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 3.0.1.24

Уважаемый пользователь!

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

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 27.05.2021

Обозначение документа: 643.46856491.00094-03 90 01

© 2021 АО "Лаборатория Касперского"

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

О "Лаборатории Касперского" <https://www.kaspersky.ru/about/company>

Содержание

О Kaspersky Industrial CyberSecurity for Networks.....	12
Об этом документе	13
Аппаратные и программные требования.....	13
Обзор функциональности Kaspersky Industrial CyberSecurity for Networks.....	17
Указания по эксплуатации и требования к среде	19
Архитектура программы	21
Типовые схемы развертывания.....	23
Установка Сервера без внешних сенсоров	23
Установка Сервера и внешних сенсоров.....	24
Подключение Kaspersky Industrial CyberSecurity for Networks к промышленной сети через диод данных	26
Установка и удаление программы.....	28
Подготовка к установке программы	28
Используемые порты для установки и работы компонентов.....	34
Использование скрипта централизованной установки компонентов программы.....	37
Централизованная установка компонентов программы	37
Команды меню централизованной установки	39
Изменение параметров и централизованная переустановка компонентов программы.....	43
Централизованная установка компонентов программы в неинтерактивном режиме	44
Усиление защиты компьютеров с установленными компонентами программы.....	46
Централизованное удаление компонентов программы	47
Использование скрипта локальной установки компонентов программы.....	48
Использование скрипта локального удаления компонентов программы	49
Установка плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center	50
Подготовка программы к работе	51
Начальная настройка программы после установки Сервера	52
Запуск и остановка программы.....	54
Подключение к Серверу через веб-интерфейс.....	54
Завершение сеанса подключения к Серверу через веб-интерфейс	55
Подключение к сенсору через веб-интерфейс	56
Процедура приемки	57
Безопасное состояние	57
Проверка регистрации событий с помощью тестового сетевого пакета	58
Контроль целостности модулей программы	60
Интерфейс программы	62
Веб-интерфейс Сервера Kaspersky Industrial CyberSecurity for Networks	62
О веб-интерфейсе Сервера в режиме начальной настройки программы.....	62

О веб-интерфейсе Сервера в основном режиме работы программы	64
Веб-интерфейс сенсора Kaspersky Industrial CyberSecurity for Networks	72
Лицензирование программы	73
О Лицензионном соглашении	73
О Политике конфиденциальности	74
О лицензии	74
О лицензионном сертификате	75
О лицензионном ключе для активации функциональности обновления	75
О файле лицензионного ключа для активации функциональности обновления	75
Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс	76
Просмотр информации о добавленном лицензионном ключе	76
Удаление лицензионного ключа	77
Предоставление данных	78
Директории для хранения данных программы	80
О журналах	82
Администрирование Kaspersky Industrial CyberSecurity for Networks	84
Управление узлами с установленными компонентами программы	84
Добавление и подключение сенсора с использованием веб-интерфейса сенсора	85
Изменение имени узла с установленным компонентом программы	88
Изменение параметров хранения данных программы на узле	88
Создание нового файла свертки для сенсора	89
Удаление сенсора	89
Управление точками мониторинга на узлах	90
Добавление точки мониторинга	91
Включение точек мониторинга	91
Выключение точек мониторинга	92
Переименование точки мониторинга	93
Удаление точки мониторинга	93
Определение Ethernet-порта, связанного с сетевым интерфейсом	94
Контроль состояния Kaspersky Industrial CyberSecurity for Networks	95
Контроль состояния программы при подключении через веб-интерфейс	95
Просмотр сообщений программы	96
Просмотр записей аудита действий пользователей	100
Просмотр сведений об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах	104
Просмотр статуса сервисов, обеспечивающих работу компонентов программы	107
Перезагрузка компьютера с установленными компонентами программы	108
Синхронизация времени на узлах Kaspersky Industrial CyberSecurity for Networks с источником времени для устройств промышленной сети	109
Обновление сертификатов SSL-соединений	109
Обновление баз и программных модулей	110

Запуск обновления вручную	111
Настройка автоматического обновления.....	111
Просмотр сведений об установке обновлений	112
Разделение доступа к функциям программы.....	113
Об учетных записях пользователей программы.....	114
Функции программы, доступные при подключении к Серверу через веб-интерфейс.....	114
Просмотр сведений об учетных записях пользователей программы.....	118
Создание учетной записи пользователя программы	118
Изменение роли учетной записи пользователя программы.....	119
Удаление учетной записи пользователя программы	119
Изменение пароля учетной записи	120
Настройка контроля активов.....	120
Методы и режимы контроля активов	121
Выбор применяемых методов и изменение режима контроля активов	123
Добавление устройств вручную	124
Объединение устройств.....	127
Удаление устройств.....	129
Изменение статусов устройств вручную	130
Формирование списка подсетей для контроля активов	133
Просмотр сведений об устройствах с IP-адресами из выбранных подсетей	134
О распределении устройств по группам.....	134
Автоматическая группировка устройств по заданному критерию.....	135
Распределение устройств по группам вручную.....	137
Перемещение узлов и групп в другие группы на карте сети	141
Формирование дерева групп устройств вручную	141
Установка и удаление меток для устройств.....	144
Изменение сведений об устройстве	150
Добавление, изменение и удаление пользовательских полей для устройства	151
Настройка контроля процесса	152
Поддерживаемые устройства и протоколы.....	153
Устройства для контроля процесса	155
Параметры контроля процесса для устройств	156
Об автоматическом определении параметров контроля процесса для устройств.....	157
Включение и выключение автоматического определения параметров контроля процесса для устройств	158
Добавление параметров контроля процесса для устройства вручную.....	158
Изменение параметров контроля процесса для устройства.....	159
Выбор отслеживаемых системных команд	160
Очистка параметров контроля процесса, заданных для устройства	161
Импорт конфигураций устройств и тегов из внешних проектов.....	162
Теги	163

Об обнаружении неизвестных тегов	164
Включение и выключение обнаружения неизвестных тегов	165
Выбор тегов в таблице	165
Добавление тега вручную	166
Изменение параметров тега	167
Добавление тегов в список избранных	168
Удаление тегов	169
Просмотр правил контроля процесса, связанных с тегами	169
Правила контроля процесса	170
Правила с заданными условиями для значений тегов	171
Правила с Lua-скриптами	173
Режим обучения правилам контроля процесса	174
Включение и выключение контроля процесса по правилам	175
Просмотр таблицы правил контроля процесса	176
Выбор правил контроля процесса	180
Создание правила контроля процесса с параметрами условий	181
Создание правила контроля процесса с Lua-скриптом	182
Изменение параметров правила контроля процесса	183
Создание, просмотр и изменение глобального Lua-скрипта	183
Удаление правил контроля процесса	183
Просмотр сведений об устройствах, связанных с правилами контроля процесса	184
Просмотр тегов, связанных с правилами контроля процесса	184
Настройка контроля взаимодействий	185
Режим обучения для технологий контроля взаимодействий	187
Режим наблюдения для технологий контроля взаимодействий	188
Выбор применяемых технологий контроля взаимодействий	189
Автоматическое формирование правил контроля взаимодействий в режиме обучения	189
Просмотр правил контроля взаимодействий в таблице разрешающих правил	190
Выбор правил контроля взаимодействий в таблице разрешающих правил	196
Создание правил контроля взаимодействий вручную	197
Изменение параметров правила контроля взаимодействий	201
Включение и выключение правил контроля взаимодействий	201
Удаление правил контроля взаимодействий	202
Настройка обнаружения вторжений	202
Правила обнаружения вторжений	203
Дополнительные методы обнаружения вторжений	204
Включение и выключение обнаружения вторжений по правилам	205
Включение и выключение дополнительных методов обнаружения вторжений	206
Просмотр таблицы с наборами правил обнаружения вторжений	207
Выбор наборов правил обнаружения вторжений	208

Включение и выключение наборов правил обнаружения вторжений.....	209
Загрузка и замена пользовательских наборов правил обнаружения вторжений.....	209
Удаление пользовательских наборов правил обнаружения вторжений.....	210
Управление журналами.....	211
Управление параметрами хранения журналов в базе данных Сервера.....	211
Управление параметрами сохранения трафика в базе данных Сервера.....	212
Включение и выключение аудита действий пользователей.....	213
Изменение уровней ведения журналов работы процессов.....	213
Управление технологиями.....	214
Управление коннекторами.....	216
Об отправке событий, сообщений программы и записей аудита в сторонние системы.....	217
Добавление коннектора.....	218
Просмотр таблицы коннекторов.....	220
Включение и выключение коннекторов.....	223
Изменение параметров коннектора.....	223
Создание нового файла свертки для коннектора.....	224
Удаление коннекторов.....	225
Настройка типов событий.....	225
Просмотр таблицы типов событий.....	227
Выбор типов событий в таблице.....	229
Изменение параметров системного типа события.....	230
Настройка автоматического сохранения трафика для системных типов событий.....	230
Настройка передачи событий через коннекторы.....	231
Общие переменные для подстановки значений в Kaspersky Industrial CyberSecurity for Networks.....	232
Управление политикой безопасности.....	236
Экспорт политики безопасности в файл.....	237
Импорт политики безопасности из файла.....	238
Очистка текущей политики безопасности.....	239
Использование Kaspersky Industrial CyberSecurity for Networks API.....	240
Обеспечение безопасного взаимодействия при использовании Kaspersky Industrial CyberSecurity for Networks API.....	241
Создание и использование коннекторов для Kaspersky Industrial CyberSecurity for Networks API.....	242
Подписка на уведомления о значениях тега по протоколу WebSocket.....	243
Решение типовых задач.....	253
Мониторинг системы в онлайн-режиме.....	253
Добавление виджета.....	255
Настройка отображения виджетов.....	255
Информация в виджете Устройства.....	257
Информация в виджете События.....	259
Удаление виджета.....	261
Контроль активов.....	262

Таблица устройств.....	262
Просмотр таблицы устройств.....	265
Просмотр подсетей для контроля активов.....	270
Выбор устройств в таблице устройств.....	273
Выбор подсетей в таблице подсетей.....	274
Просмотр сведений об устройстве.....	275
Автоматическое добавление и обновление устройств.....	275
Автоматическое изменение статусов устройств.....	276
Дерево групп устройств.....	277
Контроль чтения и записи проектов ПЛК.....	277
Просмотр событий, связанных с устройствами.....	279
Экспорт устройств в файл.....	279
Экспорт подсетей в файл.....	281
Работа с картой сети.....	282
Узлы на карте сети.....	283
Группы устройств на карте сети.....	285
Соединения на карте сети.....	286
Просмотр подробных сведений об объектах.....	286
Изменение масштаба карты сети.....	288
Позиционирование карты сети.....	289
Закрепление и открепление узлов и групп.....	289
Изменение местоположения узлов и групп вручную.....	290
Автоматическое распределение узлов и групп.....	290
Фильтрация объектов на карте сети.....	291
Сохранение и загрузка параметров отображения карты сети.....	297
Поиск узлов на карте сети.....	300
Просмотр событий, связанных с узлами известных программе устройств.....	301
Просмотр событий, связанных с соединением.....	302
Просмотр сведений в таблице устройств по выбранным узлам.....	303
Просмотр сведений в таблице устройств по выбранному соединению.....	304
Мониторинг событий и инцидентов.....	305
Уровни важности событий.....	307
Технологии регистрации событий.....	307
Статусы событий.....	308
Таблица зарегистрированных событий.....	308
Выбор событий в таблице событий.....	309
Просмотр событий, включенных в инцидент.....	311
Фильтрация событий.....	311
Поиск событий.....	315
Сброс заданных параметров фильтрации и поиска в таблице событий.....	316

Сортировка событий.....	316
Настройка таблицы зарегистрированных событий	317
Просмотр подробных данных о событии.....	319
Просмотр сведений об устройствах, связанных с событиями	319
Переход на карту сети для отображения информации по событиям	320
Изменение статусов событий	321
Создание разрешающих правил для событий.....	321
Установка меток.....	324
Копирование событий в текстовый редактор.....	325
Экспорт событий в файл.....	325
Загрузка трафика для событий.....	328
Создание директории для экспорта событий на сетевой ресурс.....	329
Контроль уязвимостей устройств	331
Сценарий реализации для процесса непрерывного управления уязвимостями.....	332
Сведения об устройствах, используемые для проверки уязвимостей.....	334
Просмотр устройств с обнаруженными уязвимостями	334
Просмотр таблицы уязвимостей	335
Выбор уязвимостей в таблице уязвимостей	340
Просмотр сведений об уязвимости	341
Автоматическое изменение состояний уязвимостей	341
Изменение состояний уязвимостей вручную	342
Просмотр сведений об устройствах с обнаруженной уязвимостью	342
Просмотр событий, связанных с уязвимостью	343
Экспорт уязвимостей в файл.....	343
Контроль технологического процесса.....	344
Мониторинг значений параметров технологического процесса.....	344
Параметры тегов	345
Просмотр таблицы тегов.....	346
Просмотр сведений об устройствах, связанных с тегами	350
Обнаружение паролей по умолчанию при подключении к устройствам	350
Обнаружение проблем безопасности в протоколах шифрования	352
Взаимодействие программы с Kaspersky Security Center	354
Подключение к компьютеру Сервера из Kaspersky Security Center	354
Добавление лицензионного ключа в Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center	355
Использование Сервера администрирования Kaspersky Security Center в качестве источника обновлений.....	356
Мониторинг событий через Kaspersky Security Center	356
Типы событий в Kaspersky Security Center для событий Kaspersky Industrial CyberSecurity for Networks.....	358
Соответствие уровней важности событий в Kaspersky Security Center	360

Контроль состояния безопасности АСУ ТП: Kaspersky Security Center и SCADA	360
Устранение неисправностей	362
Не выполняется установка компонента программы на выбранном узле	362
Обнаружены проблемы в работе программы	363
Новое сообщение программы	363
Закончилось свободное пространство на жестком диске	364
При включении точки мониторинга возникает ошибка	364
Отсутствует трафик на точке мониторинга	365
Не загружается трафик для событий или инцидентов	366
Профилактические и пусконаладочные работы на АСУ ТП	366
Непредвиденная перезагрузка системы	367
После переустановки Сервера администрирования Kaspersky Security Center не выполняется синхронизация Агента администрирования	368
Не выполняется подключение к Серверу через веб-интерфейс	369
При подключении к Серверу браузер выводит предупреждение о сертификате	369
Обращение в Службу технической поддержки	370
Способы получения технической поддержки	370
Техническая поддержка по телефону	370
Техническая поддержка через Kaspersky CompanyAccount	371
Получение информации для технической поддержки	371
Информация о стороннем коде	373
Уведомления о товарных знаках	374
Соответствие терминов	375
Глоссарий	376
Приложения	381
Настройка синхронизации времени по протоколу NTP	381
Поддерживаемые типы кадров ASDU в протоколах стандартов IEC 60870-5-104 и IEC 60870-5-101	382
Отправка событий Kaspersky Industrial CyberSecurity for Networks в SIEM-системы	387
Изменение времени действия для сеансов подключения и токенов аутентификации с помощью скрипта	395
Файлы для импорта проекта универсального формата	396
Файл описания устройств: devices.csv	397
Файл описания соединений и протоколов: connections.csv	400
Файл описания переменных и тегов: variables.csv	405
Файл описания перечислений: enums.csv	410
Файл описания наборов данных (группы тегов): datasets.csv	411
Файл описания отчетов протокола MMS: iec61850_mms_reports.csv	412
Системные типы событий в Kaspersky Industrial CyberSecurity for Networks	414
Системные типы событий по технологии Контроль технологического процесса	414
Системные типы событий по технологии Контроль системных команд	415
Системные типы событий по технологии Контроль целостности сети	415

Системные типы событий по технологии Обнаружение вторжений	416
Системные типы событий по технологии Контроль активов	419
Системные типы событий по технологии Внешние системы	425

О Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks представляет собой систему обнаружения вторжений на объекты критической информационной инфраструктуры. Программа предназначена для обеспечения автоматизированного анализа сетевой безопасности промышленных объектов путем выявления аномалий в технологическом процессе и сетевых взаимодействиях между узлами технологической сети, а также выявления сетевых атак на промышленные объекты.

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы решающих правил системы обнаружения вторжений;
- анализ данных программы;
- аудит безопасности программы;
- получение данных о событиях и активности в контролируемой информационной системе;
- реагирование программы;
- контроль параметров технологического процесса;
- контроль целостности.

В этом разделе

Об этом документе	13
Аппаратные и программные требования.....	13
Обзор функциональности Kaspersky Industrial CyberSecurity for Networks.....	17
Указания по эксплуатации и требования к среде	19

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Industrial CyberSecurity for Networks 3.0.1" (далее также "Kaspersky Industrial CyberSecurity for Networks", "программа").

Подготовительные процедуры изложены в разделах "Установка и удаление программы", "Запуск и остановка программы" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Аппаратные и программные требования" приведены минимально необходимые системные требования для безопасной установки программы.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Industrial CyberSecurity for Networks, поддержка организаций, использующих Kaspersky Industrial CyberSecurity for Networks, а также специалистам, которые имеют опыт работы с системой удаленного централизованного управления программами "Лаборатории Касперского" Kaspersky Security Center.

Аппаратные и программные требования

Kaspersky Industrial CyberSecurity for Networks имеет следующие минимальные требования к аппаратному обеспечению компьютеров для установки компонентов программы (см. раздел «Архитектура программы» на стр. [21](#)):

- 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 каждым сенсором должна быть не менее 50% от суммарного входящего трафика на сенсор (по всем точкам мониторинга сенсора).

Пример:

На сенсоре используются две точки мониторинга, на одну из которых поступает трафик 100 Мбит/с, на другую 200 Мбит/с. В этом случае пропускная способность канала между сенсором и Сервером должна быть не менее 150 Мбит/с $((200+100)/2=150)$.

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

- Операционная система Astra Linux® SE 1.6 с установленным обновлением 20200722SE16 (<https://wiki.astralinux.ru/pages/viewpage.action?pageId=103025136>).

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 Astra Linux SE 1.6 должны быть выполнены следующие условия:
 - Установлены стандартные компоненты операционной системы "Средства работы в сети" и "Сетевые сервисы" (дополнительно к стандартным компонентам, включенным по умолчанию для установки в операционной системе).
 - В операционной системе активен межсетевой экран, реализуемый программой настройки сетевой защиты UFW (для автоматической настройки сетевой фильтрации).
 - В операционной системе подключены репозитории с актуальными стабильными версиями пакетов для установки (например, подключены репозитории на дисках, содержащих обновление установочного диска операционной системы и обновление диска со средствами разработки)

► *Чтобы подключить репозиторий на диске,*

вставьте диск и в консоли операционной системы введите следующие команды:

```
sudo apt-cdrom add
sudo apt update
```

- Установлен интерпретатор языка Python версии 2.7.

► *Чтобы установить пакеты python2,*

в консоли операционной системы введите команду:

```
sudo apt install python2 libnsl
```

- Установлен пакет libcap2-bin.

▶ *Чтобы установить пакет libcap2-bin,*

в консоли операционной системы введите команду:

```
sudo apt install libcap2-bin
```

- Настроена символическая ссылка на установленную версию пакета python2.

▶ *Чтобы настроить символическую ссылку на установленную версию пакета python2,*

в консоли операционной системы введите команду:

```
sudo alternatives --set python /usr/bin/python2
```

- Установлен пакет python2-pyyaml.

▶ *Чтобы установить пакет python2-pyyaml,*

в консоли операционной системы введите команду:

```
sudo apt install python2-pyyaml
```

- Установлен пакет python-apt.

▶ *Чтобы установить пакет python-apt,*

в консоли операционной системы введите команду:

```
sudo apt install python-apt
```

- Установлен пакет сервера SSH (для централизованной установки компонентов программы).

▶ *Чтобы установить пакет сервера SSH,*

в консоли операционной системы введите следующие команды:

```
sudo apt install ssh  
systemctl enable ssh  
systemctl start ssh
```

- Включена локаль en_US.utf8 (на компьютере, с которого будет выполняться централизованная установка компонентов программы).

► *Чтобы включить локаль en_US.utf8,*

в консоли операционной системы введите команду:

```
sudo localedef -i en_US -f UTF-8 en_US.utf8
```

- Для работы компонентов программы на всех компьютерах, которые будут выполнять функции Сервера и сенсоров, в операционной системе Astra Linux SE 1.6 должны быть выполнены следующие условия:
 - Разрешены информационные потоки без ограничений со стороны механизма мандатного разграничения доступа (для всех объектов доступа установлена нулевая мандатная метка).
 - В операционной системе выключен механизм замкнутой программной среды.
- Для работы компонентов программы на компьютере, который будет выполнять функции Сервера, в операционной системе Astra Linux SE 1.6 дополнительно должны быть выполнены следующие условия:
 - Установлен интерпретатор языка Python версии 3.5, а также пакеты для работы коннекторов и скриптов преобразования данных python3-urllib3 python3-yaml python3-tz python3-dateutil python3-psycopg2 python3-cffi (если коннекторы будут работать на других компьютерах, перечисленные пакеты также требуется установить на эти компьютеры).

► *Чтобы установить пакеты для работы коннекторов и скриптов преобразования данных,*

в консоли операционной системы введите команду:

```
sudo apt install python3-urllib3 python3-yaml python3-tz  
python3-dateutil python3-psycopg2 python3-cffi
```

- Установлен и настроен почтовый сервер (Mail Transfer Agent – MTA) для отправки сообщений электронной почты через коннектор электронной почты.
- Установлен интерпретатор языка Perl версии 5.10 и выше (если устанавливается Агент администрирования Kaspersky Security Center).

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

Для 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 через веб-интерфейс могут использоваться следующие браузеры:

- Google Chrome™ версии 89.
- Mozilla™ Firefox™ версии 86.
- Microsoft® Edge версии 89.
- Chromium™ для Astra Linux версии 83.

Программа Kaspersky Industrial CyberSecurity for Networks совместима с Kaspersky Security Center версии 11 или 12.

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 активов.** 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. Дополнительно программа может определять параметры устройств для контроля процесса. 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.
- **Контроль взаимодействий.** Эта функциональность позволяет отслеживать взаимодействия между устройствами промышленной сети. Обнаруженные взаимодействия проверяются на соответствие разрешающим правилам контроля взаимодействий. При обнаружении взаимодействия, которое описано во включенном правиле, 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.

Функциональность для решения типовых задач оператора

Для решения типовых задач при наблюдении за состоянием технологического процесса и устройств 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 контролировать потребление аппаратных ресурсов, различные динамические данные и основные сведения об устройствах и событиях.
- **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 и отобразить эти сведения как в таблице событий, так и в виде взаимодействовавших объектов на карте сети. 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 значений тегов в онлайн-режиме.** Эта функциональность позволяет просматривать текущие значения параметров технологического процесса, которые обнаружены в трафике на текущий момент. Информация о получаемых значениях отображается в таблице тегов, сформированной для контроля процесса.
- **Отображение сведений об обнаруженных уязвимостях устройств.** Эта функциональность позволяет обнаруживать уязвимости в контролируемых устройствах промышленной сети. Для обнаружения уязвимостей программа сравнивает имеющиеся сведения об устройствах с определенными полями в базе данных уязвимостей. Информацию об уязвимостях можно просматривать как при работе с устройствами, так и в общей таблице уязвимостей.

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 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.
- **Управление узлами и точками мониторинга.** Эта функциональность позволяет добавить в программу узлы сенсоров и 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).
- **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.
- **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 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.

Указания по эксплуатации и требования к среде

Чтобы обеспечить безопасную работу программы на предприятии, рекомендуется усилить защиту компьютеров (см. раздел "Усиление защиты компьютеров с установленными компонентами программы" на стр. [46](#)), на которых установлены Сервер и сенсоры Kaspersky Industrial CyberSecurity for Networks, после установки Kaspersky Industrial CyberSecurity for Networks. Требуемый уровень защиты для безопасной работы программы реализуется операционной системой и ее средствами защиты. Для поддержания безопасного состояния рекомендуется регулярно устанавливать обновления баз и программных модулей (см. раздел "Обновление баз и программных модулей" на стр. [110](#)) Kaspersky Industrial CyberSecurity for Networks и обновления безопасности операционной системы.

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

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

При внедрении Kaspersky Industrial CyberSecurity for Networks рекомендуются следующие меры:

- Ограничение удаленного и локального доступа к компьютерам с установленными компонентами Kaspersky Industrial CyberSecurity for Networks.
- Регулярная проверка и обновление парольных политик для действующих учетных записей в операционных системах на компьютерах с установленными компонентами программы. Парольные

политики должны соответствовать рекомендациям по обеспечению требуемого уровня безопасности операционной системы.

- Обеспечение доступа к интерфейсам программы исключительно для персонала, обладающего полномочиями для установки и настройки программы, а также для пользователей, которые решают типовые задачи с помощью программы (операторы).
- Контроль физического доступа к оборудованию, на котором работает программа, и к используемому сетевому оборудованию с помощью технических средств или службы охраны.
- Мониторинг контролируемых помещений с помощью средств охранной сигнализации и видеонаблюдения.

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

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

- Обеспечение защиты трафика внутри интранет-системы.
- Обеспечение защиты подключений к внешним сетям.
- Использование цифровых сертификатов, изданных доверенными центрами сертификации.
- Использование учетных данных, удовлетворяющих требованиям к именам и паролям учетных записей пользователей программы (см. раздел "Создание учетной записи пользователя программы" на стр. [118](#)).
- Обеспечение конфиденциальности и уникальности паролей.

При угрозе компрометации пароля пользователь программы должен своевременно изменить свой пароль (см. раздел "Изменение пароля учетной записи" на стр. [120](#)).

- Настроенная синхронизация времени (см. раздел "Синхронизация времени на узлах Kaspersky Industrial CyberSecurity for Networks с источником времени для устройств промышленной сети" на стр. [109](#)) на узлах Kaspersky Industrial CyberSecurity for Networks.
- Завершение сеанса подключения через веб-интерфейс перед окончанием работы с браузером.

Для принудительного завершения сеанса подключения нужно использовать пункт **Выход** в меню пользователя (см. раздел "Завершение сеанса подключения к Серверу через веб-интерфейс" на стр. [55](#)).

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 каждой схеме развертывания Kaspersky Industrial CyberSecurity for Networks может использоваться только один Сервер.
- *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.

Для управления работой программы и для просмотра сведений пользователи подключаются к компонентам программы через веб-интерфейс. Подключение к компоненту через веб-интерфейс обеспечивает *веб-сервер*, который дополнительно устанавливается на компьютере с установленным компонентом. Для безопасного соединения с веб-сервером используются сертификаты.

Для получения данных от Kaspersky Industrial CyberSecurity for Networks или для обмена данными с программой к Серверу могут подключаться сторонние системы, а также Kaspersky Security Center. Подключение сторонних систем обеспечивают специальные программные модули – *коннекторы*. Для безопасного соединения через коннекторы также используются сертификаты.

Сервер Kaspersky Industrial CyberSecurity for Networks выполняет следующие функции:

- принимает информацию о трафике от сенсоров Kaspersky Industrial CyberSecurity for Networks и / или самостоятельно получает и обрабатывает поступающий трафик промышленной сети;
- обрабатывает и сохраняет полученные сведения об устройствах и их взаимодействиях;
- регистрирует и сохраняет события;
- анализирует накопленные данные;
- контролирует работоспособность программы;
- контролирует действия пользователей программы;
- обрабатывает поступающие запросы через веб-интерфейс и коннекторы и предоставляет запрашиваемые данные.

Сенсор Kaspersky Industrial CyberSecurity for Networks выполняет следующие функции:

- 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).

Для соединения с Сервером сенсоров и других компонентов 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 и сенсорам через веб-интерфейс;
- компьютер с Kaspersky Industrial CyberSecurity for Nodes;
- компьютер с Kaspersky Security Center;
- сетевой коммутатор.

Типовые схемы развертывания

В Kaspersky Industrial CyberSecurity for Networks предусмотрены следующие способы установки компонентов (см. раздел "Архитектура программы" на стр. [21](#)):

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

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

При любом способе установки рекомендуется использовать специальную выделенную сеть для соединения компонентов решения Kaspersky Industrial CyberSecurity (Kaspersky Industrial CyberSecurity for Networks, Kaspersky Industrial CyberSecurity for Nodes, Kaspersky 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 (на стр. [13](#)).

В этом разделе

Установка Сервера без внешних сенсоров	23
Установка Сервера и внешних сенсоров	24
Подключение Kaspersky Industrial CyberSecurity for Networks к промышленной сети через диод данных	26

Установка Сервера без внешних сенсоров

При установке Сервера без внешних 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 (см. раздел "Добавление точки мониторинга" на стр. [91](#)) на эти сетевые интерфейсы. 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.

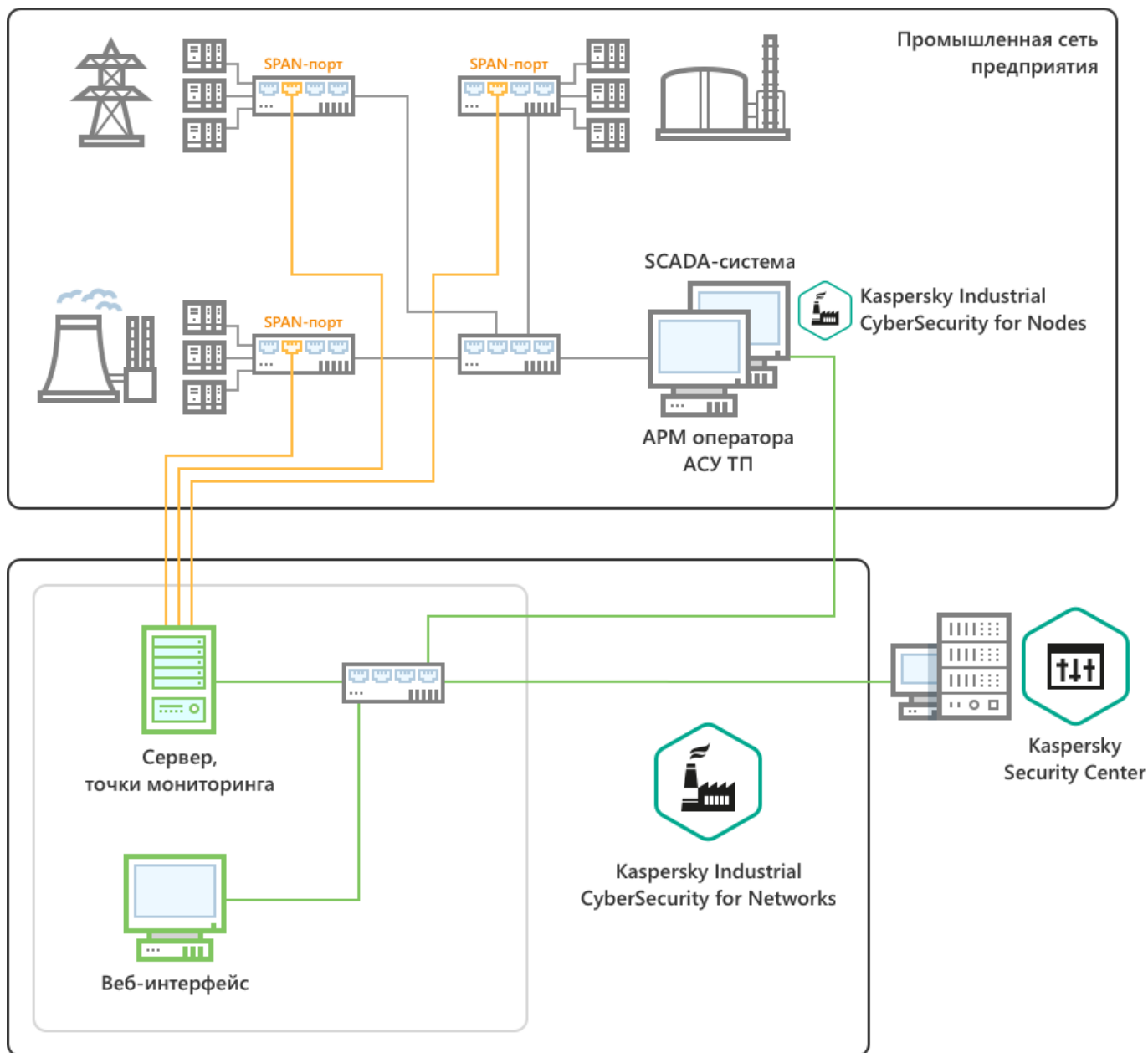


Рисунок 1. Пример схемы развертывания Сервера без сенсоров

Установка Сервера и внешних сенсоров

Для установки Сервера и внешних 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 (см. раздел "Добавление точки мониторинга" на стр. 91). Если компьютер с установленным Сервером имеет сетевой интерфейс, подключенный к промышленной сети, вы также можете добавить точку мониторинга на этот сетевой 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 разворачивания 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.

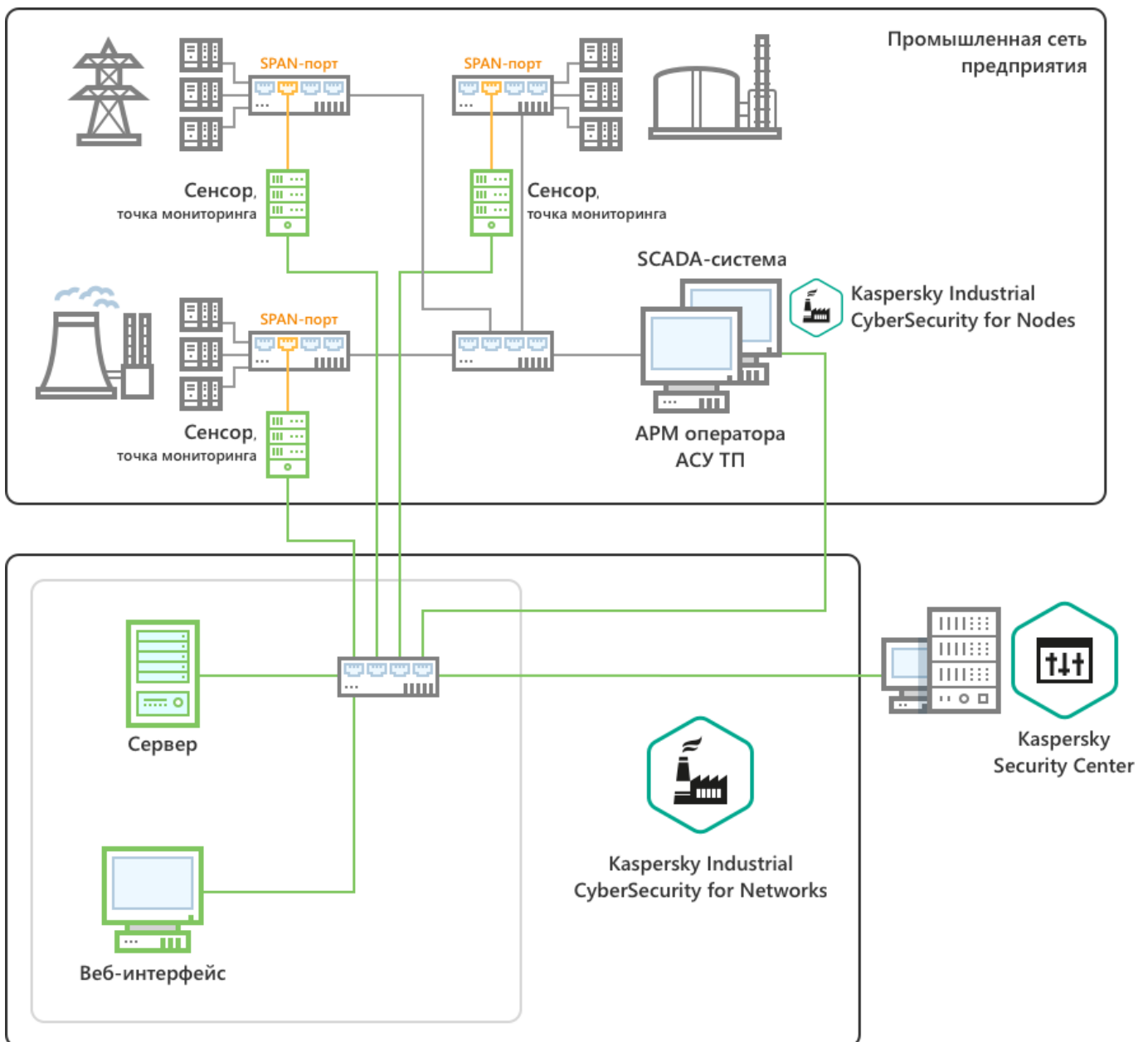


Рисунок 2. Пример схемы разворачивания Сервера и трех сенсоров

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

Для подключения Kaspersky Industrial CyberSecurity for Networks к промышленной сети вы можете дополнительно использовать специальные устройства, обеспечивающие одностороннюю передачу данных из промышленной сети. Такие устройства называются *диодом данных*. Диоды данных могут быть установлены на линиях соединений точек мониторинга Kaspersky Industrial CyberSecurity for Networks и SPAN-портов сетевых коммутаторов.

В примере (см. рис. ниже) показано подключение через диод данных к точке мониторинга на Сервере. В этой схеме развертывания применяется способ установки Сервера без внешних сенсоров.

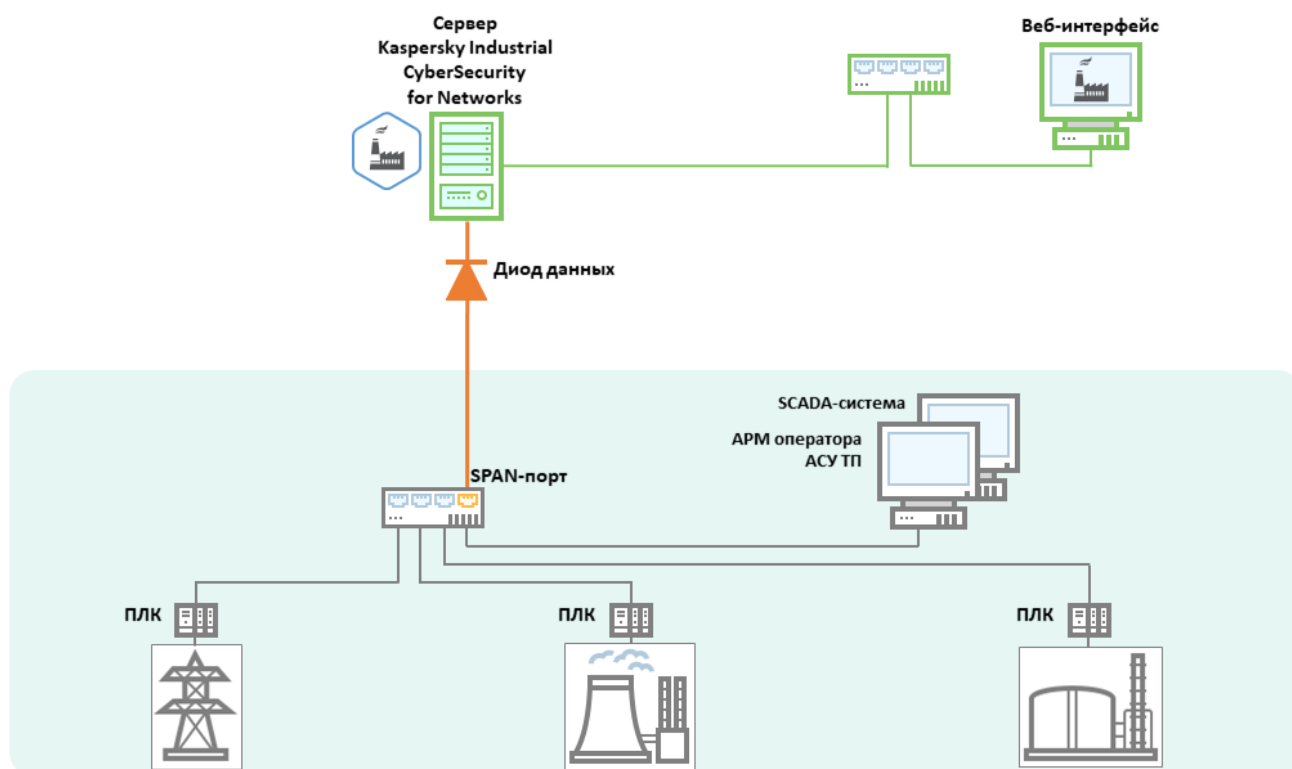


Рисунок 3. Пример схемы подключения Сервера через диод данных

В примере (см. рис. ниже) показано подключение нескольких сенсоров Kaspersky Industrial CyberSecurity for Networks через диоды данных. В этой схеме развертывания применяется способ установки Сервера и трех сенсоров.

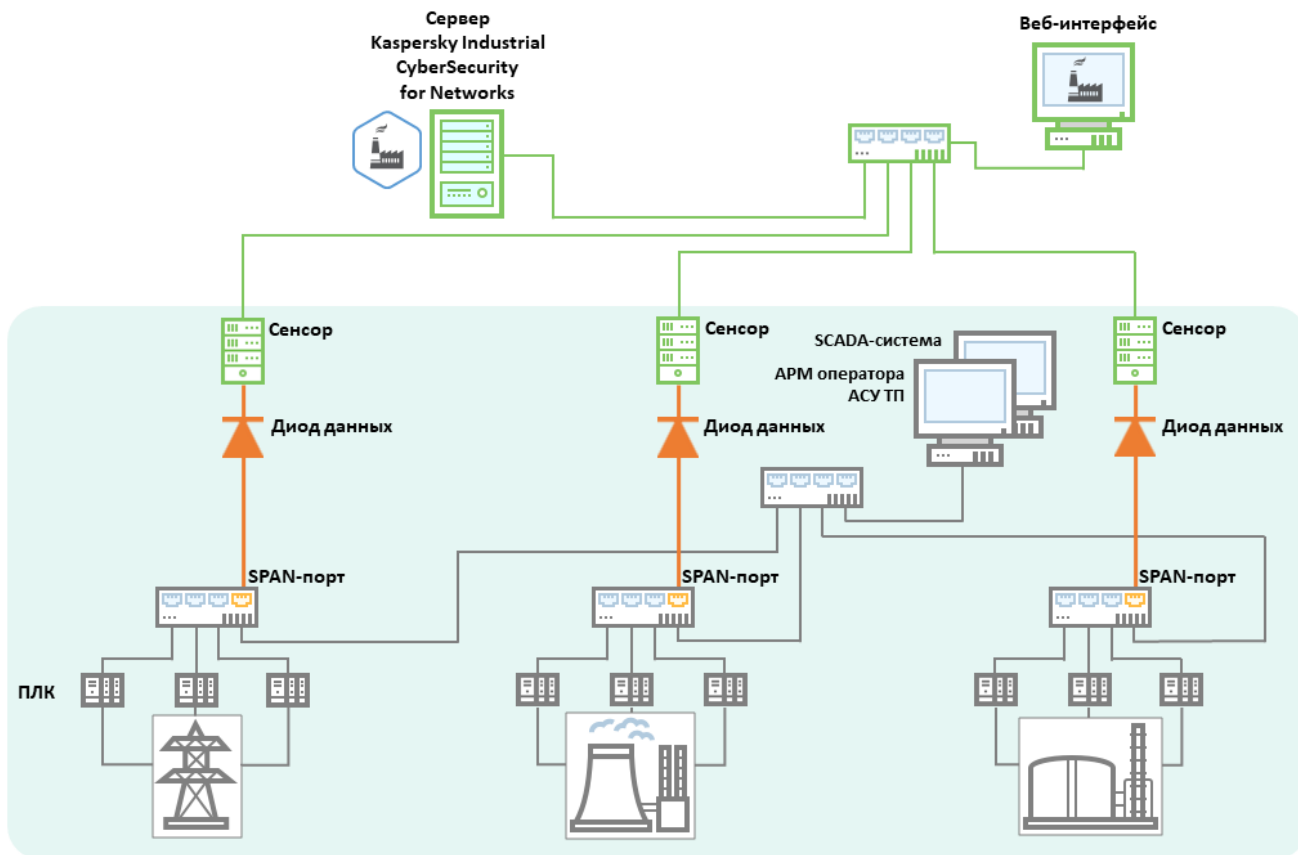


Рисунок 4. Пример схемы подключения сенсоров через диоды данных

Установка и удаление программы

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

В этом разделе

Подготовка к установке программы	28
Используемые порты для установки и работы компонентов.....	34
Использование скрипта централизованной установки компонентов программы	37
Использование скрипта локальной установки компонентов программы.....	48
Использование скрипта локального удаления компонентов программы	49
Установка плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center	50
Подготовка программы к работе	51
Начальная настройка программы после установки Сервера	52

Подготовка к установке программы

Перед началом установки Kaspersky Industrial CyberSecurity for Networks убедитесь, что компьютеры удовлетворяют аппаратным и программным требованиям (см. раздел «Аппаратные и программные требования» на стр. [13](#)). Также убедитесь, что соблюдаются рекомендации по обеспечению безопасной работы (см. раздел «Указания по эксплуатации и требования к среде» на стр. [19](#)) в отношении оборудования, аппаратного и программного обеспечения компьютеров.

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

Для установки компонентов программы на каждом компьютере должна быть учетная запись пользователя с root-правами, от имени которого будет выполняться установка. Вы можете добавить нужные учетные записи с помощью стандартных средств операционной системы. Если учетная запись пользователя с root-правами создается после установки операционной системы, для этой учетной записи требуется задать максимальный уровень целостности, чтобы предоставить возможность записи в директории для хранения данных программы (на стр. [80](#)) (уровень задается с помощью команды `sudo pdpl-user -i 63 <имя пользователя>`).

В зависимости от используемого скрипта установки компонентов программы и от типа устанавливаемых компонентов программы (см. раздел «Архитектура программы» на стр. [21](#)) вы можете выполнить следующие действия для подготовки к установке программы:

- Подготовка к централизованной установке компонентов

На компьютерах для централизованной установки компонентов проверьте выполнение следующих условий:

- К компьютерам есть сетевой доступ, настроен и открыт доступ по протоколу SSH.
- На компьютерах есть учетные записи пользователей с root-правами (от имени этих пользователей будет выполняться установка компонентов программы).
- На компьютерах отсутствуют учетные записи пользователей и групп со следующими именами, зарезервированными для взаимодействия компонентов программы (если такие учетные записи существуют, после установки программы они могут получить повышенные права доступа вплоть до root-прав):
 - kics4net;
 - kics4net-postgresql;
 - kics4net-websensor;
 - kics4net-websensor;
 - kics4net-connectors;
 - kics4net-fts.

► Чтобы подготовить компьютеры к установке компонентов программы, выполните следующие действия:

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

После установки компонентов программы рекомендуется изменить пароли для этих пользователей.

2. Выясните и сохраните следующие данные о компьютерах:
 - Имя и IP-адрес компьютера, который будет выполнять функции Сервера.
 - IP-адреса компьютеров, которые будут выполнять функции сенсоров.
 - Имя или IP-адрес и SSL-порт компьютера с Kaspersky Security Center.

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

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

Для подключения выполните следующие действия:

- a. Введите в командной строке команду:

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

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

- c. Для завершения сеанса подключения используйте команду:

```
exit
```

4. 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 централизованной установки компонентов программы kics4net-deploy-<номер версии программы>.bundle.sh.
- Если установка будет выполняться на компьютеры с операционной системой Astra Linux SE 1.6, скопируйте следующие файлы:
 - пакет для установки Сервера и сенсоров: kics4net_<номер версии программы>_amd64.deb;
 - пакет для установки системных коннекторов: kics4net-connectors_<номер версии программы>_amd64.deb;
 - пакет для установки системы полнотекстового поиска: kics4net-fts_<номер версии программы>_amd64.deb;
 - пакет для установки СУБД: kics4net-postgresql_<номер версии СУБД>_amd64.deb;
 - пакет для установки системы обнаружения вторжений: kics4net-suricata_<номер версии системы>_amd64.deb;
 - пакет для установки веб-сервера для сенсора программы: kics4net-websensor_<номер версии программы>_amd64.deb (этот пакет нужен, если вы хотите установить компонент сенсор на один или несколько компьютеров и подключаться к этому компоненту через веб-интерфейс);
 - пакет для установки веб-сервера для Сервера программы: kics4net-webserver_<номер версии программы>_amd64.deb;
 - пакет для установки Агента администрирования из состава комплекта поставки Kaspersky Security Center: klnagent64_<номер версии Агента администрирования>_amd64.deb (этот пакет 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 централизованном удалении компонентов программы.

- Подготовка к локальной установке Сервера

На компьютере для установки Сервера проверьте выполнение следующих условий:

- К компьютеру есть сетевой доступ.
- На компьютере есть учетная запись пользователя с root-правами (от имени этого пользователя будет запущен скрипт локальной установки).
- На компьютере отсутствуют учетные записи пользователей и групп со следующими именами, зарезервированными для взаимодействия компонентов программы (если такие учетные записи существуют, после установки программы они могут получить повышенные права доступа вплоть до root-прав):
 - kics4net;
 - kics4net-postgresql;
 - kics4net-webserver;
 - kics4net-connectors;
 - kics4net-fts.

► *Чтобы подготовить компьютер к локальной установке Сервера, выполните следующие действия:*

1. Выясните и сохраните следующие данные о компьютере:
 - Учетные данные пользователя с root-правами, от имени которого будет выполнен запуск скрипта локальной установки.
 - Имя и IP-адрес компьютера (для последующего подключения к этому компьютеру после установки Сервера).

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

2. Создайте произвольную директорию для хранения файлов установки.
3. В созданную директорию скопируйте следующие файлы из комплекта поставки Kaspersky Industrial CyberSecurity for Networks:
 - Скрипт локальной установки компонентов программы: `kics4net-install.sh`.
 - Если установка будет выполняться на компьютер с операционной системой Astra Linux SE 1.6, скопируйте следующие файлы:
 - пакет для установки Сервера и сенсоров: `kics4net_<номер версии программы>_amd64.deb`;
 - пакет для установки системных коннекторов: `kics4net-connectors_amd64.deb<номер версии программы>_amd64.deb`;

- пакет для установки системы полнотекстового поиска: kics4net-fts_amd64.deb<номер версии программы>_amd64.deb;
- пакет для установки СУБД: kics4net-postgresql_<номер версии СУБД>_amd64.deb;
- пакет для установки системы обнаружения вторжений: kics4net-suricata_<номер версии системы>_amd64.deb;
- пакет для установки веб-сервера для Сервера программы: kics4net-webserver_<номер версии программы>_amd64.deb;
- пакет для установки Агента администрирования из состава комплекта поставки Kaspersky Security Center: klnagent64_<номер версии Агента администрирования>_amd64.deb (этот пакет 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.

- Подготовка к локальной установке сенсора

На компьютере для установки сенсора проверьте выполнение следующих условий:

- К компьютеру есть сетевой доступ.
- На компьютере есть учетная запись пользователя с root-правами (от имени этого пользователя будет запущен скрипт локальной установки).
- На компьютере отсутствуют учетные записи пользователей и групп со следующими именами, зарезервированными для взаимодействия компонентов программы (если такие учетные записи существуют, после установки программы они могут получить повышенные права доступа вплоть до root-прав):
 - kics4net;
 - kics4net-websensor.

► Чтобы подготовить компьютер к локальной установке сенсора, выполните следующие действия:

1. Выясните и сохраните следующие данные о компьютере:

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

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

2. Создайте произвольную директорию для хранения файлов установки.

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

- Скрипт локальной установки компонентов программы: `kics4net-install.sh`.
- Если установка будет выполняться на компьютер с операционной системой Astra Linux SE 1.6, скопируйте следующие файлы:
 - пакет для установки Сервера и сенсоров: `kics4net_<номер версии программы>_amd64.deb`;
 - пакет для установки системы обнаружения вторжений: `kics4net-suricata_<номер версии системы>_amd64.deb`;
 - пакет для установки веб-сервера для сенсора программы: `kics4net-websensor_<номер версии программы>_amd64.deb`.

Используемые порты для установки и работы компонентов

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

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

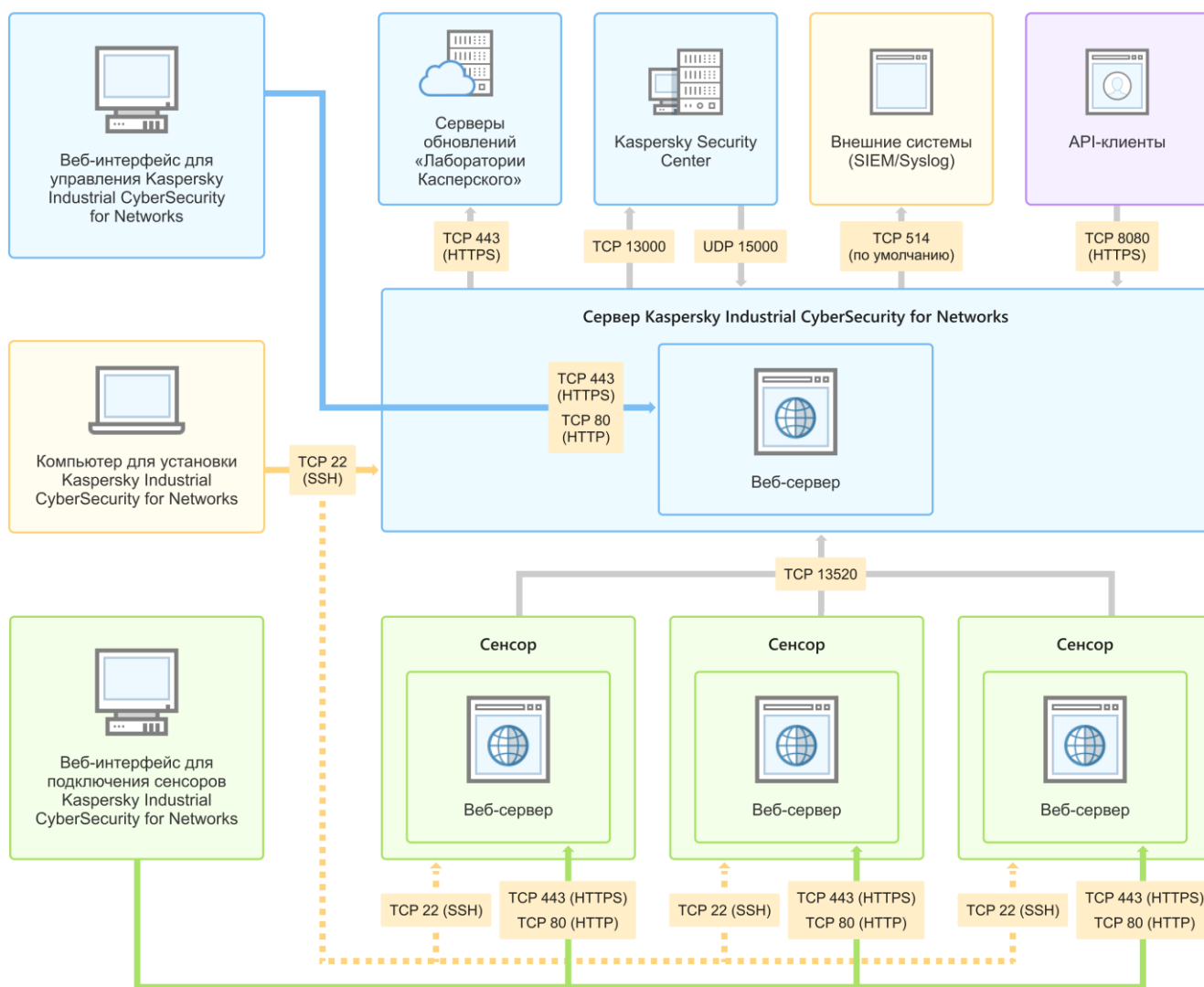


Рисунок 5. Используемые порты и протоколы

Назначение используемых портов описано в таблице ниже.

Таблица 1. Назначение используемых портов

Порт	Протокол	Описание
Компьютер для установки компонентов программы		
22	TCP (SSH)	Используется для подключения к узлам и установки компонентов Сервера и сенсоров.
Компьютер, выполняющий функции Сервера		
22	TCP (SSH)	Используется для взаимодействия с компьютером для установки компонентов программы.
80	TCP (HTTP)	Используется для подключения через веб-интерфейс.
443	TCP (HTTPS)	Используется для следующих целей: <ul style="list-style-type: none"> • подключение через веб-интерфейс; • подключение к серверам обновлений "Лаборатории Касперского".
8080	TCP (HTTP)	Используется для подключения через Kaspersky Industrial CyberSecurity for Networks API.
514	TCP	Используется для подключения сторонних систем через коннекторы.
13000	TCP	Используется для подключения к Серверу администрирования Kaspersky Security Center.
13520	TCP	Используется для подключений сенсоров.
15000	UDP	Используется для взаимодействия программы с Kaspersky Security Center.
Компьютер, выполняющий функции сенсора		
22	TCP (SSH)	Используется для взаимодействия с компьютером для установки компонентов программы.
80	TCP (HTTP)	Используется для подключения через веб-интерфейс.

Использование скрипта централизованной установки компонентов программы

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

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

В этом разделе

Централизованная установка компонентов программы	37
Команды меню централизованной установки	39
Изменение параметров и централизованная переустановка компонентов программы	43
Централизованная установка компонентов программы в неинтерактивном режиме	44
Усиление защиты компьютеров с установленными компонентами программы	46
Централизованное удаление компонентов программы	47

Централизованная установка компонентов программы

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

Перед централизованной установкой компонентов требуется выполнить действия для подготовки к установке программы (см. раздел "Подготовка к установке программы" на стр. [28](#)).

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

При централизованной установке компонентов 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 централизованную установку компонентов 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 централизованно установить компоненты 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 централизованной установки компонентов 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 компонентов 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. Возможность выбора языка локализации компонентов программы доступна при начальной настройке Kaspersky Industrial CyberSecurity for Networks (см. раздел "Начальная настройка программы после установки Сервера" на стр. [52](#)) после установки Сервера.

4. Если при запуске скрипта 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 централизованной установки компонентов программы.

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

На экране отобразится главное меню централизованной установки (см. раздел "Команды меню централизованной установки" на стр. [39](#)).

6. Выполните следующие действия:
 - a. С помощью пункта меню **Добавить Сервер** добавьте узел Сервера Kaspersky Industrial CyberSecurity for Networks.
 - b. При установке Сервера с сенсорами (см. раздел "Типовые схемы развертывания" на стр. [23](#)) добавьте узлы сенсоров с помощью пункта меню **Добавить сенсор**.
 - c. С помощью пункта меню **Изменить пользователя, от имени которого выполняется установка** укажите учетную запись пользователя с root-правами, от имени которого будет выполняться централизованная установка компонентов программы. Эта учетная запись будет использоваться на тех узлах, для которых не указана дополнительная учетная запись при настройке дополнительных параметров.

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

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

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

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

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

После завершения установки компонентов Kaspersky Industrial CyberSecurity for Networks программа не выполняет функции по контролю промышленной сети. Чтобы использовать программу, вам нужно выполнить действия для подготовки программы к работе (см. раздел "Подготовка программы к работе" на стр. [51](#)).

См. также

Команды меню централизованной установки[39](#)

Команды меню централизованной установки

В этом разделе приведены сведения об основных командах меню централизованной установки. Меню выводится на экран при запуске скрипта централизованной установки компонентов программы `kics4net-deploy-<номер версии программы>.bundle.sh`. Этот файл требуется запускать в директории, созданной при подготовке к установке программы (см. раздел "Подготовка к установке программы" на стр. [28](#)).

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

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

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

Главное меню содержит следующие группы команд:

- команды управления установкой Сервера

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

- **Добавить Сервер** – добавляет новый узел, которому будут назначены функции Сервера. Пункт присутствует, если Сервер еще не добавлен. При выборе этого пункта вам нужно указать основные параметры Сервера при появлении следующих запросов:
 - **Введите IP-адрес узла для установки** – задает IP-адрес, который будет использоваться для подключения к компьютеру по протоколу SSH и установки Сервера.
 - **Добавить функциональность взаимодействия программы с Kaspersky Security Center** – добавляет функциональность, которая позволит использовать Сервер администрирования Kaspersky Security Center для получения лицензионного ключа и загрузки обновлений, а также передавать в Kaspersky Security Center события и состояние программы. Для передачи событий в другие сторонние системы не требуется добавлять эту функциональность.

Если добавлена функциональность взаимодействия программы с Kaspersky Security Center, при установке программы устанавливается компонент Агент администрирования Kaspersky Security Center. 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 (не применяется в текущей версии).

- **Изменить параметры Сервера** – изменяет параметры добавленного Сервера. С помощью этого пункта меню вы можете изменить доступные для изменения основные параметры компонента и настроить дополнительные параметры. После выбора этого пункта появляется вложенное меню, в котором вы можете изменить следующие параметры:
 - **Указать дополнительного пользователя, от имени которого выполняется установка** – задает дополнительную учетную запись пользователя, от имени которого будет выполняться установка на узле Сервера. Дополнительную учетную запись нужно указать, если на этом узле имя пользователя с root-правами отличается от имени пользователя, заданного в пункте **Изменить пользователя, от имени которого выполняется установка**. Пароли всех учетных записей пользователей, от имени которых будет выполняться установка, должны совпадать.
 - **Включить аппаратный таймер наблюдения** – включает использование аппаратного таймера наблюдения. *Аппаратный таймер наблюдения* – это аппаратно реализованная схема контроля над зависанием системы. При наличии на узле аппаратного таймера наблюдения вы можете включить его использование в Kaspersky Industrial CyberSecurity for Networks. Если использование аппаратного таймера наблюдения включено, укажите для него путь в пункте **Указать путь к аппаратному таймеру наблюдения**.
 - **Добавить функциональность взаимодействия программы с Kaspersky Security Center** – добавляет функциональность взаимодействия программы с Kaspersky Security Center, если эта функциональность не была добавлена. Этот пункт меню аналогичен пункту **Добавить функциональность взаимодействия программы с Kaspersky Security Center** в меню **Добавить Сервер**.
 - **Удалить функциональность взаимодействия программы с Kaspersky Security Center** – удаляет функциональность взаимодействия программы с Kaspersky Security Center.
 - **Создать базу данных заново** – удаляет существующую базу данных и создает новую при переустановке программы.

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

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

- команды управления установкой сенсоров

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

- **Добавить сенсор** – добавляет новый узел, которому будут назначены функции сенсора. При выборе этого пункта вам нужно указать основные параметры сенсора при появлении запроса **Введите IP-адрес узла для установки**. В запросе вы можете задать IP-адрес, который будет использоваться для подключения к компьютеру по протоколу SSH и установки сенсора.
- **Изменить параметры сенсора** – изменяет параметры добавленного сенсора. С помощью этого пункта меню вы можете изменить доступные для изменения основные параметры сенсора и настроить дополнительные параметры. При выборе этого пункта меню отображается список узлов, на которых добавлены сенсоры. После выбора узла появляется вложенное меню, в котором вы можете изменить следующие параметры:
 - **Указать дополнительного пользователя, от имени которого выполняется установка** – задает дополнительную учетную запись пользователя, от имени которого будет выполняться централизованная установка на узле сенсора. Дополнительную учетную запись нужно указать, если на этом узле имя пользователя с root-правами отличается от имени пользователя, заданного в пункте **Изменить пользователя, от имени которого выполняется установка**. Пароли всех учетных записей пользователей, от имени которых будет выполняться установка, должны совпадать.
 - **Включить аппаратный таймер наблюдения** – включает использование аппаратного таймера наблюдения. *Аппаратный таймер наблюдения* – это аппаратно реализованная схема контроля над зависанием системы. При наличии на узле аппаратного таймера наблюдения вы можете включить его использование в Kaspersky Industrial CyberSecurity for Networks. Если использование аппаратного таймера наблюдения включено, укажите для него путь в пункте **Указать путь к аппаратному таймеру наблюдения**.
- **Удалить сенсор** – удаляет узел сенсора. При выборе этого пункта отображается список узлов, на которых добавлены сенсоры.

- общие команды установки

К общим командам меню установки относятся следующие команды:

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

- команды выхода из меню установки

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

- **Сохранить параметры и начать установку** – установить компоненты программы Kaspersky Industrial CyberSecurity for Networks в соответствии с заданными параметрами установки. При этом заданные параметры сохраняются в файле параметров установки. Скрипт централизованной установки программы сохраняет файл параметров установки на каждом компьютере, на котором этот скрипт выполняется.
- **Сохранить параметры и выйти без установки** – сохранить изменения в файле параметров установки, завершить работу скрипта централизованной установки программы и не выполнять установку компонентов.
- **Выйти без сохранения параметров** – завершить работу скрипта централизованной установки программы без сохранения изменений в файле параметров установки.

Изменение параметров и централизованная переустановка компонентов программы

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

- для добавления нового сенсора;
- для изменения параметров, которые могут быть заданы с помощью скрипта централизованной установки компонентов программы.

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

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

1. Запустите скрипт централизованной установки программы, выполнив пункты 1–4 процедуры установки (см. раздел "Централизованная установка компонентов программы" на стр. [37](#)).
2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.
На экране отобразится главное меню централизованной установки (см. раздел "Команды меню централизованной установки" на стр. [39](#)).

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 (см. раздел "Типовые схемы развертывания" на стр. [23](#)) укажите нужные параметры сенсоров с помощью пункта меню **Изменить параметры сенсора**.
Вы не можете изменить IP-адрес ранее добавленного сенсора. Если вы хотите изменить IP-адрес, вам нужно сначала удалить имеющийся сенсор и затем добавить его заново с новым IP-адресом с помощью пункта меню **Добавить сенсор**. Вы также можете использовать этот пункт меню для добавления новых сенсоров.
- С помощью пункта меню **Изменить пользователя, от имени которого выполняется установка** укажите имя пользователя с root-правами, от имени которого будет выполняться централизованная установка компонентов программы на компьютерах. Эта учетная запись будет использоваться на тех узлах, для которых не указана дополнительная учетная запись при настройке дополнительных параметров Сервера или сенсоров.

4. По окончании настройки параметров выберите пункт **Сохранить параметры и начать установку**.
На экране отобразится приглашение для ввода пароля пользователя, от имени которого выполняется установка.
5. Введите пароль пользователя, от имени которого выполняется установка. Пароль требуется ввести дважды: сначала в приглашении `SSH password` и затем в приглашении `BECOME password`.
Скрипт установки начнет установку компонентов. Во время установки на экране выводятся служебные сообщения о выполняемых операциях.

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

См. также

Команды меню централизованной установки[39](#)

Централизованная установка компонентов программы в неинтерактивном режиме

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

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

- ▶ Чтобы подготовить файл параметров централизованной установки с помощью скрипта, выполните следующие действия:
 1. Настройте параметры централизованной установки, выполнив пункты 1–6 процедуры установки (см. раздел "Централизованная установка компонентов программы" на стр. [37](#)).
 2. Сохраните файл параметров установки с помощью пункта меню **Сохранить параметры и выйти без установки**.
Файл параметров установки `inventory.json` сохранится в директории `/home/<user>/.config/kaspersky/kics4net-deploy/` (при этом компоненты программы не будут установлены).
 3. При необходимости скопируйте файл параметров централизованной установки в другую директорию.

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

При централизованной 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 централизованной установки компонентов в неинтерактивном режиме.

- ▶ Чтобы централизованно установить компоненты программы в неинтерактивном режиме, выполните следующие действия:
 1. На компьютере, с которого будет выполняться централизованная 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
```

где `silent-mode` – параметр включения неинтерактивного режима установки (обязательный параметр).
Дополнительно к обязательному параметру вы можете указать следующие параметры запуска скрипта установки:
 - `-i <путь к файлу параметров установки>` – указывает полный путь и имя файла параметров централизованной установки. Если параметр не задан, используется файл `inventory.json` в директории `/home/<user>/.config/kaspersky/kics4net-deploy/`.
 - `--enable-debug-grpc-server` – устанавливает отладочный gRPC-сервер. Этот gRPC-сервер используется для тестирования и не требуется при нормальном использовании программы.

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

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

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

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

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

Усиление защиты компьютеров с установленными компонентами программы

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

С помощью скрипта вы можете выполнить следующие действия:

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

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

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

► Чтобы усилить защиту компьютеров с помощью скрипта `kics4net-deploy-<номер версии программы>.bundle.sh`, выполните следующие действия:

1. На компьютере, с которого выполнялась централизованная 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 `BECOME password` введите пароль учетной записи пользователя, от имени которого выполняется централизованная установка.

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

Централизованное удаление компонентов программы

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

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

► Чтобы централизованно удалить компоненты программы на отдельных узлах, выполните следующие действия:

1. Запустите скрипт централизованной установки компонентов программы, выполнив пункты 1–4 процедуры установки (см. раздел "Централизованная установка компонентов программы" на стр. [37](#)).
2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.
На экране отобразится главное меню централизованной установки (см. раздел "Команды меню централизованной установки" на стр. [39](#)).
3. Выполните следующие действия (в зависимости от нужного результата):
 - С помощью пункта меню **Удалить Сервер** удалите узел Сервера.

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

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

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

► Чтобы полностью удалить программу, выполните следующие действия:

1. Запустите скрипт централизованной установки компонентов программы, выполнив пункты 1–4 процедуры установки (см. раздел "Централизованная установка компонентов программы" на стр. [37](#)).
2. В меню выбора варианта установки выберите пункт **Изменить параметры текущей установки**.
На экране отобразится главное меню централизованной установки (см. раздел "Команды меню централизованной установки" на стр. [39](#)).
3. С помощью пункта меню **Удалить Сервер** удалите узел Сервера.

4. Если в программу добавлены сенсоры, с помощью пункта меню **Удалить сенсор** последовательно удалите все узлы сенсоров.
5. С помощью пункта меню **Параметры удаления** настройте дополнительные параметры централизованного удаления. При выборе этого пункта выводятся следующие запросы:
 - **Удалить программу вместе с данными.** Если вы хотите удалить все данные, сохраненные программой в системе, введите символ `y`. Если удалять данные не требуется, введите символ `n`.
 - **Удалить Агент администрирования.** Если вы хотите удалить компонент Kaspersky Security Center Агент администрирования, введите символ `y`. Если удалять этот компонент не требуется, введите символ `n`. Запрос выводится при обнаружении установленного Агента администрирования.
6. Выберите пункт **Сохранить параметры и начать установку.**
7. В приглашениях `SSH password` и `BECOME password` введите пароль пользователя, от имени которого выполняется централизованное удаление.

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

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

Использование скрипта локальной установки компонентов программы

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

Перед локальной установкой компонентов требуется выполнить действия для подготовки к установке программы (см. раздел "Подготовка к установке программы" на стр. [28](#)).

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

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

► *Чтобы локально установить компонент Kaspersky Industrial CyberSecurity for Networks на компьютер, выполните следующие действия:*

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить скрипт локальной установки.
2. Перейдите в директорию с сохраненными файлами из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.
3. Введите команду запуска скрипта локальной установки компонентов программы:

```
bash kics4net-install.sh --<тип компонента>
```

где <тип компонента> – один из следующих параметров запуска:

- `server` – для установки Сервера;
- `sensor` – для установки сенсора.

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

Дождитесь завершения работы скрипта `kics4net-install.sh`.

Использование скрипта локального удаления компонентов программы

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

Скрипт локального удаления компонентов программы удаляет на компьютере файлы установленного компонента за исключением данных, сохраненных программой в системе.

► *Чтобы локально удалить компонент Kaspersky Industrial CyberSecurity for Networks на компьютере, выполните следующие действия:*

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить скрипт локального удаления.
2. Перейдите в директорию с сохраненными файлами из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.
3. Введите команду запуска скрипта локального удаления компонентов программы:

```
bash kics4net-remove.sh
```

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

Дождитесь завершения работы скрипта `kics4net-remove.sh`.

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

Плагин управления Kaspersky Industrial CyberSecurity for Networks 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. **Начальная настройка программы** (см. раздел "**Начальная настройка программы после установки Сервера**" на стр. [52](#))

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

2. **Добавление и подключение сенсоров** (см. раздел "**Добавление и подключение сенсора с использованием веб-интерфейса сенсора**" на стр. [85](#))

Этот этап выполняется для способа установки Сервера и внешних сенсоров (см. раздел "Типовые схемы развертывания" на стр. [23](#)). После выполнения этого этапа узлы с установленными сенсорами будут готовы к дальнейшей настройке.

3. **Добавление точек мониторинга** (см. раздел "**Управление точками мониторинга на узлах**" на стр. [90](#))

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

4. **Добавление пользователей программы** (см. раздел "**Разделение доступа к функциям программы**" на стр. [113](#))

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

5. **Добавление лицензионного ключа** (см. раздел "**Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс**" на стр. [76](#))

Этот этап выполняется для добавления в программу лицензионного ключа для активации функциональности обновления. После выполнения этого этапа вы сможете настроить и использовать функциональность обновления баз и программных модулей.

6. **Настройка обновления баз и программных модулей** (см. раздел "**Обновление баз и программных модулей**" на стр. [110](#))

Этот этап выполняется, если в программу добавлен лицензионный ключ. После выполнения этого этапа вы сможете устанавливать обновления баз и программных модулей.

7. **Настройка контроля активов** (на стр. [120](#))

На этом этапе формируются списки известных программе устройств и подсетей. После выполнения этого этапа в программе будет настроено отслеживание нужных устройств в промышленной сети.

8. **Настройка контроля процесса** (на стр. [152](#))

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

9. Настройка контроля взаимодействий (на стр. [185](#))

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

10. Настройка обнаружения вторжений (на стр. [202](#))

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

Начальная настройка программы после установки Сервера

После установки Сервера, выполненной с помощью скрипта централизованной установки (см. раздел «Централизованная установка компонентов программы» на стр. [37](#)) или другим способом, программа ожидает завершения начальной настройки. Завершить начальную настройку может любой пользователь, подключившийся к Серверу через веб-интерфейс.

► *Чтобы выполнить начальную настройку программы после установки Сервера, выполните следующие действия:*

1. Подключитесь к Серверу (см. раздел "Подключение к Серверу через веб-интерфейс" на стр. [54](#)) Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс. Для подключения используйте IP-адрес компьютера Сервера.
2. Выберите раздел **Начальная настройка**.
3. В поле **Язык локализации программы** выберите язык локализации компонентов Kaspersky Industrial CyberSecurity for Networks (и данных, которые предоставляют эти компоненты).
4. В блоке параметров **Учетная запись Администратора** задайте имя и пароль учетной записи первого пользователя программы. Этому пользователю будет назначена роль Администратор (см. раздел "Об учетных записях пользователей программы" на стр. [114](#)). Для этого пользователя не требуется регистрация в качестве учетной записи операционной системы компьютера Сервера или другого компьютера.

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

Пароль должен удовлетворять следующим требованиям:

- содержит от 12 до 256 символов ASCII;
- содержит одну или несколько прописных букв латинского алфавита;
- содержит одну или несколько строчных букв латинского алфавита;
- содержит одну или несколько цифр;
- содержит не более трех одинаковых символов подряд.

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

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

6. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности. Для этого последовательно откройте документы по соответствующим ссылкам в названиях флажков **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения и Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Я подтверждаю, что полностью прочитал и понимаю условия Политики конфиденциальности.**
7. Если вы полностью согласны с условиями Лицензионного соглашения и Политики конфиденциальности, то установите оба флажка.

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

8. Нажмите на кнопку **Продолжить**.

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

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

Запуск и остановка программы

Компонент программы, установленный на компьютере, запускается автоматически при загрузке операционной системы компьютера. Для работы компонента программы требуется выполнить его настройку. Настройка работы компонентов выполняется при подготовке программы к работе (см. раздел "Подготовка программы к работе" на стр. [51](#)).

Программа выполняет свои функции, если получает трафик промышленной сети через точки мониторинга (см. раздел "Управление точками мониторинга на узлах" на стр. [90](#)). Вы можете выключать (см. раздел "Выключение точек мониторинга" на стр. [92](#)) и включать (см. раздел "Включение точек мониторинга" на стр. [91](#)) точки мониторинга, чтобы приостанавливать и возобновлять анализ трафика, поступающего на эти точки мониторинга.

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

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

В этом разделе

Подключение к Серверу через веб-интерфейс.....	54
Завершение сеанса подключения к Серверу через веб-интерфейс	55
Подключение к сенсору через веб-интерфейс	56

Подключение к Серверу через веб-интерфейс

Вы можете подключиться к Серверу через веб-интерфейс с помощью любого поддерживаемого браузера (см. раздел "Аппаратные и программные требования" на стр. [13](#)). Подключение возможно с компьютера, который имеет доступ по сети к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks.

В Kaspersky Industrial CyberSecurity for Networks невозможно одновременно открыть несколько сеансов подключения к Серверу для одного и того же пользователя. Если пользователь подключился к Серверу через веб-интерфейс в тот момент, когда сеанс подключения этого пользователя не завершен в другом браузере (на этом или на другом компьютере), предыдущий сеанс подключения этого пользователя автоматически завершается.

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

1. Откройте браузер и введите в адресной строке:

`https://<имя Сервера>:<порт>`

где:

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

Если для веб-сервера не указан номер порта (до начальной настройки программы (см. раздел "Начальная настройка программы после установки Сервера" на стр. 52)) или указан номер порта по умолчанию (443), в адресной строке достаточно ввести только IP-адрес или имя компьютера Сервера. В этом случае протокол HTTPS и номер порта будут определены автоматически.

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

В окне браузера откроется страница веб-интерфейса Сервера (см. раздел "Веб-интерфейс Сервера Kaspersky Industrial CyberSecurity for Networks" на стр. 62) Kaspersky Industrial CyberSecurity for Networks. В имени закладки браузера со страницей веб-интерфейса будет указано имя Сервера, заданное при начальной настройке программы после установки (см. раздел "Начальная настройка программы после установки Сервера" на стр. 52).


Сеанс подключения к Серверу ограничен по времени. По умолчанию время действия сеанса составляет 10 часов (вы можете изменять время действия сеанса с помощью скрипта kics4net-params.py (см. раздел "Изменение времени действия для сеансов подключения и токенов аутентификации с помощью скрипта" на стр. 395)). Если с момента подключения прошло 10 часов, происходит переход с текущей страницы веб-интерфейса программы на страницу ввода учетных данных. В этом случае для продолжения работы вам потребуется снова ввести имя и пароль пользователя программы.

Завершение сеанса подключения к Серверу через веб-интерфейс

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

Если вы закрыли окно браузера без завершения сеанса подключения, сеанс останется действующим. По умолчанию время действия сеанса составляет 10 часов (вы можете изменять время действия сеанса с помощью скрипта kics4net-params.py (см. раздел "Изменение времени действия для сеансов подключения и токенов аутентификации с помощью скрипта" на стр. 395)). В течение этого времени программа может предоставить доступ к веб-интерфейсу Сервера Kaspersky Industrial CyberSecurity for Networks без запроса учетных данных пользователя, если для повторного подключения используются те же компьютер, браузер и учетная запись операционной системы.

► *Чтобы завершить сеанс подключения к Серверу Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:*

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

В окне браузера отобразится страница ввода учетных данных.

Подключение к сенсору через веб-интерфейс

Вы можете подключиться к сенсору Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс. На странице веб-интерфейса сенсора вы можете выполнять следующие действия:

- загружать на сенсор файл свертки (см. раздел "Добавление и подключение сенсора с использованием веб-интерфейса сенсора" на стр. [85](#)) для подключения сенсора к Серверу Kaspersky Industrial CyberSecurity for Networks;
- просматривать отпечаток запроса на подпись сертификата для сравнения с отпечатком на странице веб-интерфейса Сервера, если подключение сенсора к Серверу выполняется автоматически по сети;
- просматривать сведения о состоянии подключения сенсора к Серверу.

Для подключения к сенсору через веб-интерфейс вы можете использовать любой поддерживаемый браузер (см. раздел "Аппаратные и программные требования" на стр. [13](#)). Подключение возможно с компьютера, который имеет доступ по сети к компьютеру сенсора.

► *Чтобы подключиться к сенсору Kaspersky Industrial CyberSecurity for Networks,*

откройте браузер и введите в адресной строке:

`https://<имя сенсора>:<порт>`

где:

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

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

В окне браузера откроется страница веб-интерфейса сенсора (см. раздел "Веб-интерфейс сенсора Kaspersky Industrial CyberSecurity for Networks" на стр. [72](#)) Kaspersky Industrial CyberSecurity for Networks. В имени закладки браузера со страницей веб-интерфейса будет указано имя сенсора, заданное при добавлении сенсора (см. раздел "Добавление и подключение сенсора с использованием веб-интерфейса сенсора" на стр. [85](#)).

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние.....	57
Проверка регистрации событий с помощью тестового сетевого пакета	58
Контроль целостности модулей программы	60

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполнены все действия, указанные в разделах Подготовка к установке программы (на стр. [28](#)), Централизованная установка компонентов программы (на стр. [37](#)) и Подготовка программы к работе (на стр. [51](#)).

Для проверки безопасного состояния программы убедитесь, что выполняются следующие условия:

- Все компьютеры, на которых установлены компоненты программы, удовлетворяют требованиям, указанным в разделе Аппаратные и программные требования (на стр. [13](#)).
- Программа установлена согласно инструкции в разделе Централизованная установка компонентов программы (на стр. [37](#)).
- Все узлы с установленными компонентами программы находятся в состоянии *ОК* (см. раздел *"Просмотр сведений об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах"* на стр. [104](#)).
- Включен аудит действий пользователей (см. раздел "Включение и выключение аудита действий пользователей" на стр. [213](#)).
- Все функции защиты в программе включены (на странице веб-интерфейса Сервере не отображается значок и уведомление о выключенных функциях защиты (см. раздел "Контроль состояния программы при подключении через веб-интерфейс" на стр. [95](#))).
- Настроен контроль активов (см. раздел "Настройка контроля активов" на стр. [120](#)).
- Настроены все необходимые правила контроля технологического процесса (см. раздел "Настройка контроля процесса" на стр. [152](#)).
- Настроен контроль взаимодействий (см. раздел "Настройка контроля взаимодействий" на стр. [185](#)) (отсутствуют включенные правила для неразрешенных сетевых взаимодействий).
- Настроены параметры регистрации событий (см. раздел "Настройка типов событий" на стр. [225](#)) (включая параметры передачи событий в сторонние системы (см. раздел "Настройка передачи событий через коннекторы" на стр. [231](#))).
- Загружены и применены все необходимые правила обнаружения вторжений (см. раздел "Настройка обнаружения вторжений" на стр. [202](#)).

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 активов. Событие регистрируется независимо от наличия устройств в таблице устройств, известных программе. При этом должно быть включено применение метода обнаружения активности устройств.

Для регистрации используются системные типы событий (см. раздел «Системные типы событий в Kaspersky Industrial CyberSecurity for Networks» на стр. [414](#)), которым присвоены следующие коды:

- 4000000001 – для события по технологии Контроль технологического процесса;
- 4000000002 – для события по технологии Контроль целостности сети;
- 4000000003 – для события по технологии Обнаружение вторжений;
- 4000000004 – для события по технологии Контроль активов.

Вы можете просмотреть тестовые события в таблице зарегистрированных событий (см. раздел "Мониторинг событий и инцидентов" на стр. [305](#)).

Для проверки функции аудита Kaspersky Industrial CyberSecurity for Networks сохраняет информацию о регистрации тестовых событий в журнале аудита (см. раздел "Просмотр записей аудита действий пользователей" на стр. [100](#)). 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 (<http://www.secdev.org/projects/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.

Контроль целостности модулей программы

Вы можете проверить целостность установленных модулей программы, чтобы убедиться в отсутствии изменений в этих модулях после установки.

Для проверки целостности используется скрипт `kics4net-manifest-checker-<номер версии программы>.bundle.sh`, который входит в комплект поставки Kaspersky Industrial CyberSecurity for Networks. Скрипт сравнивает контрольные суммы установленных модулей программы с эталонными значениями.

Скрипт проверяет файлы модулей программы по специальным спискам, которые хранятся в *файлах манифеста*. Файлы манифеста включены в пакеты для установки программы и содержат списки файлов соответствующих пакетов. Для каждого пакета программы имеется свой файл манифеста. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

Результаты работы скрипта `kics4net-manifest-checker-<номер версии программы>.bundle.sh` могут быть неправильными в случае внесения каких-либо изменений в файл скрипта. Для правильных результатов работы используйте только ту версию скрипта, которая входит в комплект поставки Kaspersky Industrial CyberSecurity for Networks.

Проверка целостности модулей программы с помощью скрипта выполняется локально на каждом компьютере с установленными компонентами программы.

В процессе работы скрипт последовательно проверяет контрольные суммы файлов из пакетов программы, установленных в операционной системе.

На компьютере, который выполняет функции Сервера, при проверке целостности должны быть проверены контрольные суммы для файлов из следующих пакетов программы (пакеты должны быть установлены на компьютере):

- `kics4net`;
- `kics4net-postgresql`;
- `kics4net-suricata`;
- `kics4net-webserver`;
- `kics4net-connectors`;
- `kics4net-fts`;
- `klagent64` (при использовании функциональности передачи событий и состояния программы в Kaspersky Security Center).

На компьютере, который выполняет функции сенсора, при проверке целостности должны быть проверены контрольные суммы для файлов из следующих пакетов программы (пакеты должны быть установлены на компьютере):

- `kics4net`;
- `kics4net-suricata`;
- `kics4net-websensor`.

► Чтобы проверить целостность модулей программы на компьютере, выполните следующие действия:

1. Скопируйте в произвольную директорию файл скрипта `kics4net-manifest-checker-<номер версии программы>.bundle.sh` из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.
2. В консоли операционной системы перейдите в директорию, в которой находится файл скрипта, и введите команду:

```
sudo bash kics4net-manifest-checker-<номер версии программы>.bundle.sh
```

Информация о результатах проверки отобразится в консоли операционной системы.

Результаты проверки целостности модулей программы на компьютере признаются успешными, если выполнены оба следующих условия:

- Скрипт `kics4net-manifest-checker-<номер версии программы>.bundle.sh` завершил работу с сообщением: Проверка файлов всех установленных пакетов, содержащих файл манифеста, завершена успешно.
- Для всех пакетов программы, которые должны быть установлены на компьютере согласно выполняемым функциям (см. выше), отсутствуют сообщения об ошибках или хотя бы одно из следующих сообщений:
 - Пакет не установлен в операционной системе.
 - Файл манифеста для пакета не найден.

Интерфейс программы

Этот раздел содержит информацию об основных элементах интерфейса программы.

В этом разделе

Веб-интерфейс Сервера Kaspersky Industrial CyberSecurity for Networks	62
Веб-интерфейс сенсора Kaspersky Industrial CyberSecurity for Networks	72

Веб-интерфейс Сервера Kaspersky Industrial CyberSecurity for Networks

При подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс (см. раздел "Подключение к Серверу через веб-интерфейс" на стр. [54](#)) в браузере открывается страница веб-интерфейса Сервера. Содержание страницы веб-интерфейса зависит от режима работы программы и от роли учетной записи (см. раздел "Об учетных записях пользователей программы" на стр. [114](#)) подключенного пользователя.

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

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

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

В этом разделе



О веб-интерфейсе Сервера в режиме начальной настройки программы	62
О веб-интерфейсе Сервера в основном режиме работы программы	64

О веб-интерфейсе Сервера в режиме начальной настройки программы

После установки программы при первом подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс (см. раздел «Подключение к Серверу через веб-интерфейс» на стр. [54](#)) программа не запрашивает учетные данные пользователя для входа. Вместо страницы ввода учетных данных открывается страница, содержащая элементы управления для настройки Сервера и для просмотра и принятия Лицензионного соглашения и Политики конфиденциальности.

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

Меню веб-интерфейса содержит следующие элементы:

-  – разворачивает и сворачивает меню. Если меню свернуто, элементы отображаются без текстовых пояснений.
-  – открывает раздел **Начальная настройка**

В разделе **Начальная настройка** веб-интерфейса Сервера (см. рис. ниже) вы можете указать основные параметры Сервера программы (см. раздел «Начальная настройка программы после установки Сервера» на стр. 52), которые требуются для начала работы программы после ее установки.

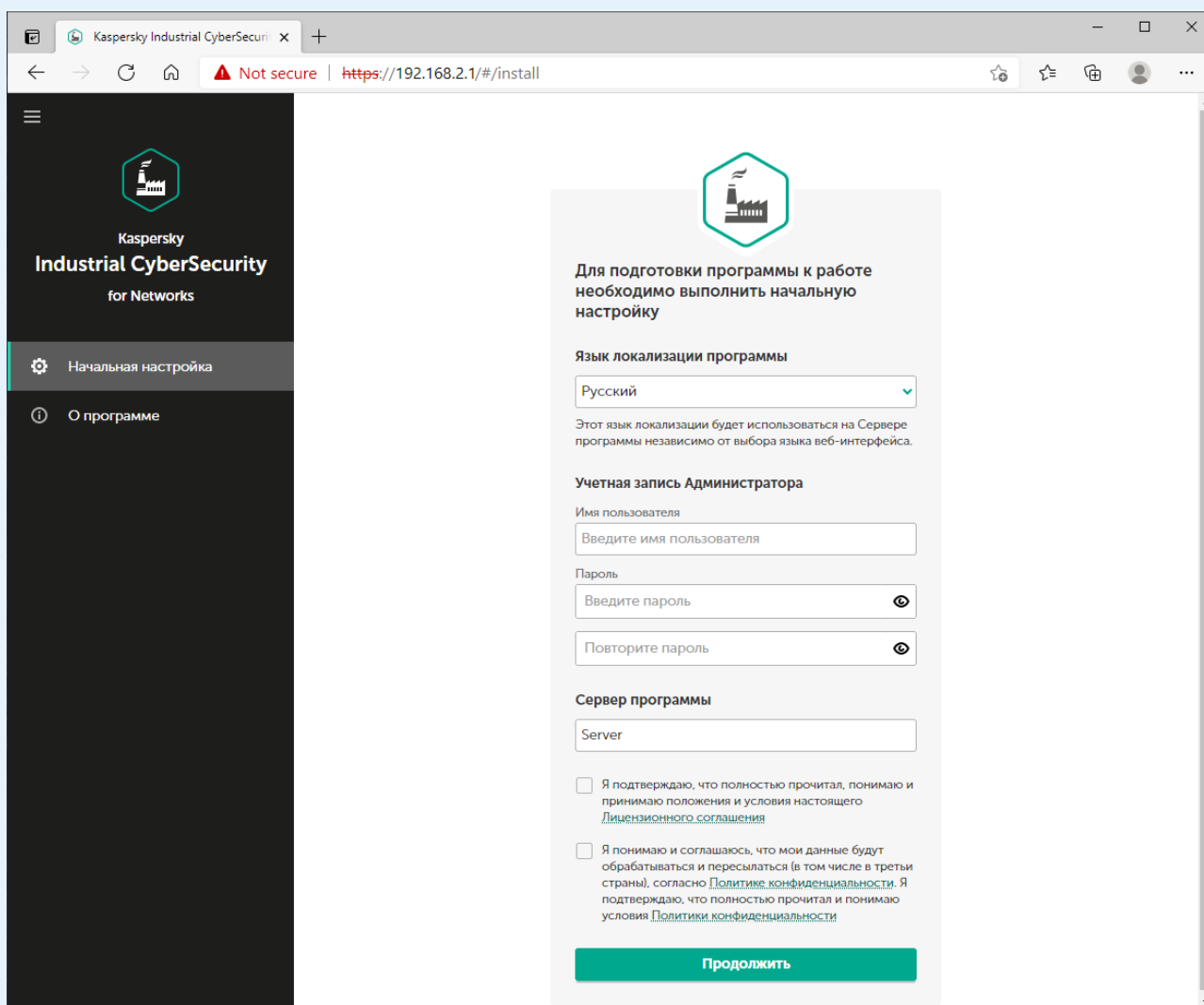


Рисунок 6. Раздел **Начальная настройка**

Раздел содержит окно, с помощью которого вы можете настроить основные параметры Сервера, создать первого пользователя с ролью Администратор и ознакомиться и принять условия Лицензионного соглашения и Политики конфиденциальности. После выполнения этих действий данная страница веб-интерфейса автоматически закрывается (в том числе и в других сеансах подключения к Серверу через веб-интерфейс) и происходит переход на страницу веб-интерфейса Сервера в основном режиме работы программы (см. раздел "Веб-интерфейс Сервера Kaspersky Industrial CyberSecurity for Networks" на стр. [62](#)).





-  – открывает раздел с краткой информацией о программе.

О веб-интерфейсе Сервера в основном режиме работы программы

В основном режиме работы программы после подключения к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс (см. раздел «Подключение к Серверу через веб-интерфейс» на стр. [54](#)) открывается страница, содержащая средства для работы с программой. Состав доступных средств и их функциональность зависят от роли пользователя (см. раздел «Об учетных записях пользователей программы» на стр. [114](#)), под которым выполнено подключение к Серверу.

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

Меню веб-интерфейса содержит следующие элементы:

-  – разворачивает и сворачивает меню. Если меню свернуто, элементы отображаются без текстовых пояснений.
-  – открывает список уведомлений о проблемах в работе программы (см. раздел "Контроль состояния программы при подключении через веб-интерфейс" на стр. [95](#)). О наличии уведомлений информирует значок, цвет которого соответствует статусу уведомлений.
-  – открывает список фоновых операций. Список содержит информацию о выполнении операций, занимающих длительное время (например, формирование файла при экспорте большого количества событий). О количестве активных фоновых операций и о статусе их выполнения информирует значок. Значок имеет красный цвет, если есть операции, при выполнении которых возникли ошибки.
-  – открывает раздел **Мониторинг**

В разделе **Мониторинг** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать в онлайн-режиме (см. раздел "Мониторинг системы в онлайн-режиме" на стр. 253) сведения о текущем состоянии системы.

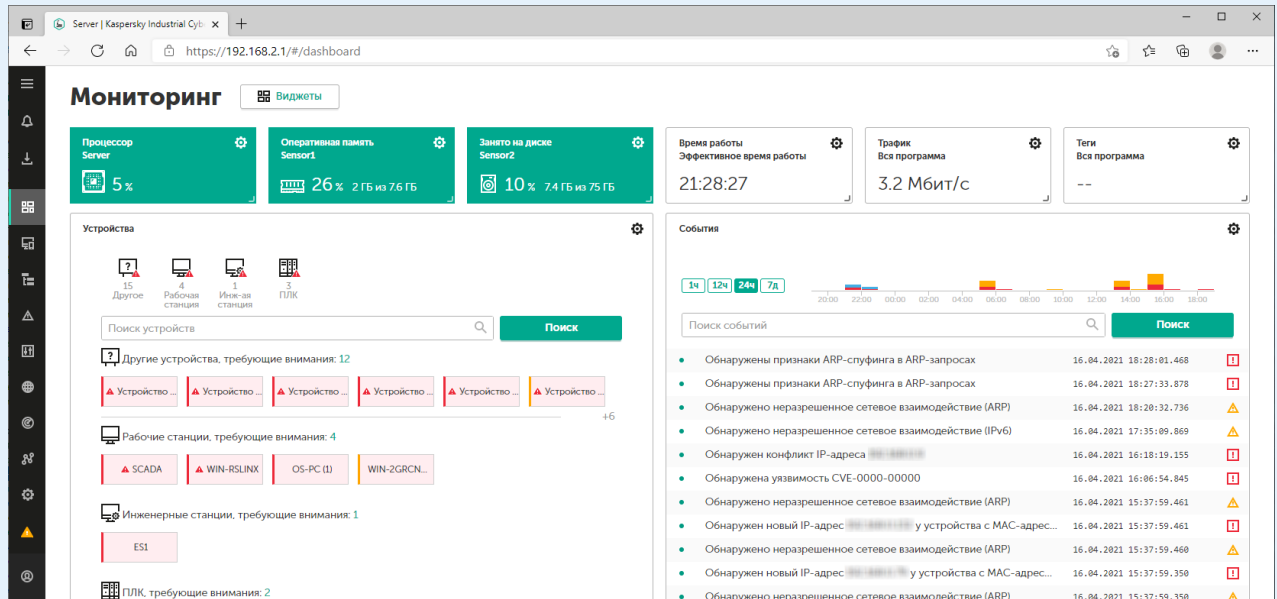


Рисунок 7. Раздел **Мониторинг**

- открывает раздел **Активы**

В разделе **Активы** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и изменять (см. раздел "Настройка контроля активов" на стр. 120) сведения об устройствах и параметры подсетей, известных программе.

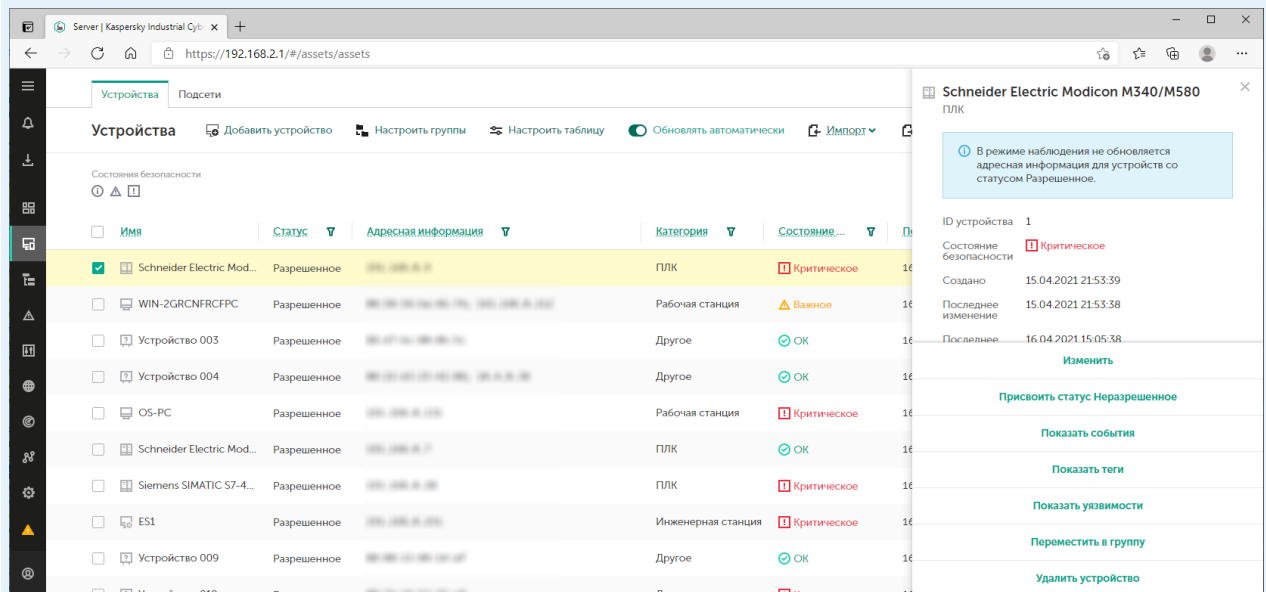



Рисунок 8. Раздел **Активы**

Раздел **Активы** содержит закладки с таблицами устройств и подсетей.

При выборе устройства или подсети открывается область деталей в правой части раздела.

Область деталей содержит сведения о выбранных элементах и инструменты для работы с ними.

-  – открывает раздел **Карта сети**

В разделе **Карта сети** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать (см. раздел "Работа с картой сети" на стр. [282](#)) сведения о взаимодействиях устройств.

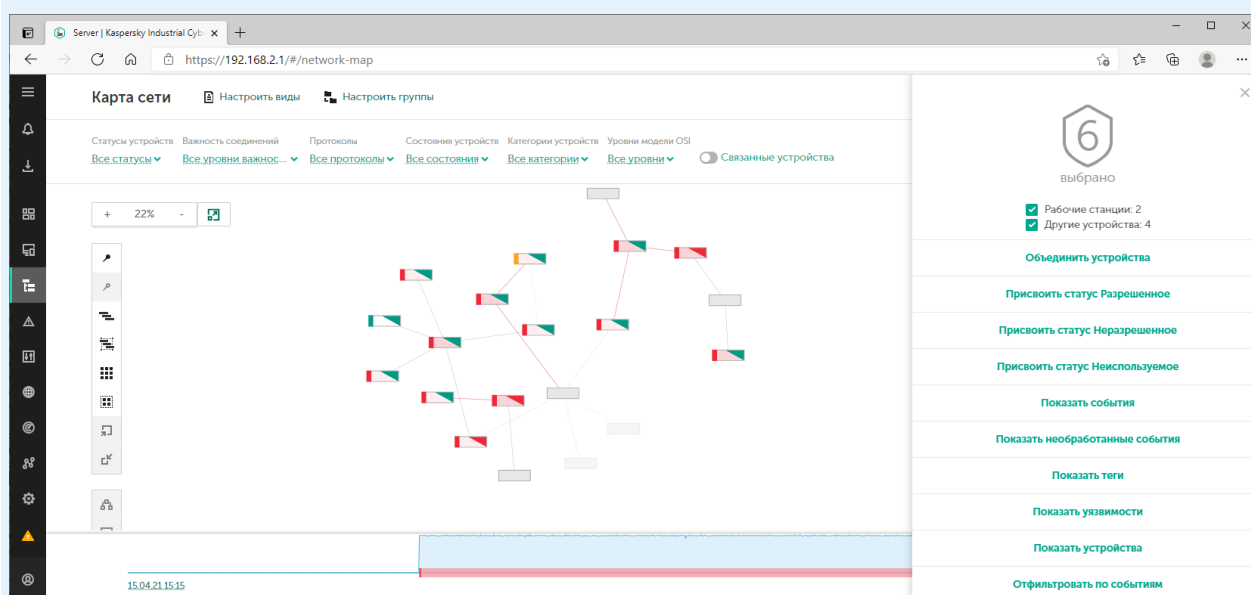



Рисунок 9. Раздел **Карта сети**

Раздел **Карта сети** содержит основную панель инструментов в верхней части, область отображения объектов карты сети и дополнительные панели инструментов для управления размещением объектов. В нижней части раздела расположена временная шкала для фильтрации объектов по периоду времени.

При выборе объектов открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранных объектах и инструменты для работы с ними.

-  – открывает раздел **События**

В разделе **События** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и обрабатывать (см. раздел "Мониторинг событий и инцидентов" на стр. [305](#)) события и инциденты, зарегистрированные программой.

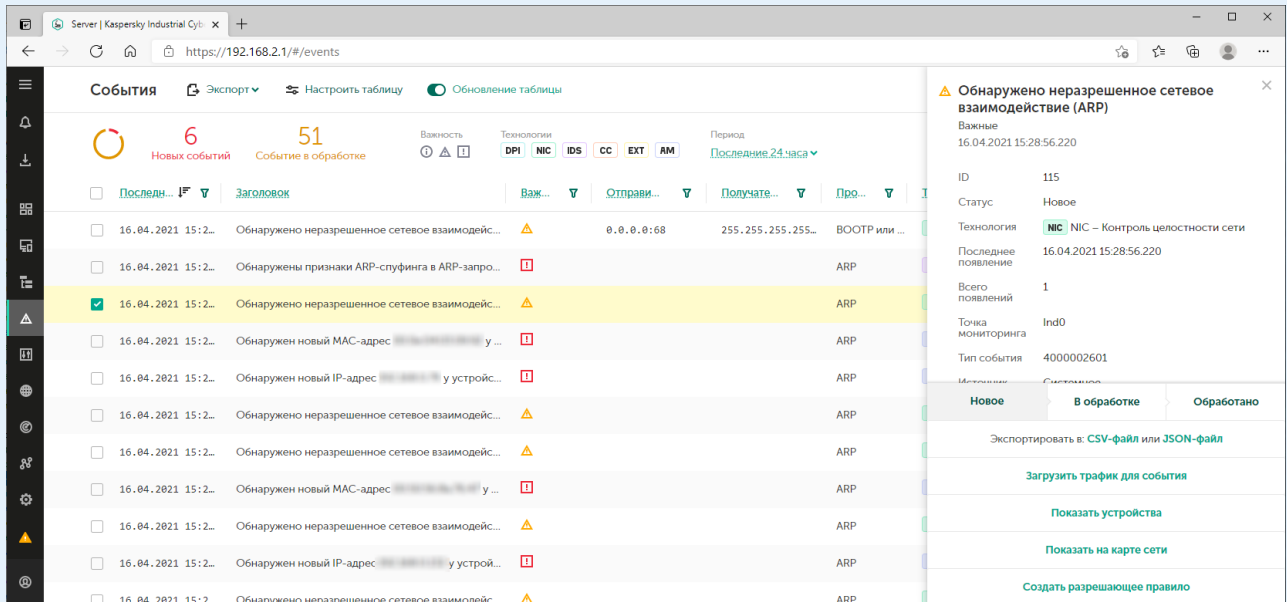



Рисунок 10. Раздел **События**

Раздел **События** содержит панель инструментов и таблицу событий.

При выборе событий открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранных событиях и инструменты для работы с ними.

-  – открывает раздел **Контроль процесса**

В разделе **Контроль процесса** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и изменять (см. раздел "Настройка контроля процесса" на стр. [152](#)) теги и правила контроля процесса.

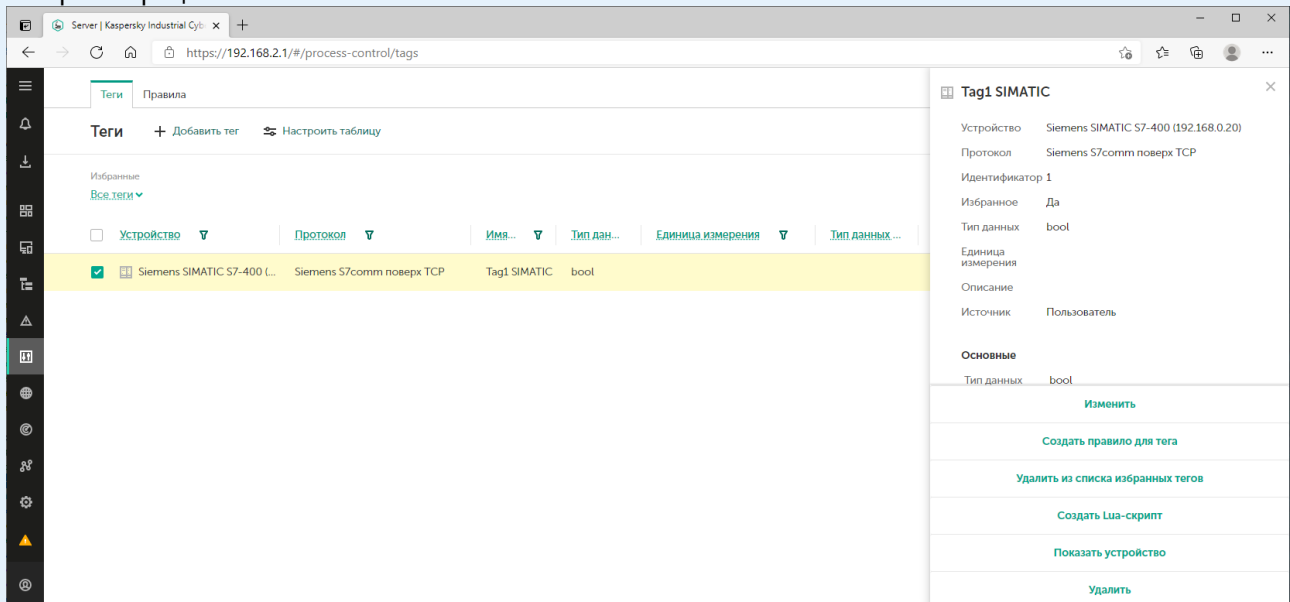



Рисунок 11. Раздел **Контроль процесса**

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

При выборе тегов или правил открывается область деталей в правой части раздела.

-  – открывает раздел **Разрешающие правила**

В разделе **Разрешающие правила** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и изменять (см. раздел "Настройка контроля взаимодействий" на стр. [185](#)) разрешающие правила для программы.

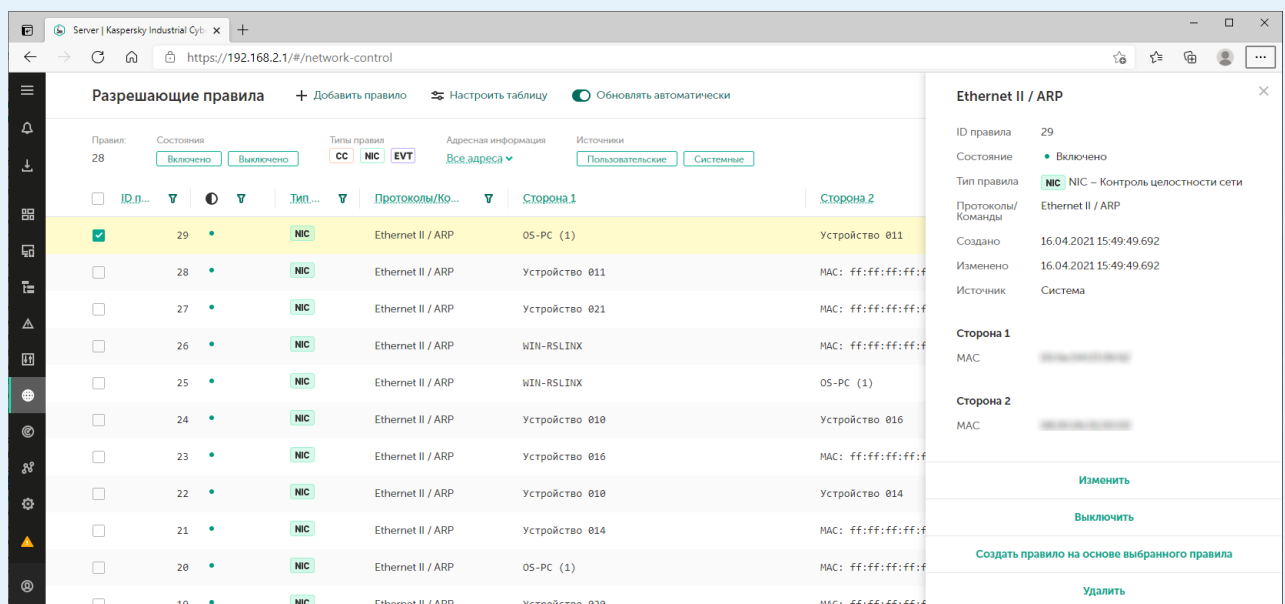


Рисунок 12. Раздел **Разрешающие правила**

Раздел **Разрешающие правила** содержит панель инструментов и таблицу разрешающих правил для контроля взаимодействий (см. раздел «Настройка контроля взаимодействий» на стр. [185](#)) и для событий (см. раздел «Мониторинг событий и инцидентов» на стр. [305](#)).

При выборе правил открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранных правилах и инструменты для работы с ними.

-  – открывает раздел **Обнаружение вторжений**

В разделе **Обнаружение вторжений** веб-интерфейса Сервера программы (см. рис. ниже) вы можете управлять наборами правил обнаружения вторжений (см. раздел "Настройка обнаружения вторжений" на стр. [202](#)).

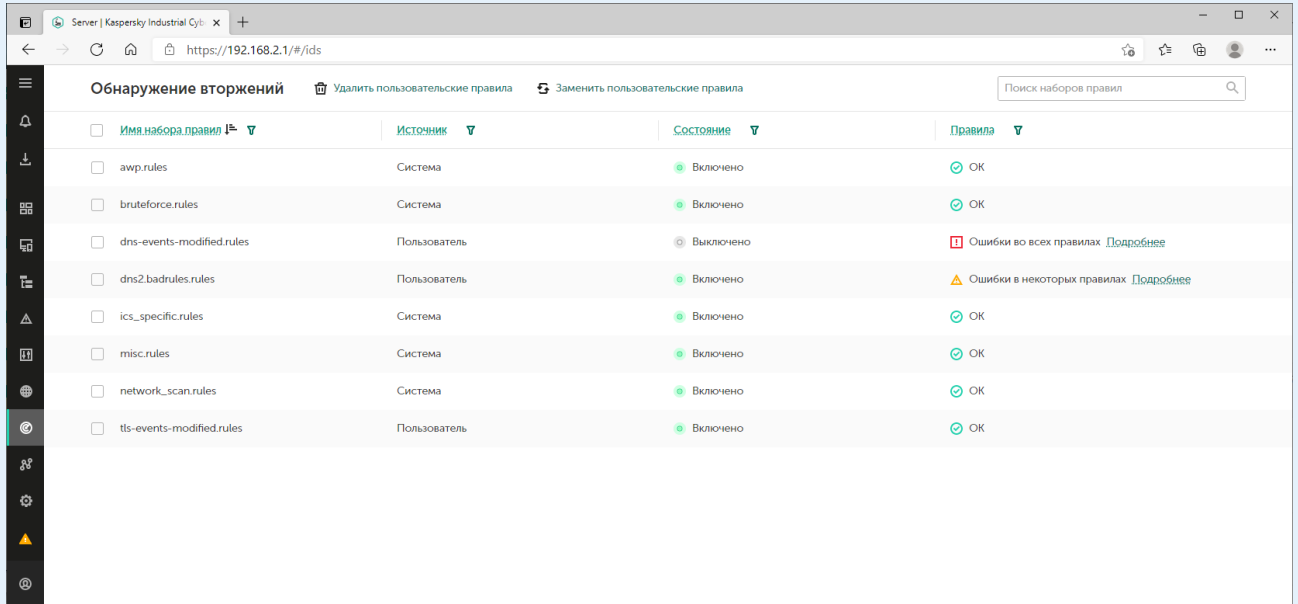



Рисунок 13. Раздел **Обнаружение вторжений**

Раздел **Обнаружение вторжений** содержит панель инструментов и таблицу с наборами правил.

-  – открывает раздел **Уязвимости**

В разделе **Уязвимости** веб-интерфейса Сервера программы (см. рис. ниже) вы можете просматривать и обрабатывать (см. раздел "Контроль уязвимостей устройств" на стр. [331](#)) уязвимости, обнаруженные в устройствах.

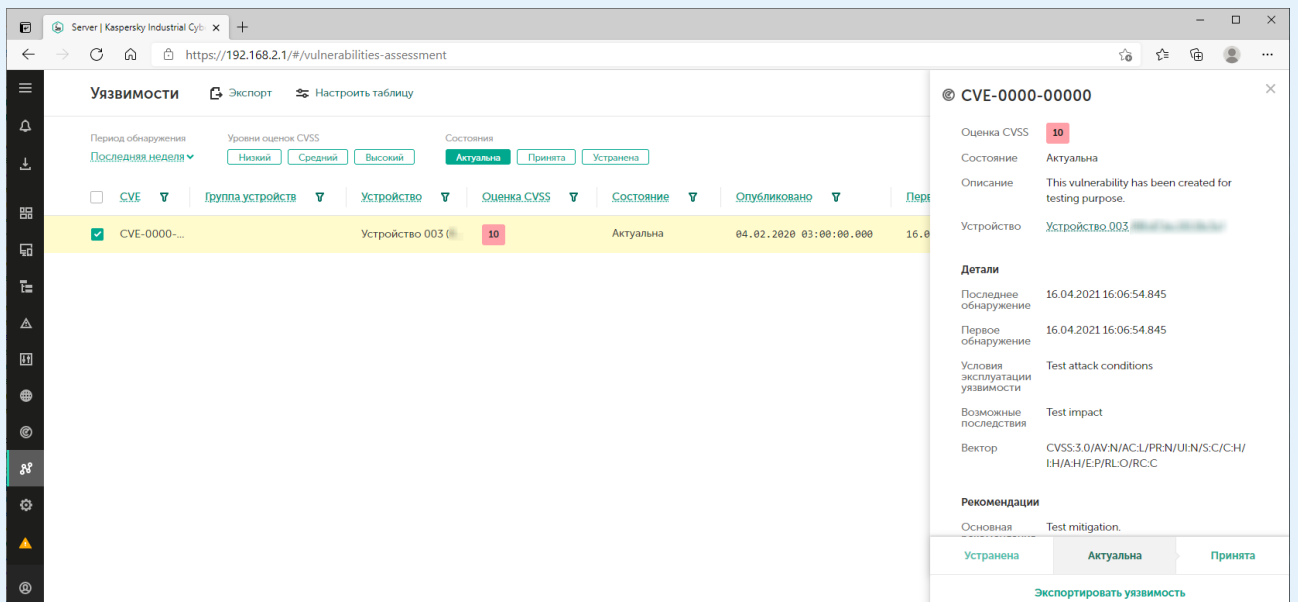



Рисунок 14. Раздел **Уязвимости**

Раздел **Уязвимости** содержит панель инструментов и таблицу уязвимостей.

При выборе уязвимостей открывается область деталей в правой части раздела. Область деталей содержит сведения о выбранных уязвимостях и инструменты для работы с ними.

-  – открывает раздел **Параметры**

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

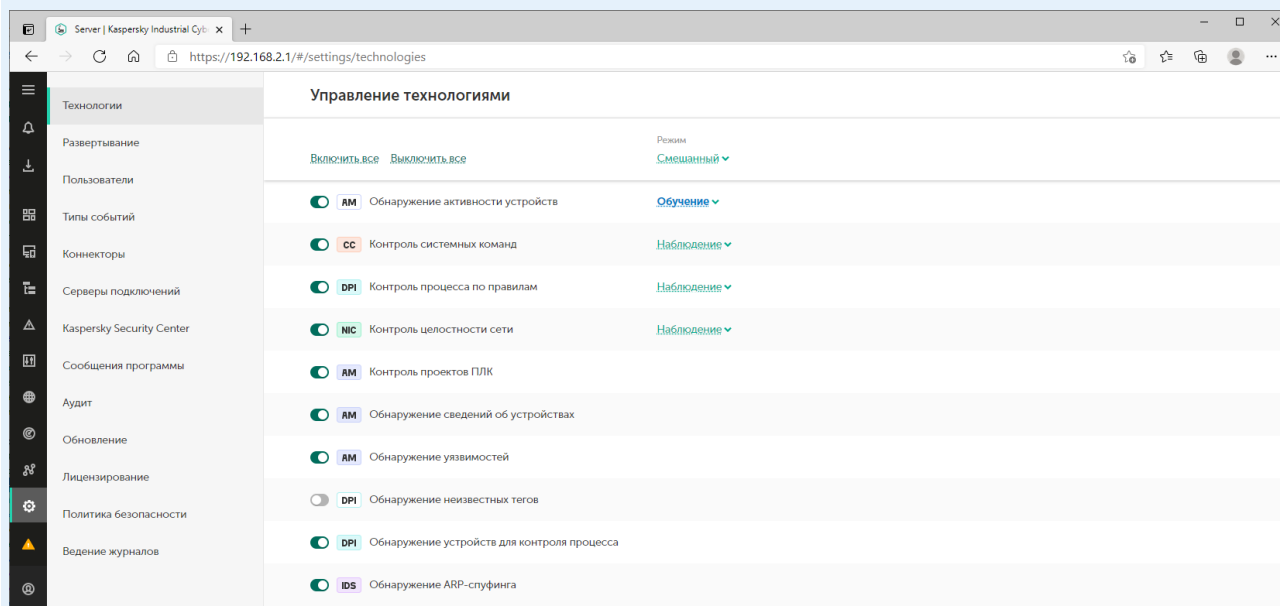


Рисунок 15. Раздел **Параметры**

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

- **Серверы подключений.**
В этом разделе вы можете просматривать и изменять параметры веб-сервера и сервера REST API на компьютере Сервера.
- **Технологии.**
В этом разделе вы можете управлять технологиями и методами для анализа трафика в Kaspersky Industrial CyberSecurity for Networks (см. раздел "Управление технологиями" на стр. 214). Раздел **Технологии** отображается, если подключение к Серверу выполнено под учетной записью Администратора.
- **Развертывание.**
В этом разделе вы можете просматривать сведения об узлах с установленными компонентами программы и о точках мониторинга на узлах. Если подключение к Серверу выполнено под учетной записью Администратора, в этом разделе также доступно управление узлами (см. раздел "Управление узлами с установленными компонентами программы" на стр. 84) и управление точками мониторинга (см. раздел "Управление точками мониторинга на узлах" на стр. 90).

- **Пользователи.**

В этом разделе вы можете управлять учетными записями пользователей программы (см. раздел "Разделение доступа к функциям программы" на стр. [113](#)). Раздел **Пользователи** отображается, если подключение к Серверу выполнено под учетной записью Администратора.

- **Типы событий.**

В этом разделе вы можете просматривать и изменять параметры типов событий (см. раздел "Настройка типов событий" на стр. [225](#)).

- **Коннекторы.**

В этом разделе вы можете управлять коннекторами для программы (см. раздел "Управление коннекторами" на стр. [216](#)).

- **Kaspersky Security Center.**

В этом разделе вы можете просматривать и изменять параметры подключения к Серверу администрирования Kaspersky Security Center (если добавлена функциональность взаимодействия программы с Kaspersky Security Center).

- **Сообщения программы.**

В этом разделе вы можете просматривать сообщения о работе программы (см. раздел "Просмотр сообщений программы" на стр. [96](#)).

- **Аудит.**

В этом разделе вы можете просматривать записи журнала аудита (см. раздел "Просмотр записей аудита действий пользователей" на стр. [100](#)), а также включать и выключать аудит действий пользователей (см. раздел "Включение и выключение аудита действий пользователей" на стр. [213](#)). Раздел **Аудит** отображается, если подключение к Серверу выполнено под учетной записью пользователя с ролью Администратор.

- **Обновление.**

В этом разделе вы можете настроить и запустить обновление баз и модулей программы (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).

- **Лицензирование.**



В этом разделе вы можете управлять лицензионным ключом для обновления баз и модулей программы (см. раздел "Лицензирование программы" на стр. [73](#)).


- **Политика безопасности.**

В этом разделе вы можете управлять политикой безопасности программы (см. раздел "Управление политикой безопасности" на стр. [236](#)).

- **Ведение журналов.**

В этом разделе вы можете настроить уровни ведения журналов работы процессов (см. раздел "Изменение уровней ведения журналов работы процессов" на стр. [213](#)).

-  – 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.
- **Сервер подключения** – отображает имя Сервера, к которому выполнено подключение (имя, заданное при начальной настройке программы после установки (см. раздел "Начальная настройка программы после установки Сервера" на стр. [52](#))).

-  – 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. Этот компонент использует язык локализации, заданный при установке или переустановке Kaspersky Industrial CyberSecurity for Networks (см. раздел "Установка и удаление программы" на стр. 28). Вследствие этого язык локализации данных, которые предоставляет Сервер, может отличаться от выбранного языка локализации веб-интерфейса. Например, события и сообщения, которые поступают от Сервера (в том числе некоторые сообщения об ошибках), выводятся на языке локализации Сервера.

- **Тема оформления** – позволяет выбрать тему цветового оформления страницы веб-интерфейса:
 - **Светлая** – элементы отображаются на белом фоне.
 - **Темная** – элементы отображаются на темном фоне.
- **Учетная запись** – группирует пункты меню для выполнения действий с учетной записью текущего пользователя:
 - **Изменить пароль** – открывает окно для изменения пароля текущего пользователя.
 - **Выход** – завершает сеанс подключения к Серверу и открывает страницу ввода учетных данных для подключения.
- **Дополнительная информация** – содержит пункт **Справка** для перехода на страницу онлайн-справки Kaspersky Industrial CyberSecurity for Networks.

Веб-интерфейс сенсора Kaspersky Industrial CyberSecurity for Networks

При подключении к сенсору Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс (см. раздел "Подключение к сенсору через веб-интерфейс" на стр. 56) в браузере открывается страница веб-интерфейса сенсора. Содержание страницы веб-интерфейса зависит от состояния подключения сенсора к Серверу программы.

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

- До подключения сенсора к Серверу – элементы управления для выбора файла свертки и / или данные для автоматического подключения сенсора по сети (см. раздел "Добавление и подключение сенсора с использованием веб-интерфейса сенсора" на стр. 85).
- После подключения сенсора к Серверу – данные о Сервере и сенсоре (с возможностью перехода на страницу веб-интерфейса Сервера) и состояние соединения.

Лицензирование программы

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

В этом разделе

О Лицензионном соглашении	73
О Политике конфиденциальности	74
О лицензии	74
О лицензионном сертификате	75
О лицензионном ключе для активации функциональности обновления	75
О файле лицензионного ключа для активации функциональности обновления	75
Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс	76
Просмотр информации о добавленном лицензионном ключе	76
Удаление лицензионного ключа	77

О Лицензионном соглашении

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

Внимательно ознакомьтесь и примите условия Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- при начальной настройке программы (см. раздел "Начальная настройка программы после установки Сервера" на стр. [52](#));
- открыв документ license_ru.txt, входящий в комплект поставки программы (копия этого документа также сохраняется в директории установки программы).

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

О Политике конфиденциальности

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

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

Вы можете ознакомиться с условиями Политики конфиденциальности следующими способами:

- при начальной настройке программы (см. раздел "Начальная настройка программы после установки Сервера" на стр. [52](#));
- открыв документ `privacy_policy_ru.txt`, входящий в комплект поставки программы (копия этого документа также сохраняется в директории установки программы).

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

О лицензии

Лицензия – это право на использование программы, предоставляемое вам на основании Лицензионного соглашения. Вы можете использовать функциональность программы при условии приобретения Лицензионного сертификата (см. раздел "О лицензионном сертификате" на стр. [75](#)).

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 (см. раздел "О лицензионном ключе для активации функциональности обновления" на стр. [75](#)). 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 при подключении к Серверу через веб-интерфейс (см. раздел "Просмотр информации о добавленном лицензионном ключе" на стр. [76](#)).

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 при подключении к Серверу через веб-интерфейс

Вы можете добавить лицензионный ключ (см. раздел "О лицензионном ключе для активации функциональности обновления" на стр. [75](#)) в Kaspersky Industrial CyberSecurity for Networks при подключении к Серверу через веб-интерфейс или с использованием функциональности автоматического распространения лицензионных ключей в Kaspersky Security Center (см. раздел "Добавление лицензионного ключа в Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center" на стр. [355](#)).

Добавлять лицензионный ключ могут только пользователи с ролью Администратор.

► *Чтобы добавить лицензионный ключ, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Лицензирование**.
3. Нажмите на кнопку **Добавить лицензионный ключ**. Кнопка отсутствует, если лицензионный ключ уже был добавлен в программу.
Откроется стандартное окно используемого браузера для выбора файла лицензионного ключа.
4. Укажите путь к файлу лицензионного ключа с расширением key.
5. Нажмите на кнопку открытия файла.

Лицензионный ключ из выбранного файла будет загружен в программу.

Просмотр информации о добавленном лицензионном ключе

При подключении к Серверу через веб-интерфейс вы можете просматривать информацию о добавленном лицензионном ключе. Информация о лицензионном ключе отображается в разделе **Параметры** → **Лицензирование**. Дополнительно в списке уведомлений о проблемах в работе программы (см. раздел "Контроль состояния программы при подключении через веб-интерфейс" на стр. [95](#)) могут отображаться предупреждения о статусе лицензионного ключа.

► *Чтобы просмотреть информацию о лицензионном ключе,*

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

Для добавленного лицензионного ключа отображается следующая информация:

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

Удаление лицензионного ключа

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

Удалять лицензионный ключ могут только пользователи с ролью Администратор.

► *Чтобы удалить добавленный лицензионный ключ, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Лицензирование**.
3. Нажмите на кнопку **Удалить**.
Откроется окно с запросом подтверждения.
4. Подтвердите удаление лицензионного ключа.
Лицензионный ключ будет удален из программы.

Предоставление данных

Принимая условия Лицензионного соглашения (см. раздел "О Лицензионном соглашении" на стр. [73](#)) и Политики конфиденциальности (см. раздел "О Политике конфиденциальности" на стр. [74](#)), 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 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 подключаются к программе через коннекторы;
- адреса электронной почты получателей, указанные в коннекторах электронной почты;
- 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 (см. раздел "О журналах" на стр. [82](#)).

Если администратор программы настроил отправку данных программы в сторонние системы (см. раздел "Об отправке событий, сообщений программы и записей аудита в сторонние системы" на стр. [217](#)), то обработка и хранение полученных данных в сторонней системе выполняется в соответствии с ее функциональностью и назначением.

Если с помощью скрипта централизованной установки программы созданы файлы для предоставления информации в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Получение информации для технической поддержки" на стр. [371](#)), в этих файлах сохраняются следующие данные:

- Содержимое директорий для хранения данных программы (см. раздел "Директории для хранения данных программы" на стр. [80](#)):
 - файлы журналов работы процессов, относящихся к компонентам программы, к СУБД и к системе обнаружения вторжений;
 - файлы рабочих данных Сервера и сенсоров;
 - файл параметров установки, созданный скриптом централизованной установки программы;
 - журнал аудита и журнал сообщений программы.
- Политика безопасности, примененная на Сервере.

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

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

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

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

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

Директории для хранения данных программы

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

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);
 - `/etc/opt/kaspersky/kics4net-webserver/` – для хранения файлов с паролями к внешним системам и конфигурационных файлов.
- Директории системы полнотекстового поиска:
 - `/opt/kaspersky/kics4net-webserver/` – директория установки системы полнотекстового поиска;
 - `/var/opt/kaspersky/kics4net-webserver/` – для хранения рабочих данных системы полнотекстового поиска (конфигурация системы полнотекстового поиска и другие сведения);

- `/var/log/kaspersky/kics4net-fts/` – для хранения журналов работы процессов, относящихся к системе полнотекстового поиска;
- `/etc/opt/kaspersky/kics4net-fts/` – для хранения файлов с паролями к внешним системам и конфигурационных файлов.
- Директории с файлами для централизованной установки компонентов программы:
 - `/home/<user>/.config/kaspersky/kics4net-deploy/` – для хранения журналов работы процессов установки и файла параметров установки (если централизованная установка компонентов программы выполнялась с этого компьютера);
 - `/var/opt/kaspersky/kics4net-deploy/` – для хранения копии файла параметров установки, созданного при централизованной установке программы.
- 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 веб-сервера:
 - `/opt/kaspersky/kics4net-websensor/` – директория установки веб-сервера;
 - `/var/opt/kaspersky/kics4net-websensor/` – для хранения рабочих данных веб-сервера (файлы сертификатов и другие сведения);

- `/var/log/kaspersky/kics4net-websensor/` – для хранения журналов работы процессов веб-сервера (также веб-сервер сохраняет данные о работе процессов в системном журнале операционной системы).
- `/etc/opt/kaspersky/kics4net-websensor/` – для хранения файлов с паролями к внешним системам и конфигурационных файлов.
- Директории с файлами для централизованной установки компонентов программы:
 - `/home/<user>/.config/kaspersky/kics4net-deploy/` – для хранения журналов работы процессов установки и файла параметров установки (если централизованная установка компонентов программы выполнялась с этого компьютера);
 - `/var/opt/kaspersky/kics4net-deploy/` – для хранения копии файла параметров установки, созданного при централизованной установке программы.
- 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.

О журналах

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

Журналы, сохраняемые в базе данных Сервера

Программа размещает в базе данных Сервера следующие журналы:

- журнал событий и инцидентов (см. раздел "Мониторинг событий и инцидентов" на стр. [305](#));
- журнал аудита (см. раздел "Просмотр записей аудита действий пользователей" на стр. [100](#));
- журнал сообщений программы (см. раздел "Просмотр сообщений программы" на стр. [96](#)).

Вы можете просматривать содержимое перечисленных журналов при подключении к Серверу через веб-интерфейс (см. раздел "Подключение к Серверу через веб-интерфейс" на стр. [54](#)).

При необходимости вы также можете настроить передачу данных из этих журналов в сторонние системы через коннекторы (см. раздел "Об отправке событий, сообщений программы и записей аудита в сторонние системы" на стр. [217](#)).

Журналы, сохраняемые в файлах

Информация о работе процессов программы сохраняется в виде файлов в локальных директориях (см. раздел "Директории для хранения данных программы" на стр. [80](#)). 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 (см. раздел "Изменение уровней ведения журналов работы процессов" на стр. [213](#)).

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

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

Администрирование Kaspersky Industrial CyberSecurity for Networks

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

В этом разделе

Управление узлами с установленными компонентами программы	84
Управление точками мониторинга на узлах	90
Контроль состояния Kaspersky Industrial CyberSecurity for Networks	95
Обновление баз и программных модулей	110
Разделение доступа к функциям программы	113
Настройка контроля активов	120
Настройка контроля процесса	152
Настройка контроля взаимодействий	185
Настройка обнаружения вторжений	202
Управление журналами	211
Управление технологиями	214
Управление коннекторами	216
Настройка типов событий	225
Управление политикой безопасности	236

Управление узлами с установленными компонентами программы

Этот раздел содержит информацию об управлении узлами, на которых установлены компоненты Kaspersky Industrial CyberSecurity for Networks: Сервер или сенсор. При управлении узлами вы можете добавлять и удалять сенсоры, а также изменять различные параметры узлов.

Управлять узлами с установленными компонентами программы могут только пользователи с ролью Администратор.

Для контроля состояния Kaspersky Industrial CyberSecurity for Networks вы можете просматривать сведения об узлах и сетевых интерфейсах на узлах (см. раздел "Просмотр сведений об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах" на стр. [104](#)).

В этом разделе

Добавление и подключение сенсора с использованием веб-интерфейса сенсора	85
Изменение имени узла с установленным компонентом программы.....	88
Изменение параметров хранения данных программы на узле	88
Создание нового файла свертки для сенсора	89
Удаление сенсора.....	89

Добавление и подключение сенсора с использованием веб-интерфейса сенсора

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

Для добавления сенсора на компьютере, который будет выполнять функции сенсора, должны быть установлены соответствующие пакеты из комплекта поставки программы. Вы можете установить эти пакеты с помощью скрипта централизованной установки компонентов программы (см. раздел "Использование скрипта централизованной установки компонентов программы" на стр. [37](#)) или скрипта локальной установки (см. раздел "Использование скрипта локальной установки компонентов программы" на стр. [48](#)).

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

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

Добавление и подключение сенсора с помощью файла свертки

► Чтобы добавить и подключить сенсор с помощью файла свертки, выполните следующие действия:

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

В правой части окна веб-интерфейса появится область деталей.

4. На закладке **С помощью файла** выполните следующие действия:
 - a. Введите имя сенсора, под которым сенсор будет представлен в составе решения Kaspersky Industrial CyberSecurity for Networks.

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

- b. Введите IP-адрес Сервера, который будет использовать сенсор для подключения к Серверу.
- c. Введите IP-адрес, используемый веб-сервером на компьютере сенсора.
- d. Введите пароль, с помощью которого будет зашифрован сертификат в файле свертки.

Пароль должен удовлетворять следующим требованиям:

- содержит от 12 до 256 символов ASCII;
- содержит одну или несколько прописных букв латинского алфавита;
- содержит одну или несколько строчных букв латинского алфавита;
- содержит одну или несколько цифр;
- содержит не более трех одинаковых символов подряд.

5. Нажмите на кнопку **Создать файл свертки**.

Браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

6. Подключитесь к сенсору (см. раздел "Подключение к сенсору через веб-интерфейс" на стр. [56](#)) через веб-интерфейс.
7. На странице веб-интерфейса сенсора нажмите на кнопку **Выберите файл**.
Откроется стандартное окно используемого браузера для выбора файла.
8. Укажите путь к файлу свертки.
9. Нажмите на кнопку открытия файла.
10. После загрузки содержимого файла введите пароль для доступа к сертификату сенсора в файле свертки.

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

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

Добавление и подключение сенсора автоматически по сети^{v+}

► Чтобы добавить и подключить сенсор автоматически по сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Нажмите на кнопку **Добавить сенсор**.
В правой части окна веб-интерфейса появится область деталей.
4. На закладке **Автоматически по сети** выполните следующие действия:
 - a. Введите имя сенсора, под которым сенсор будет представлен в составе решения Kaspersky Industrial CyberSecurity for Networks.
Имя сенсора должно быть уникальным (не совпадать с именами других сенсоров и Сервера) и может содержать не более 100 символов. Вы можете использовать буквы латинского алфавита, цифры, пробел, а также специальные символы `_` и `-` (например, `Sensor_1`). Имя сенсора должно начинаться и заканчиваться любым допустимым символом, кроме пробела.
 - b. Введите IP-адрес Сервера, который будет использовать сенсор для подключения к Серверу.
 - c. Введите IP-адрес, используемый веб-сервером на компьютере сенсора.
5. Нажмите на кнопку **Соединиться и добавить сенсор**.
Программа установит соединение с компьютером сенсора, после чего на странице веб-интерфейса Сервера появится запрос для подтверждения полученного отпечатка запроса на подпись сертификата.
6. Подключитесь к сенсору (см. раздел "Подключение к сенсору через веб-интерфейс" на стр. [56](#)) через веб-интерфейс.
На странице веб-интерфейса сенсора отобразится сообщение, содержащее информацию об отпечатке запроса сертификата, который был отправлен на Сервер.
7. Убедитесь в идентичности последовательностей символов, представляющих отпечаток запроса сертификата на страницах веб-интерфейса сенсора и Сервера.
8. На странице веб-интерфейса Сервера нажмите на кнопку подтверждения полученного отпечатка запроса сертификата.

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

Изменение имени узла с установленным компонентом программы

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

► *Чтобы изменить имя узла, выполните следующие действия:*

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

В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.
5. В поле с текущим именем узла введите новое имя.

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

6. Нажмите на кнопку **Сохранить**.

См. также

Изменение параметров хранения данных программы на узле[88](#)

Изменение параметров хранения данных программы на узле

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

► *Чтобы изменить ограничения максимального объема, выполните следующие действия:*

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

В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.
5. В блоке **Параметры хранения** задайте ограничения максимального объема для данных программы. Набор типов данных, доступных для настройки, зависит от типа узла (Сервер или сенсор).

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

Для некоторых типов данных (например, для событий) вы можете задать ограничение времени хранения в днях.

6. Нажмите на кнопку **Сохранить**.

См. также

Управление параметрами хранения журналов в базе данных Сервера[211](#)

Управление параметрами сохранения трафика в базе данных Сервера[212](#)

Создание нового файла свертки для сенсора

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

► *Чтобы создать новый файл свертки для сенсора, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку узла того сенсора, для которого вы хотите создать новый файл свертки.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Получить новый файл свертки**.
Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.
Сервер сформирует новый файл свертки для выбранного сенсора, после чего браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.
6. На компьютере сенсора переведите сенсор в начальное состояние с помощью скрипта для локального перевода узла в начальное состояние `kics4net-reset-to-defaults.sh`. Скрипт находится на компьютере с установленным компонентом программы в директории `/opt/kaspersky/kics4net/sbin/`.
7. Подключитесь к сенсору (см. раздел "Подключение к сенсору через веб-интерфейс" на стр. [56](#)) через веб-интерфейс.
8. На странице веб-интерфейса сенсора загрузите новый файл свертки.
Загрузка нового файла свертки выполняется аналогично, как при добавлении сенсора с помощью файла свертки (см. раздел "Добавление и подключение сенсора с использованием веб-интерфейса сенсора" на стр. [85](#)).

Удаление сенсора

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

После удаления сенсора на этом узле остаются файлы компонента сенсора. В дальнейшем вы можете заново добавить этот узел в качестве сенсора (см. раздел "Добавление и подключение сенсора с использованием веб-интерфейса сенсора" на стр. [85](#)) без необходимости установки соответствующих пакетов. Причем добавление сенсора возможно как к текущему Серверу, так и к любому другому Серверу Kaspersky Industrial CyberSecurity for Networks, с которым есть соединение.

► *Чтобы удалить сенсор, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку узла того сенсора, который вы хотите удалить.

В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Удалить**.

Откроется окно с запросом подтверждения.

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

Управление точками мониторинга на узлах

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

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

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

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 в разделе **Параметры** → **Развертывание** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

В этом разделе

Добавление точки мониторинга.....	91
Включение точек мониторинга	91
Выключение точек мониторинга	92
Переименование точки мониторинга	93
Удаление точки мониторинга.....	93
Определение Ethernet-порта, связанного с сетевым интерфейсом	94

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Откройте область деталей по ссылке **Добавить точку мониторинга** в карточке нужного сетевого интерфейса. Ссылка отображается, если точка мониторинга не добавлена на сетевой интерфейс.

В правой части окна веб-интерфейса появится область деталей.

4. В поле ввода в верхней части области деталей введите имя точки мониторинга.

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

Имя точки мониторинга должно удовлетворять следующим требованиям:

- является уникальным (не присвоено другой точке мониторинга);
- содержит от 1 до 100 символов.

5. Нажмите на значок  справа от поля ввода.

Включение точек мониторинга

Программа не получает и не обрабатывает трафик, поступающий на сетевой интерфейс выключенной (см. раздел "Выключение точек мониторинга" на стр. [92](#)) 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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выполните одно из следующих действий:
 - Если вы хотите включить одну точку мониторинга, нажмите на кнопку **Включить** в карточке сетевого интерфейса с точкой мониторинга. Кнопка доступна, если точка мониторинга выключена.
 - Если вы хотите включить все точки мониторинга на узле, нажмите на кнопку **Включить все** в карточке узла, к которому относятся выключенные точки мониторинга. Кнопка доступна, если на узле есть сетевые интерфейсы с выключенными точками мониторинга.
 - Если вы хотите включить все точки мониторинга на всех узлах, 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-интерфейс под учетной записью Администратора.
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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку сетевого интерфейса с точкой мониторинга, которую вы хотите переименовать.

В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на 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 (см. раздел "Выключение точек мониторинга" на стр. [92](#)), 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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку сетевого интерфейса с точкой мониторинга, которую вы хотите удалить.

В правой части окна веб-интерфейса появится область деталей.

4. В области деталей нажмите на кнопку **Удалить**.

Откроется окно с запросом подтверждения. Если точка мониторинга включена, программа предложит выключить точку мониторинга (см. раздел "Выключение точек мониторинга" на стр. [92](#)).

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Нажмите на кнопку **LED-тест** в карточке сетевого интерфейса.

Если сетевой интерфейс поддерживает LED-индикацию, в карточке сетевого интерфейса начнет мигать значок подключения сетевого кабеля. Одновременно на соответствующем сетевом адаптере компьютера начнет мигать LED-индикатор рядом с Ethernet-портом.

Пока включен режим индикации для одного сетевого интерфейса, вы не можете включить режим индикации для другого сетевого интерфейса на этом же узле.

Контроль состояния Kaspersky Industrial CyberSecurity for Networks

Этот раздел содержит инструкции для контроля состояния программы.


В этом разделе

Контроль состояния программы при подключении через веб-интерфейс	95
Просмотр сообщений программы	96
Просмотр записей аудита действий пользователей	100
Просмотр сведений об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах	104
Просмотр статуса сервисов, обеспечивающих работу компонентов программы.....	107
Перезагрузка компьютера с установленными компонентами программы	108
Синхронизация времени на узлах Kaspersky Industrial CyberSecurity for Networks с источником времени для устройств промышленной сети.....	109
Обновление сертификатов SSL-соединений	109

Контроль состояния программы при подключении через веб-интерфейс

Вы можете просматривать информацию о текущем состоянии программы при подключении к Серверу через веб-интерфейс (см. раздел "Подключение к Серверу через веб-интерфейс" на стр. [54](#)). Для контроля состояния программы предусмотрены соответствующие виджеты в разделе **Мониторинг** (см. раздел "**Мониторинг системы в онлайн-режиме**" на стр. [253](#)).

Информация о выключенных функциях защиты

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

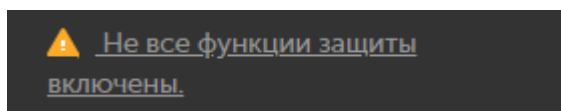



Рисунок 16. Сообщение о выключенных функциях защиты в окне веб-браузера

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).

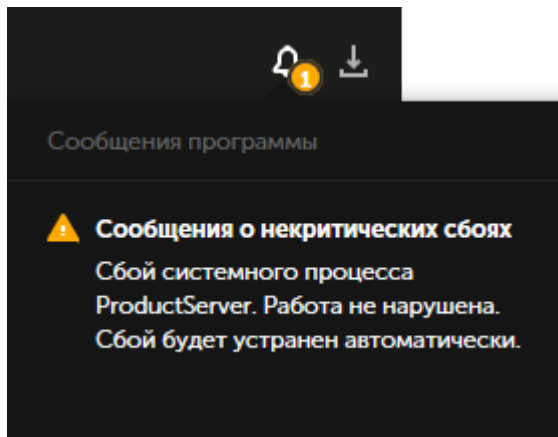



Рисунок 17. Список уведомлений о проблемах в работе программы в окне веб-браузера

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

Просмотр сообщений программы

В журнале сообщений программы сохраняется информация об ошибках в работе программы и операциях, выполненных системными процессами Kaspersky Industrial CyberSecurity for Networks.

Вы можете просматривать сообщения программы при подключении к Серверу через веб-интерфейс. При необходимости вы также можете настроить отправку сообщений программы в сторонние системы через коннекторы (см. раздел "Управление коннекторами" на стр. [216](#)).

► Чтобы просмотреть сообщения программы, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс.
2. Выберите раздел **Параметры** → **Сообщения программы**.

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

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. В разделе **Параметры** → **Сообщения программы** 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. В разделе **Параметры** → **Сообщения программы** 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 отобразятся начальная и конечная дата и время периода фильтрации.
 4. Нажмите на дату начала или окончания периода.
Откроется календарь.
 5. В календаре задайте дату начальной и конечной границ периода фильтрации. Для этого выберите дату в календаре (при этом будет указано текущее время) или введите значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс. Если указывать дату и время конечной границы периода фильтрации не требуется, вы можете не выбирать дату или удалить текущее значение.
 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. В разделе **Параметры** → **Сообщения программы** 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. В разделе **Параметры** → **Сообщения программы** 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,

в разделе **Параметры** → **Сообщения программы** 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,

в разделе **Параметры** → **Сообщения программы** нажмите на кнопку **Фильтр по умолчанию** в панели инструментов (кнопка отображается, если заданы параметры фильтрации и / или поиска).

- Сортировка сообщений программы

► *Чтобы отсортировать сообщения программы, выполните следующие действия:*

1. В разделе **Параметры** → **Сообщения программы** 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 (см. раздел "Включение и выключение аудита действий пользователей" на стр. [213](#)).

Вы можете просматривать записи аудита при подключении к Серверу через веб-интерфейс. При необходимости вы также можете настроить отправку сообщений программы в сторонние системы через коннекторы (см. раздел "Управление коннекторами" на стр. [216](#)).

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **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. В разделе **Параметры** → **Аудит** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
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. В разделе **Параметры** → **Аудит** 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. В разделе **Параметры** → **Аудит** 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 отобразятся начальная и конечная дата и время периода фильтрации.
 4. Нажмите на дату начала или окончания периода.
Откроется календарь.
 5. В календаре задайте дату начальной и конечной границ периода фильтрации. Для этого выберите дату в календаре (при этом будет указано текущее время) или введите значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс. Если указывать дату и время конечной границы периода фильтрации не требуется, вы можете не выбирать дату или удалить текущее значение.
 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**, выполните следующие действия:

1. В разделе **Параметры** → **Аудит** нажмите на значок фильтрации в графе **Действие**.
Откроется окно фильтрации.
2. В поле **Действия** укажите нужное действие из числа предусмотренных действий для аудита. Для этого начните вводить название действия и выберите нужное действие в раскрывшемся списке (список подходящих действий автоматически раскрывается при изменении значения в поле **Действия**).
Вы можете отсортировать открывшийся список действий по ссылке **Сортировка**.
3. Если вы хотите добавить еще одно действие, нажмите на кнопку **Добавить действие** и укажите другое действие в открывшемся поле.
4. Если вы хотите удалить одно из указанных действий, в окне фильтрации нажмите на значок . Вы также можете удалить все указанные действия по ссылке **Фильтр по умолчанию** в окне фильтрации.
5. Нажмите на кнопку **ОК**.

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

1. В разделе **Параметры** → **Аудит** нажмите на значок фильтрации в графе **Результат**.

Для 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. В разделе **Параметры** → **Аудит** 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,

в разделе **Параметры** → **Аудит** 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,

в разделе **Параметры** → **Аудит** нажмите на кнопку **Фильтр по умолчанию** в панели инструментов (кнопка отображается, если заданы параметры фильтрации или поиска).

- Сортировка записей аудита

► Чтобы отсортировать записи аудита, выполните следующие действия:

1. В разделе **Параметры** → **Аудит** 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.

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





В окне веб-интерфейса отобразятся карточки узлов (слева) и карточки сетевых интерфейсов, обнаруженных на этих узлах (справа от каждого узла).

3. Если вы хотите просмотреть подробные сведения об узле или сетевом интерфейсе, выберите карточку нужного узла или сетевого интерфейса.

В правой части окна веб-интерфейса появится область деталей.

Отображаемые сведения об узлах с установленными компонентами программы

В карточке узла отображаются следующие сведения:

- Заданное имя узла.
- Текущее состояние узла в виде значка и текстового описания. Возможны следующие состояния:
 -  **OK**. Узел доступен и от этого узла не поступали сообщения программы о некритических сбоях или нарушении работы.
 -  **Некритический сбой**. Узел доступен и от этого узла поступили сообщения программы со статусами *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.
- Компонент программы, установленный на узле: **Сервер** или **Сенсор**.



Подробные сведения об узле отображаются в области деталей

Для выбранного узла в области деталей отображаются следующие сведения:

- Заданное имя узла.
- **Состояние** – текущее состояние узла в виде значка и текстового описания (как и в карточке узла).
- **Тип узла** – компонент программы, установленный на узле: **Сервер** или **Сенсор**.
- **Текущий объем данных программы** – пространство на диске, занятое файлами программы. Включает в себя установленные файлы и файлы, созданные в процессе работы программы.
- **Максимально возможный объем данных программы** – пространство на диске, которое могут занять файлы программы. Включает в себя установленные файлы и сумму всех заданных ограничений по объему в правилах хранения данных. Значение не может превышать объем доступного пространства на диске.
- **Занято на диске** – пространство на диске, занятое всеми файлами. Включает в себя файлы программы и файлы операционной системы и других приложений. Объем пространства рассчитывается на диске, который содержит директорию /var/ в файловой системе узла.
- **Свободно на диске** – пространство на диске, не занятое файлами. Объем пространства рассчитывается на диске, который содержит директорию /var/ в файловой системе узла.
- **Доступное пространство на диске** – общий объем пространства на диске, который содержит директорию /var/ в файловой системе узла.
- **Правила хранения** – параметры хранения данных, сохраняемых при работе функций программы.




Отображаемые сведения о сетевых интерфейсах

В карточке сетевого интерфейса отображаются следующие сведения:

- Значок подключения сетевого кабеля к Ethernet-порту сетевого интерфейса. Предусмотрены следующие значки:
 -  – сетевой кабель подключен;
 -  – сетевой кабель отключен.



Значок мигает при включенном режиме индикации Ethernet-порта.

- Имя сетевого интерфейса в операционной системе.
- MAC-адрес.
- IP-адрес. Если на сетевом интерфейсе обнаружено несколько IP-адресов, то в карточке сетевого интерфейса отображается только один из них.
- Скорость поступления входящего трафика на сетевой интерфейс.




- Сведения о точке мониторинга, если она добавлена:
 - Имя точки мониторинга.
 - Текущее состояние точки мониторинга в виде значка и текстового описания. Возможны следующие состояния:
 -  **OK**. Точка мониторинга доступна.
 -  **Переключение**. Происходит переключение режима работы точки мониторинга.
 -  **Ошибка**. Обнаружена ошибка при переключении режима работы точки мониторинга.
 - Текущий режим работы точки мониторинга. Предусмотрены следующие режимы:
 - **Включена**.
 - **Выключена**.

Подробные сведения о сетевом интерфейсе отображаются в области деталей

Для выбранного сетевого интерфейса в области деталей 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:
 -  **OK**. 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-fts` – сервис системы полнотекстового поиска (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-webserver` – сервис веб-сервера (присутствует только на компьютере, который выполняет функции Сервера);
- `kics4net-websensor` – сервис веб-сервера (присутствует только на компьютере, который выполняет функции сенсора).

Пример:

```
sudo service kics4net status
```

Если сервис не активен, вы можете перезагрузить компьютер или перезапустить сервис (см. раздел "Перезагрузка компьютера с установленными компонентами программы" на стр. [108](#)).

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 (см. раздел "Закончилось свободное пространство на жестком диске" на стр. [364](#)).
- Произошла непредвиденная перезагрузка компьютера (см. раздел "Непредвиденная перезагрузка системы" на стр. [367](#)), после которой работа компонентов программы не восстановлена.
- Не активен один из сервисов программы (см. раздел "Просмотр статуса сервисов, обеспечивающих работу компонентов программы" на стр. [107](#)).
- 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-fts restart
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
sudo service kics4net-websensor restart
```

Синхронизация времени на узлах Kaspersky Industrial CyberSecurity for Networks с источником времени для устройств промышленной сети

Для правильного сопоставления времени регистрации событий с моментами, когда события произошли в промышленной сети, в системе необходимо обеспечить синхронизацию времени. Синхронизация времени должна выполняться на узлах с установленными компонентами Kaspersky Industrial CyberSecurity for Networks с общим источником времени, который используют устройства промышленной сети.

Синхронизацию времени рекомендуется настроить с помощью программных средств из состава операционной системы компьютеров, на которых установлены компоненты программы. Для синхронизации времени вы можете использовать стандартные протоколы Network Time Protocol (NTP) и Precision Time Protocol (PTP).

Пример последовательности действий для настройки синхронизации времени см. в Приложении (см. раздел "Настройка синхронизации времени по протоколу NTP" на стр. [381](#)).

Обновление сертификатов SSL-соединений

В Kaspersky Industrial CyberSecurity for Networks могут использоваться следующие сертификаты:

- сертификаты для соединений между узлами Kaspersky Industrial CyberSecurity for Networks;
- сертификаты для подключения к Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс;
- сертификаты для подключения коннекторов.

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.

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, выполните следующие действия:*

1. На компьютере Сервера перейдите в директорию `/opt/kaspersky/kics4net/sbin/` и введите команду запуска скрипта локального обновления сертификатов:

```
sudo bash kics4net-update-certs.sh
```

2. После завершения работы скрипта переведите все сенсоры в начальное состояние с помощью скрипта для локального перевода узла в начальное состояние `kics4net-reset-to-defaults.sh`. Скрипт находится на компьютере с установленным компонентом программы в директории `/opt/kaspersky/kics4net/sbin/`.
3. Заново добавьте и подключите сенсоры (см. раздел "Добавление и подключение сенсора с использованием веб-интерфейса сенсора" на стр. [85](#)).

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;
- база данных известных уязвимостей.

Базы и программные модули обновляются после установки обновлений, выпускаемых "Лабораторией Касперского".

Своевременная установка обновлений обеспечивает максимальную защиту промышленной сети с помощью Kaspersky Industrial CyberSecurity for Networks. Кроме того, обновления могут дополнять и обновлять программные модули, участвующие в обеспечении безопасности программы. Если не выполняется регулярная установка обновлений, с течением времени появляются риски для безопасности программы из-за появления новых угроз. Дополнительно необходимо устанавливать обновления безопасности операционной системы.

Сразу после установки компонентов Kaspersky Industrial CyberSecurity for Networks рекомендуется вручную запустить установку обновлений (см. раздел "Запуск обновления вручную" на стр. [111](#)). Для регулярной установки обновлений вы можете настроить параметры автоматического запуска по расписанию (см. раздел "Настройка автоматического обновления" на стр. [111](#)).

Вы можете использовать следующие источники обновлений:

- серверы обновлений "Лаборатории Касперского";
- Сервер администрирования Kaspersky Security Center.

В качестве источника обновлений вы также можете использовать файлы из локального ресурса, если запуск установки обновлений выполняется вручную.

Вы можете настраивать параметры и запускать установку обновлений при подключении к Серверу через веб-интерфейс.

Обновление баз и программных модулей имеет следующие особенности и ограничения:

- Функциональность обновления доступна после добавления лицензионного ключа (см. раздел "Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс" на стр. [76](#)).
- Для загрузки обновлений с серверов обновлений "Лаборатории Касперского" требуется доступ в интернет. При подключении к серверам обновлений с компьютера, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks, соединение осуществляется по протоколу HTTPS (при этом соединение через прокси-сервер не поддерживается).
- Для загрузки обновлений с Сервера администрирования Kaspersky Security Center в Kaspersky Industrial CyberSecurity for Networks должна быть добавлена функциональность взаимодействия программы с Kaspersky Security Center. Вы можете добавить эту функциональность при установке или переустановке (см. раздел "Установка и удаление программы" на стр. [28](#)) Kaspersky Industrial CyberSecurity for Networks. Загрузка обновлений выполняется из хранилища Сервера администрирования, которое заполняется при использовании соответствующей задачи (см. раздел "Использование Сервера администрирования Kaspersky Security Center в качестве источника обновлений" на стр. [356](#)) в Kaspersky Security Center.

В этом разделе

Запуск обновления вручную	111
Настройка автоматического обновления.....	111
Просмотр сведений об установке обновлений	112

Запуск обновления вручную

Вы можете запустить обновление в любой момент. Возможность запуска обновления доступна после добавления лицензионного ключа (см. раздел "Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс" на стр. [76](#)).

Запускать обновление вручную могут только пользователи с ролью Администратор.

► *Чтобы запустить обновление вручную, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Обновление**.
3. В блоке параметров **Источник для обновления вручную** выберите один из следующих вариантов использования источников обновлений:
 - Локальный источник обновлений – позволяет загрузить обновления из файлов по указанному локальному пути. Вы можете указать локальный путь к файлам с помощью кнопки **Обзор**.
 - **Серверы обновлений "Лаборатории Касперского"** – для загрузки обновлений с серверов обновлений "Лаборатории Касперского".
 - **Сервер администрирования Kaspersky Security Center** – для загрузки обновлений с Сервера администрирования Kaspersky Security Center (этот вариант доступен, если добавлена функциональность взаимодействия программы с Kaspersky Security Center).
4. Нажмите на кнопку **Обновить сейчас**.

Настройка автоматического обновления

После добавления лицензионного ключа (см. раздел «Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс» на стр. [76](#)) вы можете настроить автоматическое обновление по расписанию.

Настраивать автоматическое обновление по расписанию могут только пользователи с ролью Администратор.

► *Чтобы включить и настроить автоматическое обновление по расписанию, выполните следующие действия:*

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

3. С помощью переключателя **Обновление по расписанию** включите автоматическое обновление.
4. В блоке параметров **Источник для обновления по расписанию** выберите один из следующих вариантов использования источников обновлений:
 - **Серверы обновлений "Лаборатории Касперского"** – для загрузки обновлений с серверов обновлений "Лаборатории Касперского".
 - **Сервер администрирования Kaspersky Security Center** – для загрузки обновлений с Сервера администрирования Kaspersky Security Center (этот вариант доступен, если добавлена функциональность взаимодействия программы с Kaspersky Security Center).
5. Задайте параметры расписания для запуска обновления. Для этого выполните следующие действия:
 - a. В раскрывающемся списке **Периодичность** укажите, когда будет происходить обновление. Выберите один из следующих вариантов: **По часам**, **По дням**, **Каждую неделю**, **Каждый месяц**.
 - b. В зависимости от выбранного варианта задайте значения параметров, которые уточняют время запуска обновления.
6. Нажмите на кнопку **Сохранить параметры**.

Просмотр сведений об установке обновлений

Вы можете просматривать общие и подробные сведения об установке обновлений.

Общие сведения об установленных обновлениях

Общие сведения содержат информацию о датах и времени выпуска установленных обновлений баз и программных модулей.

► *Чтобы просмотреть общие сведения об установленных обновлениях,*

на странице веб-интерфейса программы выберите раздел **О программе**.

Подробные сведения об установке обновлений

Подробные сведения содержат информацию о запусках процессов установки обновлений. Программа сохраняет следующие подробные сведения:

- дата и время запуска процесса обновления;
- режим запуска обновления (см. раздел "Настройка автоматического обновления" на стр. [111](#));
- 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 (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).

Подробные сведения об установке обновлений сохраняются в журнале сообщений программы (см. раздел "Просмотр сообщений программы" на стр. [96](#)).

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 к Серверу 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 начальной настройке Kaspersky Industrial CyberSecurity for Networks (см. раздел «Начальная настройка программы после установки Сервера» на стр. [52](#)). После этого вы можете добавлять дополнительные учетные записи пользователей программы.

В зависимости от того, к какому компоненту выполнено подключение через веб-интерфейс, пользователю доступны следующие наборы функций:

- функции программы при подключении к Серверу (см. раздел "Функции программы, доступные при подключении к Серверу через веб-интерфейс" на стр. [114](#));
- функции программы при подключении к сенсору (см. раздел "Веб-интерфейс сенсора Kaspersky Industrial CyberSecurity for Networks" на стр. [72](#)).

При подключении к Серверу программа предоставляет доступ к функциям в зависимости от роли пользователя, который выполнил подключение.

В этом разделе

Об учетных записях пользователей программы	114
Функции программы, доступные при подключении к Серверу через веб-интерфейс.....	114
Просмотр сведений об учетных записях пользователей программы.....	118
Создание учетной записи пользователя программы	118
Изменение роли учетной записи пользователя программы.....	119
Удаление учетной записи пользователя программы	119
Изменение пароля учетной записи	120

См. также

Установка и удаление программы	28
--------------------------------------	--------------------

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.

Первой учетной записи пользователя, созданной при начальной настройке программы (см. раздел "Начальная настройка программы после установки Сервера" на стр. [52](#)), назначается роль Администратор.

При добавлении следующих учетных записей вы можете назначать им нужные роли. 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 в разделе **Параметры** → **Пользователи** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Функции программы, доступные при подключении к Серверу через веб-интерфейс

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

Доступные функции программы в зависимости от роли пользователя

Функция программы	Администратор	Оператор
Контроль состояния программы при подключении через веб-интерфейс (на стр. 95)	✓	✓
Просмотр сообщений программы (на стр. 96)	✓	✓
Включение и выключение аудита действий пользователей (на стр. 213)	✓	
Просмотр записей аудита действий пользователей (на стр. 100)	✓	
Просмотр сведений об узлах с установленными компонентами программы и о сетевых интерфейсах на узлах (на стр. 104)	✓	✓
Добавление и подключение сенсора с использованием веб-интерфейса сенсора (на стр. 85)	✓	

Функция программы	Администратор	Оператор
Изменение имени узла с установленным компонентом программы (на стр. 88)	✓	
Изменение параметров хранения данных программы на узле (на стр. 88)	✓	
Создание нового файла свертки для сенсора (на стр. 89)	✓	
Удаление сенсора (на стр. 89)	✓	
Добавление точки мониторинга (на стр. 91)	✓	
Включение точек мониторинга (на стр. 91)	✓	
Выключение точек мониторинга (на стр. 92)	✓	
Переименование точки мониторинга (на стр. 93)	✓	
Удаление точки мониторинга (на стр. 93)	✓	
Определение Ethernet-порта, связанного с сетевым интерфейсом (на стр. 94)	✓	
Просмотр информации о добавленном лицензионном ключе (на стр. 76)	✓	✓
Добавление лицензионного ключа (см. раздел "Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс" на стр. 76)	✓	
Удаление лицензионного ключа (на стр. 77)	✓	
Настройка автоматического обновления (на стр. 111)	✓	
Запуск обновления вручную (на стр. 111)	✓	
Просмотр сведений об установке обновлений (на стр. 112)	✓	✓
Просмотр сведений об учетных записях пользователей программы (на стр. 118)	✓	
Создание учетной записи пользователя программы (на стр. 118)	✓	
Изменение роли учетной записи пользователя программы (на стр. 119)	✓	
Удаление учетной записи пользователя программы (на стр. 119)	✓	
Изменение пароля своей учетной записи для подключения через веб-интерфейс (см. раздел "Изменение пароля учетной записи" на стр. 120)	✓	✓
Просмотр таблицы устройств (на стр. 265)	✓	✓
Просмотр подсетей для контроля активов (на стр. 270)	✓	✓
Экспорт устройств в файл (на стр. 279)	✓	✓
Экспорт подсетей в файл (на стр. 281)	✓	✓
Просмотр сведений об устройстве (на стр. 275)	✓	✓

Функция программы	Администратор	Оператор
Формирование дерева групп устройств (см. раздел "Формирование дерева групп устройств вручную" на стр. 141)	✓	
Добавление устройств вручную (на стр. 124)	✓	
Объединение устройств (на стр. 127)	✓	
Удаление устройств (на стр. 129)	✓	
Изменение статусов устройств (см. раздел "Изменение статусов устройств вручную" на стр. 130)	✓	
Формирование списка подсетей для контроля активов (на стр. 133)	✓	
Автоматическая группировка устройств по заданному критерию (на стр. 135)	✓	
Распределение устройств по группам вручную (на стр. 137)	✓	
Установка и удаление меток для устройств (на стр. 144)	✓	
Изменение сведений об устройстве (на стр. 150)	✓	
Добавление, изменение и удаление пользовательских полей для устройства (на стр. 151)	✓	
Просмотр событий, связанных с устройствами (на стр. 279)	✓	✓
Настройка контроля процесса (на стр. 152)	✓	
Просмотр сведений об устройствах, связанных с тегами (на стр. 350)	✓	✓
Просмотр правил контроля процесса, связанных с тегами (на стр. 169)	✓	✓
Просмотр сведений об устройствах, связанных с правилами контроля процесса (на стр. 184)	✓	✓
Мониторинг значений параметров технологического процесса (на стр. 344)	✓	✓
Просмотр таблицы правил контроля взаимодействий (см. раздел "Просмотр правил контроля взаимодействий в таблице разрешающих правил" на стр. 190)	✓	✓
Создание правил контроля взаимодействий вручную (на стр. 197)	✓	
Изменение параметров правила контроля взаимодействий (на стр. 201)	✓	
Включение и выключение правил контроля взаимодействий (на стр. 201)	✓	
Удаление правил контроля взаимодействий (на стр. 202)	✓	
Просмотр таблицы с наборами правил обнаружения вторжений (на стр. 207)	✓	✓

Функция программы	Администратор	Оператор
Включение и выключение наборов правил обнаружения вторжений (на стр. 209)	✓	
Загрузка и замена пользовательских наборов правил обнаружения вторжений (на стр. 209)	✓	
Удаление пользовательских наборов правил обнаружения вторжений (на стр. 210)	✓	
Управление параметрами хранения записей журналов в базе данных (см. раздел "Управление параметрами хранения журналов в базе данных Сервера" на стр. 211)	✓	
Управление параметрами сохранения трафика в базе данных (см. раздел "Управление параметрами сохранения трафика в базе данных Сервера" на стр. 212)	✓	
Изменение уровней ведения журналов работы процессов (на стр. 213)	✓	
Управление технологиями (на стр. 214)	✓	
Управление коннекторами (на стр. 216)	✓	
Настройка типов событий (на стр. 225)	✓	
Экспорт политики безопасности в файл (на стр. 237)	✓	✓
Импорт политики безопасности из файла (на стр. 238)	✓	
Очистка текущей политики безопасности (на стр. 239)	✓	
Мониторинг системы в онлайн-режиме (на стр. 253)	✓	✓
Работа с картой сети (на стр. 282)	✓	✓
Перемещение узлов и групп в другие группы на карте сети (на стр. 141)	✓	
Мониторинг событий и инцидентов (на стр. 305)	✓	✓
Контроль уязвимостей устройств (на стр. 331)	✓	✓

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Пользователи**.
3. Добавьте новую карточку пользователя. Для этого нажмите на карточку со знаком +.

Появится новая карточка пользователя, внутри которой отобразятся поля для ввода учетных данных и выбора роли учетной записи нового пользователя.

4. В поле для ввода имени пользователя введите имя пользователя, учетную запись которого вы хотите создать.

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

Имя учетной записи пользователя должно удовлетворять следующим требованиям:

- является уникальным в списке имен пользователей программы (регистр символов не учитывается);
 - содержит 3–20 символов;
 - начинается с буквы;
 - заканчивается любым поддерживаемым символом, кроме точки.
5. В полях для ввода пароля введите пароль, который вы хотите задать для учетной записи пользователя.

Пароль должен удовлетворять следующим требованиям:

- содержит от 12 до 256 символов ASCII;
- содержит одну или несколько прописных букв латинского алфавита;
- содержит одну или несколько строчных букв латинского алфавита;

- содержит одну или несколько цифр;
 - содержит не более трех одинаковых символов подряд.
6. В раскрывающемся списке выберите нужную роль пользователя: **Администратор** или **Оператор**.
 7. Нажмите на кнопку **Сохранить**.

В карточке пользователя отобразится значок с именем учетной записи пользователя и назначенная ему роль.

Изменение роли учетной записи пользователя программы

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Пользователи**.
3. Нажмите на кнопку **Изменить** в карточке пользователя, роль которого вы хотите изменить.
Карточка пользователя перейдет в режим редактирования параметров учетной записи.
4. В раскрывающемся списке выберите нужную роль учетной записи пользователя: **Администратор** или **Оператор**.
5. Нажмите на кнопку **Сохранить**.

В карточке пользователя отобразится значок с именем пользователя и назначенная роль для его учетной записи.

Удаление учетной записи пользователя программы

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Пользователи**.
3. Нажмите на кнопку **Удалить** в карточке пользователя, которого вы хотите удалить.
Откроется окно с запросом подтверждения.
4. В окне запроса нажмите на кнопку **ОК**.

Изменение пароля учетной записи


После 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. На странице веб-интерфейса Kaspersky Industrial CyberSecurity for Networks откройте меню пользователя:

- Если меню свернуто, нажмите на кнопку .
- Если меню развернуто, нажмите на кнопку справа от имени текущего пользователя.

2. В меню пользователя выберите пункт **Изменить пароль**.

Появится окно **Изменение пароля**.

3. В поле **Текущий пароль** введите ваш текущий пароль.

4. В полях **Новый пароль** и **Новый пароль (повторно)** введите новый пароль.

Новый пароль должен удовлетворять условиям, перечисленным в окне **Изменение пароля**. В процессе ввода пароля автоматически отмечаются выполненные условия.

5. Нажмите на кнопку **Изменить**. Кнопка доступна после ввода текущего и нового паролей и выполнения всех требований к новому паролю.

Новый пароль потребуется при следующем подключении к Серверу через веб-интерфейс.

Настройка контроля активов

Kaspersky Industrial CyberSecurity for Networks позволяет контролировать активы предприятия, представленные устройствами промышленной сети. Устройства идентифицируются программой по MAC- и / или IP-адресам в сетевых взаимодействиях. При этом IP-адреса устройств проверяются на принадлежность известным программам подсетям, которые также используются при контроле активов. Для контроля активов в программе формируются таблица устройств (на стр. [262](#)) и таблица подсетей (см. раздел «Просмотр подсетей для контроля активов» на стр. [270](#)).

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 активов (см. раздел «Методы и режимы контроля активов» на стр. [121](#)). 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 (см. раздел «Дерево групп устройств» на стр. [277](#)) или выполнять фильтрацию и поиск по меткам устройств (см. раздел «Установка и удаление меток для устройств» на стр. [144](#)).

Вы можете настраивать контроль активов и изменять сведения об устройствах на странице веб-интерфейса Сервера (см. раздел "О веб-интерфейсе Сервера в основном режиме работы программы" на стр. [64](#)) в разделе **Активы**. Также вы можете просматривать информацию о взаимодействиях устройств и выполнять различные действия с устройствами при работе с картой сети (см. раздел "Работа с картой сети" на стр. [282](#)). Для удобного представления информации о взаимодействиях устройств и для обеспечения автоматической группировки устройств по подсетям вы можете сформировать список подсетей (см. раздел "Формирование списка подсетей для контроля активов" на стр. [133](#)) и указать в программе структуру подсетей в сети вашего предприятия.

В этом разделе

Методы и режимы контроля активов	121
Выбор применяемых методов и изменение режима контроля активов	123
Добавление устройств вручную	124
Объединение устройств	127
Удаление устройств.....	129
Изменение статусов устройств вручную.....	130
Формирование списка подсетей для контроля активов	133
Просмотр сведений об устройствах с IP-адресами из выбранных подсетей	134
О распределении устройств по группам.....	134
Автоматическая группировка устройств по заданному критерию	135
Распределение устройств по группам вручную	137
Перемещение узлов и групп в другие группы на карте сети	141
Формирование дерева групп устройств вручную.....	141
Установка и удаление меток для устройств	144
Изменение сведений об устройстве	150
Добавление, изменение и удаление пользовательских полей для устройства	151

Методы и режимы контроля активов

При контроле активов в Kaspersky Industrial CyberSecurity for Networks применяются следующие методы:

- Обнаружение активности устройств. Этот метод позволяет отслеживать активность устройств в трафике промышленной сети по полученным MAC- и / или IP-адресам устройств.
- Обнаружение сведений об устройствах. Этот метод позволяет автоматически получать и обновлять сведения об устройствах 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.
- Обнаружение уязвимостей. Этот метод позволяет обнаруживать уязвимости в устройствах по сохраненным сведениям об устройствах.

Вы можете включать и выключать применение методов контроля активов по отдельности.

Для методов контроля активов предусмотрены следующие режимы:

- Режим обучения. Этот режим предназначен для временного использования. В этом режиме программа считает разрешенными все устройства, активность которых обнаружена в трафике. Вы можете включить режим обучения только для метода обнаружения активности устройств. При этом метод обнаружения активности устройств может применяться совместно с другими методами контроля активов.
- Режим наблюдения. Этот режим предназначен для постоянного использования. В этом режиме при обнаружении активности устройств программа считает разрешенными только те из них, которым присвоен статус *Разрешенное*.

В зависимости от выбранного режима программа автоматически присваивает статусы устройствам (см. раздел "Автоматическое изменение статусов устройств" на стр. [276](#)).

В режиме обучения программа не регистрирует события при обнаружении активности устройств или при автоматическом обновлении сведений об устройствах.

Режим обучения контроля активов должен быть включен на время, достаточное для обнаружения активности нужных устройств. Это время зависит от количества устройств в промышленной сети, периодичности их работы и обслуживания. Рекомендуется включать режим обучения на время не менее одного часа. В крупных промышленных сетях, для обнаружения активности всех нужных устройств, режим обучения можно включить на период от одного до нескольких дней.

Обработка полученных MAC- и IP-адресов устройств выполняется со следующими особенностями:

- Для устройств, которые выполняют функции сетевого коммутатора между сегментами промышленной сети, должен быть выставлен признак маршрутизирующего устройства (см. раздел "Просмотр сведений об устройстве" на стр. [275](#)). Если этот признак не определен автоматически, то его требуется выставить вручную. Иначе до выставления признака маршрутизирующего устройства программа может не добавить в таблицу устройств те устройства, которые взаимодействуют через это маршрутизирующее устройство в разных сегментах промышленной сети. После выставления признака взаимодействующие устройства будут добавлены в таблицу устройств при появлении соответствующего трафика с их участием.
- Если в трафике обнаружен только IP-адрес устройства (IP-адрес невозможно сопоставить с каким-либо MAC-адресом), этот IP-адрес проверяется на принадлежность известным программе подсетям (см. раздел "Просмотр подсетей для контроля активов" на стр. [270](#)). Для метода обнаружения активности устройств не учитываются IP-адреса, которые принадлежат только подсетям с типом **Публичная**.

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.

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 неверным 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 (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).

В режиме наблюдения программа регистрирует соответствующие события по технологии Контроль активов. В зависимости от применяемых методов, события могут регистрироваться в следующих случаях:

- обнаружение активности неизвестных устройств или устройств со статусом *Неиспользуемое*;
- автоматическое изменение сведений об устройствах;
- обнаружение операций чтения или записи проектов и блоков проектов ПЛК;
- обнаружение уязвимостей и изменений, связанных с уязвимостями.

При включенном методе контроля проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. [277](#)) 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.

Выбор применяемых методов и изменение режима контроля активов

Управлять методами и режимами контроля активов могут только пользователи с ролью Администратор.

► *Чтобы включить или выключить применение методов контроля активов, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Технологии**.
3. Включите или выключите применение методов контроля активов, используя следующие переключатели:
 - **Обнаружение активности устройств.**
 - **Обнаружение сведений об устройствах.**

- **Контроль проектов ПЛК.**
 - **Обнаружение уязвимостей.**
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 активов 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.

См. также

Методы и режимы контроля активов[121](#)

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 устройства 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-интерфейс под учетной записью Администратора.
2. На закладке **Устройства** в разделе **Активы** откройте область деталей по ссылке **Добавить устройство**.
3. На закладке **Адреса** в области деталей укажите уникальные 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.
4. 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).
5. 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 **Автообновление**, расположенные над полями с возможностью автоматического изменения. Для поля **Статус** переключатель автоматического изменения имеет название **Автоизменение на Неиспользуемое** из-за особенностей автоматического изменения статусов устройств (см. раздел "Автоматическое изменение статусов устройств" на стр. [276](#)).
8. На закладке **Пользовательские поля** в области деталей при необходимости сформируйте список пользовательских полей (см. раздел "Добавление, изменение и удаление пользовательских полей для устройства" на стр. [151](#)).
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 (см. раздел "Работа с картой сети" на стр. [282](#)) 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-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** выберите нужный узел, представляющий неизвестное программе устройство.

В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Добавить в таблицу устройств**.

В области деталей появятся закладки для настройки параметров нового устройства.

4. Настройте параметры нового устройства, не изменяя MAC и / или IP-адрес, которые указаны для узла.

Описание действий для настройки параметров см. в процедуре добавления устройства вручную при работе с таблицей устройств.

5. Нажмите на кнопку **Сохранить**.

В таблице устройств появится новое устройство со статусом *Разрешенное*. Узел на карте сети, который ранее представлял неизвестное программе устройство, будет представлять известное программе устройство.

После добавления устройства вы можете добавить (см. раздел "Добавление параметров контроля процесса для устройства вручную" на стр. [158](#)) параметры контроля процесса для устройства.

См. также

Устройства для контроля процесса [155](#)

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 (см. раздел "Методы и режимы контроля активов" на стр. [121](#)). 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 сохраняются 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 устройств некоторые сведения из объединяемых устройств могут не сохраниться в новом устройстве (например, содержимое динамических полей (см. раздел "Просмотр сведений об устройстве" на стр. [275](#))). Кроме того, для объединения устройств требуется, чтобы суммарное количество сетевых интерфейсов в новом устройстве получилось не более 64.

Объединять устройства вручную может только пользователь с ролью Администратор.

Объединять устройства 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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Устройства** выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. [273](#)), 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 (см. раздел "Работа с картой сети" на стр. [282](#)) 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-интерфейс под учетной записью Администратора. \!
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 программ 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.

См. также

Добавление устройств вручную124

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 активов).

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Устройства** выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. [273](#)), 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 (см. раздел "Работа с картой сети" на стр. [282](#)) 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-интерфейс под учетной записью Администратора.
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**.

Изменение статусов устройств вручную

Изменять статусы устройств может только пользователь с ролью Администратор.

Вы можете изменить статус (выбрать один из статусов *Разрешенное*, *Неразрешенное* или *Неиспользуемое*) для одного выбранного устройства или одновременно для нескольких выбранных устройств. Если вы изменяете статус одного выбранного устройства, вы можете включить или выключить автоматическое изменение статуса (см. раздел "Автоматическое изменение статусов устройств" на стр. [276](#)) этого устройства. Если вы изменяете статус нескольких выбранных устройств, вы сможете включить или выключить автоматическое изменение статуса при изменении сведений (см. раздел "Изменение сведений об устройстве" на стр. [150](#)) каждого из этих устройств по отдельности.

После присвоения устройству статуса *Неиспользуемое* программа может автоматически изменить статус этого устройства, если оно проявит активность. В зависимости от текущего режима работы контроля активов (см. раздел "Методы и режимы контроля активов" на стр. [121](#)) 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 одного устройства при работе с таблицей устройств, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. На закладке **Устройства** в разделе **Активы** 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 **Параметры**.
5. В раскрывающемся списке **Статус** выберите нужный статус устройства.
6. Включите или выключите автоматическое изменение статуса. Для этого используйте переключатель **Автоизменение на Неиспользуемое**, расположенный над раскрывающимся списком **Статус**.
Выключение автоматического изменения статуса может потребоваться, например, если вы хотите, чтобы статус *Разрешенное* не изменялся на статус *Неиспользуемое* для редко подключаемого устройства.
7. Нажмите на кнопку **Сохранить**.

► *Чтобы изменить статус нескольких устройств при работе с таблицей, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Устройства**.
3. В таблице устройств выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. [273](#)), статус которых вы хотите изменить.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку с названием нужного статуса.
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 (см. раздел "Работа с картой сети" на стр. [282](#)) 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 одного устройства при работе с картой сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** выберите узел нужного устройства.
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 **Параметры**.
5. В раскрывающемся списке **Статус** выберите нужный статус устройства.
6. Включите или выключите автоматическое изменение статуса. Для этого используйте переключатель **Автоизменение на Неиспользуемое**, расположенный над раскрывающимся списком **Статус**.
Выключение автоматического изменения статуса может потребоваться, например, если вы хотите, чтобы статус *Разрешенное* не изменялся на статус *Неиспользуемое* для редко подключаемого устройства.
7. Нажмите на кнопку **Сохранить**.

► Чтобы изменить статус нескольких устройств при работе с картой сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** выберите объекты, представляющие узлы известных программе устройств и / или свернутые группы.
Для выбора нескольких узлов и / или групп выполните одно из следующих действий:
 - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
 - Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.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 с названием нужного статуса.
Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.

Формирование списка подсетей для контроля активов

Вы можете вручную формировать список известных программе подсетей (см. раздел "Просмотр подсетей для контроля активов" на стр. [270](#)), чтобы программа работала с учетом особенностей адресации устройств в сети вашего предприятия.

Формировать список подсетей могут только пользователи с ролью Администратор.

Для формирования списка подсетей вы можете использовать следующие функции:

- Добавление подсети

► Чтобы добавить подсеть, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Подсети** откройте область деталей по ссылке **Добавить подсеть**.
4. В поле **Подсеть** введите адрес подсети в формате CIDR: <базовый адрес подсети>/<количество бит в маске>.
5. В раскрывающемся списке **Тип** выберите тип подсети в соответствии с ее назначением.
6. При необходимости включите или выключите режим пропуска обнаруженных MAC-адресов при создании разрешающих правил контроля взаимодействий. Для этого установите в нужное положение переключатель **Игнорировать MAC-адреса для правил NIC**.

Если режим включен, то MAC-адреса, обнаруженные вместе с IP-адресами из подсети, не будут добавляться в правила по технологии Контроль целостности сети в режиме обучения.
7. Нажмите на кнопку **Сохранить**.

В списке подсетей появится новая подсеть на соответствующем уровне иерархии в дереве.

- Изменение параметров подсети

► Чтобы изменить параметры подсети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Подсети** выберите нужную подсеть.

В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Измените доступные параметры подсети.

При изменении типа подсети учитывайте, что новый тип подсети может повлиять на выполняемые программой действия с IP-адресами из этой подсети. Например, при выборе типа **Публичная** на карте сети перестанут отображаться соединения с устройствами, у которых заданы IP-адреса из этой подсети.

6. Нажмите на кнопку **Сохранить**.

Если изменен параметр **Подсеть**, для подсети может измениться уровень иерархии в дереве.

- Удаление подсетей

Вы можете удалить любую подсеть, кроме корневой подсети в дереве (подсеть 0.0.0.0/0).

► *Чтобы удалить подсети, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Подсети** выберите подсети, которые вы хотите удалить.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить**.
Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление подсетей.

Удаленные подсети перестанут отображаться в списке подсетей. Если удаленная подсеть содержала вложенные подсети, эти подсети останутся в списке (при этом изменится уровень иерархии этих подсетей в дереве).

Просмотр сведений об устройствах с IP-адресами из выбранных подсетей

Вы можете просмотреть сведения об устройствах, у которых заданы IP-адреса из выбранных подсетей. Сведения об устройствах выводятся в таблице устройств. В таблице устройств автоматически применяется фильтрация по адресам подсетей.

► *Чтобы просмотреть сведения об устройствах в таблице устройств, выполните следующие действия:*

1. Выберите раздел **Активы**.
2. На закладке **Подсети** выберите подсети, для которых вы хотите просмотреть сведения об устройствах.
В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Показать устройства**.

Откроется закладка **Устройства** в разделе **Активы**. В таблице устройств будет применена фильтрация по IP-адресам в адресной информации устройств.

О распределении устройств по группам

Вы можете распределять устройства по группам, используя дерево групп устройств (на стр. [277](#)). Дерево групп устройств поддерживает до шести уровней вложенности.

Устройства могут быть помещены в группы любого уровня иерархии. При этом каждое устройство может быть добавлено только в одну из групп дерева.

Для дерева действует ограничение по количеству групп – не более 1000.

До включения устройства в какую-либо группу сведения об этом устройстве не содержат информацию о размещении устройства. Такое устройство относится к верхнему уровню иерархии в дереве групп. После включения устройства в группу в программе сохраняется размещение этого устройства в виде полного пути к группе в дереве групп.

Для распределения устройств по группам предусмотрены следующие способы:

- Автоматическая группировка устройств по заданному критерию (на стр. [135](#)).

При такой группировке устройств программа может автоматически добавлять группы в дерево групп устройств. Группы добавляются при обнаружении устройств, в которых есть сведения, соответствующие выбранному критерию группировки. Имена для групп задаются из диапазона значений выбранного критерия (например, из названий категорий устройств при группировке по категориям).

- Распределение устройств по группам вручную (на стр. [137](#)).

Вы можете вручную распределять устройства по группам, включая устройства в нужные группы и исключая из групп. При необходимости вы можете вносить изменения в дерево групп устройств, используя функции формирования дерева групп устройств вручную (см. раздел "Формирование дерева групп устройств вручную" на стр. [141](#)).




Автоматическая группировка устройств по заданному критерию

Вы можете автоматически группировать устройства в дереве групп устройств (см. раздел "Дерево групп устройств" на стр. [277](#)) по одному из следующих критериев:

- принадлежность IP-адресов известным программам подсетям;
- категории устройств;
- производители устройств.

Выполнять автоматическую группировку устройств могут только пользователи с ролью Администратор.

► *Чтобы автоматически сгруппировать устройства по заданному критерию, начиная с верхнего уровня иерархии в дереве групп, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** нажмите на одну из следующих кнопок выбора критерия группировки в панели инструментов, которая расположена в левой части области отображения карты сети:
 -  – для группировки устройств по подсетям;
 -  – для группировки устройств по категориям;
 -  – для группировки устройств по производителям.

Откроется окно запроса для выбора варианта группировки.

3. В окне запроса нажмите на одну из следующих кнопок в зависимости от нужного результата:
 - Если вы хотите сгруппировать устройства по выбранному критерию во всех группах дерева групп устройств, нажмите на кнопку **Вместе с дочерними**.
 - Если вы хотите сгруппировать устройства по выбранному критерию только на верхнем уровне иерархии дерева групп устройств, нажмите на кнопку **Только выбранную группу**.

Программа определит устройства, подходящие под выбранный критерий группировки, создаст группы для этих устройств и поместит устройства в эти группы.

► Чтобы автоматически сгруппировать устройства в выбранной группе устройств, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** выберите группу, в которой вы хотите автоматически сгруппировать устройства.
3. По правой клавише мыши откройте контекстное меню.
4. В контекстном меню выберите один из следующих пунктов:
 - **Сгруппировать по подсетям.**
 - **Сгруппировать по категориям.**
 - **Сгруппировать по производителям.**

Откроется окно запроса для выбора варианта группировки.

5. В окне запроса нажмите на одну из следующих кнопок в зависимости от нужного результата:
 - Если вы хотите сгруппировать устройства по выбранному критерию во всех дочерних группах выбранной группы, нажмите на кнопку **Вместе с дочерними.**
 - Если вы хотите сгруппировать устройства по выбранному критерию только в выбранной группе, нажмите на кнопку **Только выбранную группу.**

Программа определит устройства, подходящие под выбранный критерий группировки, создаст группы для этих устройств и поместит устройства в эти группы (при этом устройства в других группах не будут распределены по новым группам).

См. также

О распределении устройств по группам.....[134](#)

Распределение устройств по группам вручную

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-интерфейс под учетной записью Администратора.
2. Выберите устройство в разделе **Активы** на закладке **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 (см. раздел "Формирование дерева групп устройств вручную" на стр. [141](#)) 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 (см. раздел "Работа с картой сети" на стр. [282](#)) 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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Устройства** выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. [273](#)), 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 (см. раздел "Формирование дерева групп устройств вручную" на стр. [141](#)) 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-интерфейс под учетной записью Администратора.
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 (см. раздел "Формирование дерева групп устройств вручную" на стр. [141](#)) 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-интерфейс под учетной записью Администратора.
2. Выберите устройство в разделе **Активы** на закладке **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 (см. раздел "Работа с картой сети" на стр. [282](#)) 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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Устройства** выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. 273), 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-интерфейс под учетной записью Администратора.
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.

См. также

- О распределении устройств по группам.....134
- Перемещение узлов и групп в другие группы на карте сети141

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 (см. раздел "Распределение устройств по группам вручную" на стр. [137](#)).

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-интерфейс под учетной записью Администратора.
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.

Формирование дерева групп устройств вручную

Вы можете формировать дерево групп устройств (на стр. [277](#)) при работе с таблицей устройств или с картой сети. Функции для формирования дерева доступны в окне **Формирование дерева групп** или **Выбор группы в дереве**.

Формировать дерево групп устройств могут только пользователи с ролью Администратор.

► *Чтобы использовать функции для формирования дерева групп устройств, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Активы** на закладке **Устройства** или в разделе **Карта сети** выполните одно из следующих действий:
 - Откройте окно **Формирование дерева групп** по ссылке **Настроить группы**.
 - Откройте окно **Выбор группы в дереве**, выполняя добавление устройств в группы (см. раздел "Распределение устройств по группам вручную" на стр. [137](#)). Вы также можете открыть это окно при фильтрации таблицы устройств (см. раздел "Просмотр таблицы устройств" на стр. [265](#)) по графе **Группа**.

Изменения, сделанные в дереве групп устройств в окне **Формирование дерева групп** или **Выбор группы в дереве**, применяются сразу.

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** добавьте новую группу одним из следующих способов:
 - Если дерево пустое и вы хотите добавить первую группу, нажмите на кнопку **Добавить** или на любую из клавиш **INSERT** или **ENTER**.
 - Если вы хотите добавить группу на одном уровне иерархии с имеющейся группой, выберите эту группу и нажмите на клавишу **ENTER**.
 - Если вы хотите добавить дочернюю группу к имеющейся группе, выберите эту группу и нажмите на кнопку **Добавить** или на клавишу **INSERT**.
2. В поле ввода введите имя группы.

Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: ! @ # № \$ % ^ & () [] { } ' , . - _.

Имя группы должно удовлетворять следующим требованиям:

 - начинается и заканчивается любым символом, кроме пробела;
 - содержит до 255 символов;
 - не совпадает с именем другой группы из числа включенных в ту же родительскую группу (регистр символов не учитывается).
3. Нажмите на значок  справа от поля ввода.


- Переименование группы

► *Чтобы переименовать группу в дереве групп устройств, 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 групп

При удалении группы не удаляются устройства, добавленные в эту группу. Устройства из удаленной группы переводятся на тот же уровень иерархии в дереве устройств, на котором была удаленная группа.

► *Чтобы удалить группу в дереве групп устройств, 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 запроса для выбора варианта удаления.

3. В окне запроса нажмите на одну из следующих кнопок в зависимости от нужного результата:

- Если вы хотите удалить только выбранную группу и оставить ее дочерние группы, нажмите на кнопку **Только выбранную**.
- Если вы хотите удалить выбранную группу вместе со всеми ее дочерними группами, нажмите на кнопку **Вместе с дочерними**.

- 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



[См. также](#)

О распределении устройств по группам [134](#)

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-интерфейс под учетной записью Администратора.
2. Выберите устройство в разделе **Активы** на закладке **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 (см. раздел "Работа с картой сети" на стр. [282](#)) 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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Устройства** выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. 273), для которых вы хотите установить метки.
4. По правой клавише мыши откройте контекстное меню одного из выбранных устройств.
5. В контекстном меню выберите пункт **Установить метки**.

Появится окно **Добавление меток**.

6. В поле **Метки** введите текстовые описания, которые вы хотите использовать в качестве меток. Для разделения меток вы можете использовать клавишу **ENTER** или символ **;**.

Вы можете использовать прописные и строчные буквы, цифры, пробел, а также следующие специальные символы: ! @ # № \$ % ^ & () [] { } ' , . - _ .

Имя метки должно удовлетворять следующим требованиям:

- начинается и заканчивается любым символом, кроме пробела;
 - является уникальным в списке меток устройства (регистр символов не учитывается);
 - содержит от 1 до 255 символов.
7. При необходимости скопируйте список меток по ссылке **Копировать метки**. Ссылка отображается, если список меток не пустой.
 8. Если вы хотите очистить текущие списки меток для выбранных устройств и указать для этих устройств только новые метки, установите флажок **Удалить существующие**.

Если снят флажок **Удалить существующие**, на каждом устройстве останется его текущий список меток. Списки меток на всех выбранных устройствах дополнятся новыми метками. В этом случае для некоторых из выбранных устройств суммарное количество меток может превысить ограничение (до 16 меток для каждого устройства). Программа проверяет это ограничение перед добавлением новых меток.

9. Нажмите на кнопку **ОК**.

Кнопка недоступна, если имена введенных меток не удовлетворяют требованиям или если список меток пустой и при этом снят флажок **Удалить существующие**.

► Чтобы установить метки для нескольких устройств при работе с картой сети, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
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 одного из выбранных объектов.
5. В контекстном меню выберите пункт **Установить метки**.

Появится окно **Добавление меток**.

6. В поле **Метки** введите текстовые описания, которые вы хотите использовать в качестве меток. Для разделения меток вы можете использовать клавишу **ENTER** или символ ; .

Вы можете использовать прописные и строчные буквы, цифры, пробел, а также следующие специальные символы: ! @ # № \$ % ^ & () [] { } ' , . - _ .

Имя метки должно удовлетворять следующим требованиям:

- начинается и заканчивается любым символом, кроме пробела;
- является уникальным в списке меток устройства (регистр символов не учитывается);
- содержит от 1 до 255 символов.

7. При необходимости скопируйте список меток по ссылке **Копировать метки**. Ссылка отображается, если список меток не пустой.
8. Если вы хотите очистить текущие списки меток для выбранных устройств и указать для этих устройств только новые метки, установите флажок **Удалить существующие**.

Если снят флажок **Удалить существующие**, на каждом устройстве останется его текущий список меток. Списки меток на всех выбранных устройствах дополняются новыми метками. В этом случае для некоторых из выбранных устройств суммарное количество меток может превысить ограничение (до 16 меток для каждого устройства). Программа проверяет это ограничение перед добавлением новых меток.

9. Нажмите на кнопку **ОК**.

Кнопка недоступна, если имена введенных меток не удовлетворяют требованиям или если список меток пустой и при этом снят флажок **Удалить существующие**.

- Удаление меток для одного устройства

► *Чтобы очистить список меток устройства, выполните следующие действия:*


1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите устройство в разделе **Активы** на закладке **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 меток для нескольких устройств при работе с таблицей устройств.

Также при работе с картой сети (см. раздел "Работа с картой сети" на стр. [282](#)) 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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. На закладке **Устройства** выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. [273](#)), для которых вы хотите очистить списки меток.
4. По правой клавише мыши откройте контекстное меню одного из выбранных устройств.
5. В контекстном меню выберите пункт **Установить метки**.
Появится окно **Добавление меток**.
6. Установите флажок **Удалить существующие**.
7. Нажмите на кнопку **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-интерфейс под учетной записью Администратора.
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 одного из выбранных объектов.
5. В контекстном меню выберите пункт **Установить метки**.
Появится окно **Добавление меток**.
6. Установите флажок **Удалить существующие**.
7. Нажмите на кнопку **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-интерфейс под учетной записью Администратора.
2. На закладке **Устройства** в разделе **Активы** 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.
7. На закладках **Адреса** и **Параметры** в области деталей включите или выключите автоматическое изменение для нужных сведений об устройстве. Для этого используйте переключатели **Автообновление**, расположенные над полями с возможностью автоматического изменения. Для поля статус переключатель автоматического изменения имеет название **Автоизменение на Неиспользуемое** из-за особенностей автоматического изменения статусов устройств (см. раздел "Автоматическое изменение статусов устройств" на стр. [276](#)).
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 .

После сохранения изменений в сведениях об устройстве вы можете добавить (см. раздел "Добавление параметров контроля процесса для устройства вручную" на стр. [158](#)) или изменить (см. раздел "Изменение параметров контроля процесса для устройства" на стр. [159](#)) параметры контроля процесса для устройства.

См. также

Изменение статусов устройств вручную.....	130
Распределение устройств по группам вручную	137
Установка и удаление меток для устройств.....	144
Добавление, изменение и удаление пользовательских полей для устройства	151
Устройства для контроля процесса	155

Добавление, изменение и удаление пользовательских полей для устройства

Вы можете добавлять, изменять и удалять пользовательские поля (см. раздел «Просмотр сведений об устройстве» на стр. [275](#)) 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-интерфейс под учетной записью Администратора.
2. На закладке **Устройства** в разделе **Активы** 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**.

Настройка контроля процесса

Kaspersky Industrial CyberSecurity for Networks может контролировать технологический процесс, отслеживая параметры технологического процесса и системные команды, передаваемые в трафике промышленной сети. Программа отслеживает эти данные для устройств, представленных в таблице устройств (см. раздел "Таблица устройств" на стр. [262](#)) и имеющих заданные параметры контроля процесса (см. раздел "Параметры контроля процесса для устройств" на стр. [156](#)).

Параметры контроля процесса можно настроить для типов устройств и протоколов, поддерживаемых программой (см. раздел "Поддерживаемые устройства и протоколы" на стр. [153](#)).

Для контроля технологического процесса в автоматическом режиме вы можете использовать правила контроля процесса и функциональность отслеживания системных команд. Также вы можете отслеживать параметры технологического процесса в онлайн-режиме (см. раздел "Мониторинг значений параметров технологического процесса" на стр. [344](#)).

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

При выполнении условия, заданного в правиле, Kaspersky Industrial CyberSecurity for Networks регистрирует событие. Вы можете задать нужные параметры регистрации событий (например, заголовки событий) при настройке правил контроля процесса (см. раздел "Правила контроля процесса" на стр. [170](#)).

Отслеживание системных команд обеспечивает регистрацию событий обнаружения в трафике переданных системных команд. При настройке параметров контроля процесса для устройств вы можете выбрать нужные системные команды для отслеживания (см. раздел "Выбор отслеживаемых системных команд" на стр. [160](#)). Эта функциональность может использоваться независимо от правил контроля процесса.

Настраивать параметры контроля процесса для устройств, а также формировать списки контролируемых тегов и правил контроля процесса могут только пользователи с ролью Администратор. При этом возможности просмотра и экспорта данных доступны как пользователям с ролью Администратор, так и пользователям с ролью Оператор.

Вы можете формировать списки контролируемых тегов и правил контроля процесса на странице веб-интерфейса Сервера (см. раздел "О веб-интерфейсе Сервера в основном режиме работы программы" на стр. [64](#)) в разделе **Контроль процесса**. Параметры контроля процесса для устройств вы можете настраивать при работе с устройствами в разделах **Активы** и **Карта сети**.

В этом разделе

Поддерживаемые устройства и протоколы.....	153
Устройства для контроля процесса	155
Теги	163
Правила контроля процесса	170

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™;
 - AutomationDirect DirectLOGIC;
 - BECKHOFF® серий CX;
 - Emerson DeltaV серий MD, MD Plus, MQ;
 - Emerson серии ControlWave;
 - General Electric RX3i;
 - Honeywell C300 для систем управления Experion PKS / PlantCruise;
 - Honeywell ControlEDGE серии 900;
 - 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;
 - Прософт-Системы Regul R500;
 - устройства, поддерживающие протокол Allen-Bradley EtherNet/IP;
 - устройства, поддерживающие протоколы CODESYS V3;
 - устройства, поддерживающие протоколы Siemens S7comm™, S7comm-plus;
 - устройства, поддерживающие протоколы стандарта PROFINET IO.
- Интеллектуальные электронные устройства (далее IED):
 - ABB серии Relion™: REF615, RED670, REL670, RET670;
 - General Electric серии Multilin: B30, C60;
 - MiCOM C264;
 - Schneider Electric P545;
 - Schneider Electric Sepam серии 80 NPP;
 - Siemens серии SIPROTEC™ 4: 6MD66, 7SA52, 7SJ64, 7SS52, 7UM62, 7UT63;
 - Релематика TOP 300;
 - ЭКРА серий 200, БЭ2502, БЭ2704;
 - устройства, поддерживающие протокол DNP3;

- устройства, поддерживающие протокол Schneider Electric UMAS;
- устройства, поддерживающие протоколы стандарта IEC 60870: IEC 60870-5-101, IEC 60870-5-104;
- устройства, поддерживающие протоколы стандарта IEC 61850: IEC 61850-8-1 (GOOSE, MMS), IEC 61850-9-2 (Sampled Values);
- устройства, поддерживающие протокол Modbus TCP.
- Устройства с установленным серверным ПО:
 - FTP-сервер;
 - сервер OPC DA;
 - сервер OPC UA;
 - сервер TASE.2;
 - сервер с поддержкой шифрования.
- Устройства, относящиеся к сетевому оборудованию:
 - Моха серии NPort;
 - устройства ввода-вывода, поддерживающие протоколы BACnet™, FTP, IEC 60870-5-101, IEC 60870-5-104, Modbus TCP, OPC DA, протокол взаимодействия устройств по технологии WMI, OPC UA Binary.

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

- ABB SPA-Bus;
- Allen-Bradley EtherNet/IP;
- BACnet;
- BECKHOFF ADS/AMS;
- CODESYS V3 Gateway поверх TCP и CODESYS V3 Gateway поверх UDP;
- 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 DA, протокол взаимодействия устройств по технологии WMI;
- OPC UA Binary;

- PROFINET IO и RPC для PROFINET IO;
- Schneider Electric UMAS;
- Siemens Industrial Ethernet;
- Siemens S7comm, S7comm-plus;
- TASE.2;
- Yokogawa Vnet/IP;
- Релематика BDUBus;
- модификация протокола Modbus TCP для устройств ЭКРА серии 200;
- протокол взаимодействия устройств Foxboro FCP270, FCP280;
- протоколы начальной настройки и взаимодействия устройств Мохэ серии NPort;
- протокол взаимодействия устройств AutomationDirect DirectLOGIC;
- протокол взаимодействия устройств MiCOM C264;
- 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.

Для анализа трафика и взаимодействий устройств в программе используются модули обработки протоколов прикладного уровня. После установки программы используются исходные модули, обеспечивающие поддержку перечисленных типов устройств и протоколов прикладного уровня.

Вы можете обновлять модули обработки протоколов, устанавливая обновления (см. раздел «Обновление баз и программных модулей» на стр. [110](#)). При установке обновлений в программу могут быть добавлены новые модули, обеспечивающие поддержку дополнительных типов устройств и / или протоколов прикладного уровня.

Устройства для контроля процесса

Для контроля технологического процесса вы можете использовать устройства из таблицы устройств (см. раздел "Таблица устройств" на стр. [262](#)), у которых заданы параметры контроля процесса.

В Kaspersky Industrial CyberSecurity for Networks для контроля процесса поддерживаются различные типы устройств и протоколы прикладного уровня (см. раздел "Поддерживаемые устройства и протоколы" на стр. [153](#)).

Вы можете просматривать и изменять параметры контроля процесса в области деталей устройства, выбранного в разделе **Активы** или **Карта сети** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

В этом разделе

Параметры контроля процесса для устройств.....	156
Об автоматическом определении параметров контроля процесса для устройств	157
Включение и выключение автоматического определения параметров контроля процесса для устройств	158
Добавление параметров контроля процесса для устройства вручную	158
Изменение параметров контроля процесса для устройства	159
Выбор отслеживаемых системных команд	160
Очистка параметров контроля процесса, заданных для устройства	161
Импорт конфигураций устройств и тегов из внешних проектов	162

Параметры контроля процесса для устройств

Параметры контроля процесса для устройств отображаются в области деталей при выборе устройства в таблице устройств (см. раздел «Таблица устройств» на стр. [262](#)) или на карте сети (см. раздел «Работа с картой сети» на стр. [282](#)). Если для устройства заданы параметры контроля процесса, область деталей содержит отдельный блок со следующими параметрами:

- **Тип устройства** – тип устройства из числа поддерживаемых типов устройств для контроля процесса.
- **Протокол** – название используемого протокола. Для каждого протокола отображаются следующие сведения:
 - **Системные команды** – основные параметры отслеживания системных команд для протокола. В поле отображается общее количество системных команд для протокола и количество отслеживаемых системных команд, при обнаружении которых программа регистрирует события.
 - **Адрес** – в зависимости от выбранного протокола содержит IP-адрес и порт, MAC-адрес или идентификатор домена (для протокола IEC 61850: GOOSE).
 - Дополнительные параметры.

Дополнительные параметры протокола появляются в блоке параметров контроля процесса, если для этого протокола в программе можно настроить не только системные команды и адресную информацию.

При выборе протокола Modbus TCP отображается дополнительный параметр **Обратный порядок регистров**. Параметр позволяет включить или выключить поддержку обратной последовательности регистров (машинных слов) в 32-разрядных значениях данных.

При выборе протокола IEC 60870-5-101 отображаются следующие дополнительные параметры:

- **Адрес ASDU два байта** – позволяет включить или выключить режим двухбайтовой адресации для блоков данных прикладного уровня (Application Service Data Unit, ASDU). Если режим выключен, используется однобайтовая адресация.
- **Инициатор** – позволяет включить или выключить использование дополнительного байта для адреса инициатора в идентификаторе блока данных.
- **Блок адреса канала (байт)** – количество байт в блоке адреса канального уровня.
- **Блок адреса объекта (байт)** – количество байт в блоке адреса объекта информации.

Программа может автоматически определять и добавлять параметры контроля процесса (см. раздел "Об автоматическом определении параметров контроля процесса для устройств" на стр. [157](#)). Также вы можете вручную добавлять (см. раздел "Добавление параметров контроля процесса для устройства вручную" на стр. [158](#)) или изменять (см. раздел "Изменение параметров контроля процесса для устройства" на стр. [159](#)) параметры контроля процесса для устройств.

Об автоматическом определении параметров контроля процесса для устройств

Kaspersky Industrial CyberSecurity for Networks может автоматически определять параметры контроля процесса для устройств (на стр. [156](#)) и сохранять эти параметры в сведениях об устройствах. Определение параметров выполняется путем анализа обнаруженных в трафике протокольных команд для устройств, участвующих в технологическом процессе.

Программа автоматически добавляет или изменяет параметры контроля процесса для устройств, которые добавлены в таблицу устройств (см. раздел "Таблица устройств" на стр. [262](#)). Добавление устройств в таблицу также может происходить автоматически, если для контроля активов включен метод обнаружения активности устройств (см. раздел "Методы и режимы контроля активов" на стр. [121](#)).

Автоматически добавленные параметры контроля процесса считаются *системными*. Программа может изменять эти параметры, если в трафике обнаружены протокольные команды с обновленной информацией о параметрах.

Параметры контроля процесса, добавленные пользователем вручную (см. раздел "Добавление параметров контроля процесса для устройства вручную" на стр. [158](#)), считаются *пользовательскими*. Программа не изменяет пользовательские параметры контроля процесса. Если пользователь вручную изменит (см. раздел "Изменение параметров контроля процесса для устройства" на стр. [159](#)) системные параметры контроля процесса, эти параметры также становятся пользовательскими.

Автоматическое определение параметров контроля процесса для устройств выполняется при работе программы в режиме обнаружения устройств для контроля процесса. Вы можете включать и выключать (см. раздел "Включение и выключение автоматического определения параметров контроля процесса для устройств" на стр. [158](#)) этот режим.

Для автоматического определения параметров контроля процесса в программе используются модули обработки протоколов прикладного уровня. После установки программы используются исходные модули, обеспечивающие определение основных параметров для ряда устройств и протоколов из числа поддерживаемых типов устройств и протоколов (см. раздел "Поддерживаемые устройства и протоколы" на стр. [153](#)). Вы можете обновлять модули обработки протоколов, устанавливая обновления (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).

Включение и выключение автоматического определения параметров контроля процесса для устройств

При включенном автоматическом определении параметров контроля процесса для устройств программа может добавлять и изменять параметры только для тех устройств, которые добавлены в таблицу устройств. Если вы хотите, чтобы при определении параметров выполнялось и автоматическое добавление устройств, вам нужно включить применение метода обнаружения активности устройств (см. раздел "Выбор применяемых методов и изменение режима контроля активов" на стр. [123](#)).

Включать и выключать автоматическое определение параметров контроля процесса для устройств могут только пользователи с ролью Администратор.

► *Чтобы включить или выключить автоматическое определение параметров контроля процесса для устройств, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Технологии**.
3. С помощью переключателя **Обнаружение устройств для контроля процесса** включите или выключите автоматическое определение параметров контроля процесса.
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 параметров контроля процесса для устройства вручную

Вы можете вручную добавить параметры контроля процесса для устройства при работе с таблицей устройств или с картой сети. Добавленные параметры контроля процесса для устройства считаются пользовательскими. Пользовательские параметры не изменяются при автоматическом определении параметров контроля процесса для устройств (см. раздел "Об автоматическом определении параметров контроля процесса для устройств" на стр. [157](#)).

Добавлять параметры контроля процесса могут только пользователи с ролью Администратор.

► *Чтобы добавить параметры контроля процесса для устройства, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Активы** на закладке **Устройства** или в разделе **Карта сети** 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 нажмите на кнопку **Добавить параметры контроля процесса** (кнопка отображается, если параметры контроля процесса не заданы).
Появится окно **Добавление параметров контроля процесса**.

5. Настройте параметры контроля процесса (см. раздел "Параметры контроля процесса для устройств" на стр. [156](#)):
 - a. Выберите тип устройства.
 - b. Выберите протокол, по которому осуществляется взаимодействие с устройством в рамках технологического процесса.
 - c. При необходимости измените параметры отслеживания системных команд (см. раздел "Выбор отслеживаемых системных команд" на стр. [160](#)) по выбранному протоколу. По умолчанию отслеживаются все системные команды, кроме тех, которые часто возникают при нормальной работе устройства.
 - d. Если для выбранного протокола требуется настроить другие параметры (например, адресную информацию для взаимодействия с устройством), укажите нужные значения в появившихся полях.
 - e. Если вы хотите дополнительно указать другой протокол (поддерживаемый для выбранного типа устройства) или другую комбинацию параметров для ранее выбранного протокола (в случае использования нескольких подключаемых модулей в составе одного устройства), добавьте параметры для этого протокола по ссылке **Добавить протокол**.
6. Нажмите на кнопку **Сохранить**.

Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

В нижней части закладки **Адреса** в области деталей появится отдельный блок с заданными параметрами.

Изменение параметров контроля процесса для устройства

Если для устройства добавлены параметры контроля процесса, вы можете вручную изменить эти параметры при работе с таблицей устройств или с картой сети. После сохранения изменений параметры контроля процесса для устройства считаются пользовательскими. Пользовательские параметры не изменяются при автоматическом определении параметров контроля процесса для устройств (см. раздел "Об автоматическом определении параметров контроля процесса для устройств" на стр. [157](#)).

Изменять параметры контроля процесса могут только пользователи с ролью Администратор.

► *Чтобы изменить параметры контроля процесса для устройства, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Активы** на закладке **Устройства** или в разделе **Карта сети** 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 нажмите на значок  в блоке с заданными параметрами контроля процесса (блок отображается, если заданы параметры контроля процесса). Появится окно **Изменение параметров контроля процесса**.

5. Настройте параметры контроля процесса (см. раздел "Параметры контроля процесса для устройств" на стр. [156](#)). Вы можете изменить параметры по отдельности (например, изменить параметры отслеживания системных команд для протокола) или заново настроить все параметры в том же порядке, как при добавлении параметров контроля процесса (см. раздел "Добавление параметров контроля процесса для устройства вручную" на стр. [158](#)).

При изменении параметров, которые используются в ранее созданных тегах, программа автоматически удаляет эти теги и связанные с ними правила контроля процесса. Например, если вы удаляете протокол, то после сохранения параметров программа удалит все теги, в которых были указаны устройство и удаленный протокол (в том числе будут удалены и правила контроля процесса, связанные с этими тегами).

6. Нажмите на кнопку **Сохранить**.

Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

В нижней части закладки **Адреса** в области деталей обновятся сведения в блоке с заданными параметрами.

Выбор отслеживаемых системных команд

Вы можете настроить отслеживание в трафике системных команд, переданных и полученных устройствами для контроля процесса. В Kaspersky Industrial CyberSecurity for Networks к системным командам относятся как команды управления 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 (см. раздел "Системные типы событий по технологии Контроль системных команд" на стр. [415](#)), которому присвоен код 4000002602. Вы можете настроить параметры (см. раздел "Настройка типов событий" на стр. [225](#)) для этого типа события.

Настраивать отслеживание системных команд для устройств могут только пользователи с ролью Администратор.

► *Чтобы настроить отслеживание системных команд для устройства, выполните следующие действия:*

1. В разделе **Активы** на закладке **Устройства** или в разделе **Карта сети** выберите нужное устройство, для которого заданы параметры контроля процесса.

Если параметры контроля процесса не заданы для устройства, добавьте параметры (см. раздел "Добавление параметров контроля процесса для устройства вручную" на стр. [158](#)).

2. На закладке **Адреса** в области деталей нажмите на значок  в блоке с заданными параметрами контроля процесса.

Появится окно **Изменение параметров контроля процесса**.

3. Для первого протокола укажите нужные системные команды. Для этого раскройте список **Системные команды** под полем **Протокол** и установите флажки у тех системных команд, которые вы хотите отслеживать. После выбора системных команд нажмите на кнопку **ОК**.

4. Если в параметрах контроля процесса дополнительно указан другой протокол (или тот же протокол, но с другой адресной информацией), выберите системные команды, которые будут отслеживаться при взаимодействиях по этому протоколу. Для этого используйте раскрывающийся список **Системные команды** под полем с названием этого протокола. Аналогичным образом настройте отслеживание системных команд для всех остальных указанных протоколов устройства.
5. Нажмите на кнопку **Сохранить**.
Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

В нижней части закладки **Адреса** в области деталей обновятся сведения в блоке с заданными параметрами.

Очистка параметров контроля процесса, заданных для устройства

Вы можете очистить параметры контроля процесса, заданные для устройства, при работе с таблицей устройств или с картой сети.

При очистке параметров контроля процесса, заданных для устройства, программа автоматически удаляет все теги, которые были созданы для этого устройства. Также вместе с тегами удаляются и связанные с ними правила контроля процесса.

Выполнять очистку параметров контроля процесса для устройств могут только пользователи с ролью Администратор.

► *Чтобы очистить параметры контроля процесса для устройства, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Активы** на закладке **Устройства** или в разделе **Карта сети** 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 нажмите на значок  в блоке с заданными параметрами контроля процесса (блок отображается, если заданы параметры контроля процесса).
Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление параметров.

В нижней части закладки **Адреса** в области деталей появится кнопка **Добавить параметры контроля процесса**.

Импорт конфигураций устройств и тегов из внешних проектов

Вы можете импортировать в Kaspersky Industrial CyberSecurity for Networks конфигурации параметров контроля процесса для устройств (далее также "конфигурации устройств") и теги из файлов, представляющих внешние проекты. *Внешними проектами* для Kaspersky Industrial CyberSecurity for Networks считаются проекты с данными об устройствах и тегах, сохраненные средствами других систем (например, в системе SCADA).

Для импорта конфигураций устройств и тегов поддерживаются файлы данных, представляющие следующие типы проектов:

- Проект универсального формата.
Этот тип проекта может быть получен из любых источников путем преобразования и сохранения данных в текстовых файлах с разделителями в формате CSV. Сведения о составе файлов в проекте универсального формата см. в Приложении (см. раздел "Файлы для импорта проекта универсального формата" на стр. [396](#)). Для импорта в программу CSV-файлы проекта должны быть упакованы в ZIP-архив.
- Проект DirectSOFT6.
Этот тип проекта может быть получен с помощью программного обеспечения для управления устройствами DirectLOGIC. Если проект содержит несколько файлов, для импорта в программу эти файлы должны быть упакованы в ZIP-архив.

Вы можете обновлять и дополнять поддерживаемые типы проектов, устанавливая обновления (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).


► *Чтобы импортировать конфигурации устройств и тегов из внешнего проекта, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Активы**.
3. По ссылке **Импорт** в панели инструментов на закладке **Устройства** откройте меню для выбора типа импортируемого проекта.
4. В открывшемся меню выберите пункт с нужным типом проекта.
На экране появится окно **Импортируется <тип проекта>**.
5. В поле **Имя проекта** введите локальный путь к проекту. Вы можете указать локальный путь с помощью кнопки **Обзор**.
6. Выберите нужный вариант действий с имеющимися конфигурациями устройств и тегами. Для этого нажмите на одну из следующих кнопок:
 - **Добавить** – импортируемые конфигурации устройств и теги будут добавлены к имеющимся конфигурациям устройств и тегам.
 - **Заменить** – при импорте удаляются имеющиеся конфигурации устройств и теги, связанные с теми устройствами, для которых импортируются новые конфигурации и теги (при этом не удаляются теги, для которых есть пользовательские правила контроля процесса).

7. Подтвердите импорт с помощью кнопки **Продолжить**.

Запустится процесс импорта данных. Сведения о выполнении операции импорта отображаются в списке фоновых операций. По окончании процесса импортированные конфигурации устройств и теги будут доступны для загрузки в таблице устройств (см. раздел "Просмотр таблицы устройств" на стр. [265](#)) и в таблице тегов (см. раздел "Просмотр таблицы тегов" на стр. [346](#)).

8. Если вы хотите просмотреть отчет о результатах импорта, выполните следующие действия:

- a. Нажмите на кнопку  в меню веб-интерфейса программы.
Откроется список фоновых операций.
- b. Дождитесь завершения операции импорта.
- c. Нажмите на кнопку **Показать отчет**.

Теги

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

Вы можете добавлять теги в программу следующими способами:

- вручную (см. раздел "Добавление тега вручную" на стр. [166](#));
- автоматически при обнаружении неизвестных тегов (см. раздел "Об обнаружении неизвестных тегов" на стр. [164](#));
- при импорте из внешних проектов (см. раздел "Импорт конфигураций устройств и тегов из внешних проектов" на стр. [162](#)).

Добавление тега возможно при следующих условиях:

- В таблице устройств (см. раздел "Таблица устройств" на стр. [262](#)) есть устройство, к которому относится добавляемый тег.
- Для устройства заданы параметры контроля процесса (см. раздел "Параметры контроля процесса для устройств" на стр. [156](#)), в которых указан протокол добавляемого тега.

После добавления тега в программу этот тег может быть использован в правилах контроля процесса (см. раздел "Правила контроля процесса" на стр. [170](#)). В соответствии с условиями, заданными в правилах контроля процесса, программа будет регистрировать соответствующие события (см. раздел "Мониторинг событий и инцидентов" на стр. [305](#)), в которых могут сохраняться полученные значения тега.

Для контроля значений тега при мониторинге параметров технологического процесса (см. раздел "Мониторинг значений параметров технологического процесса" на стр. [344](#)) не требуется добавлять этот тег в правила контроля процесса.

Вы можете просматривать и изменять теги на закладке **Теги** в разделе **Контроль процесса** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

В этом разделе

Об обнаружении неизвестных тегов	164
Включение и выключение обнаружения неизвестных тегов	165
Выбор тегов в таблице	165
Добавление тега вручную	166
Изменение параметров тега	167
Добавление тегов в список избранных	168
Удаление тегов	169
Просмотр правил контроля процесса, связанных с тегами	169

Об обнаружении неизвестных тегов

Kaspersky Industrial CyberSecurity for Networks может анализировать трафик для обнаружения и сохранения информации о неизвестных тегах. Неизвестными считаются теги, отсутствующие в таблице тегов.

Программа добавляет обнаруженный тег в таблицу тегов, если выполнены условия для добавления тега (см. раздел "Устройства для контроля процесса" на стр. [155](#)). Если не выполнено одно из условий, обнаруженный тег игнорируется (например, если в параметрах контроля процесса для устройства не указан протокол, к которому относится тег).

Получение из трафика информации о неизвестных тегах выполняется при работе программы в режиме обнаружения неизвестных тегов. Вы можете включать и выключать (см. раздел "Включение и выключение обнаружения неизвестных тегов" на стр. [165](#)) 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 с заданными параметрами контроля процесса. После добавления обнаруженных тегов в таблицу рекомендуется выключить этот режим.

Обнаружение неизвестных тегов поддерживается для следующих протоколов:

- Allen-Bradley EtherNet/IP;
- BACnet;
- CODESYS V3 Gateway;
- DMS для устройств ABB AC 700F;
- DNP3;
- Emerson DeltaV;
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104;
- OPC DA;
- OPC UA Binary;
- TASE.2;
- Yokogawa Vnet/IP;

- протокол взаимодействия устройств Foxboro FCP270, FCP280;
- протокол обмена данными с устройствами Emerson серии ControlWave.

Включение и выключение обнаружения неизвестных тегов

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 программу параметры контроля процесса для всех устройств, теги которых вы хотите обнаружить в трафике.

Вы можете добавлять параметры контроля процесса для устройств следующими способами:

- вручную (см. раздел "Добавление параметров контроля процесса для устройства вручную" на стр. [158](#));
- автоматически при включенном обнаружении устройств для контроля процесса (см. раздел "Об автоматическом определении параметров контроля процесса для устройств" на стр. [157](#));
- при импорте из внешних проектов (см. раздел "Импорт конфигураций устройств и тегов из внешних проектов" на стр. [162](#)).

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **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.

Выбор тегов в таблице

В таблице тегов вы можете выбирать теги для просмотра сведений и для работы с этими тегами. При выборе тегов в правой части окна веб-интерфейса появляется область деталей.

► *Чтобы выбрать нужные теги в таблице, выполните одно из следующих действий:*

- Если вы хотите выбрать один тег, установите флажок напротив этого тега или выберите тег с помощью мыши.
- Если вы хотите выбрать несколько тегов, установите флажки напротив нужных тегов или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**.
- Если вы хотите выбрать все теги, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:
 - выберите любой тег в таблице и нажмите комбинацию клавиш **CTRL+A**;
 - установите флажок в заголовке левой крайней графы таблицы.

При выборе нескольких тегов в области деталей отображается общее количество выбранных тегов. Если вы выбрали все теги, удовлетворяющие текущим параметрам фильтрации и поиска, в области деталей отображается одно из следующих значений:

- Если выбрано до 1000 тегов включительно, отображается точное количество. В этом случае программа проверяет вхождение тегов в список избранных, как и при других способах выбора нескольких тегов.
- Если выбрано более 1000 тегов, отображается 1000+. В этом случае программа не проверяет вхождение тегов в список избранных.

В заголовке левой крайней графы таблицы отображается флажок выбора тегов. В зависимости от количества выбранных тегов флажок может быть в одном из следующих состояний:

- – в таблице не выполнялся выбор всех тегов, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбран один тег или выбраны несколько тегов с помощью флажков напротив тегов или с использованием клавиш **CTRL** или **SHIFT**.
- – в таблице выбраны все теги, удовлетворяющие текущим параметрам фильтрации и поиска.
- – в таблице были выбраны все теги, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых тегов были сняты флажки. Это состояние сохраняется и в случае, если флажки сняты для всех тегов, выбранных таким способом (из-за того, что количество выбранных тегов может измениться).

Если выбраны все теги, удовлетворяющие параметрам фильтрации и поиска, количество выбранных тегов может автоматически изменяться. Например, состав тегов в таблице может быть изменен пользователем программы в другом сеансе подключения или при автоматическом добавлении обнаруженных тегов (см. раздел "Об обнаружении неизвестных тегов" на стр. 164). Рекомендуется настраивать параметры фильтрации и поиска таким образом, чтобы в выборку попали только нужные теги (например, перед выбором всех тегов вы можете отфильтровать теги по идентификаторам).

Добавление тега вручную

Добавлять теги вручную могут только пользователи с ролью Администратор.

► Чтобы вручную добавить новый тег, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Теги** откройте область деталей по ссылке **Добавить тег**.
4. Откройте окно выбора устройств по ссылке **Выбрать устройство**.
5. В окне выбора устройств выберите устройство, для которого вы хотите создать тег, и нажмите на кнопку **ОК**.

Окно выбора устройств содержит таблицу, в которой можно настраивать отображение и порядок граф, выполнять фильтрацию, поиск и сортировку аналогично таблице устройств (см. раздел "Просмотр таблицы устройств" на стр. 265) в разделе **Активы**.

6. Выберите протокол, который указан в параметрах контроля процесса (см. раздел "Параметры контроля процесса для устройств" на стр. [156](#)) для выбранного устройства. Требуется выбрать протокол, в котором поддерживается передача тегов.

Если нужный протокол отсутствует, вы можете настроить параметры контроля процесса и указать нужный протокол. Для открытия окна настройки используйте кнопку справа от поля для выбора протокола. Настройка параметров контроля процесса выполняется аналогично, как при добавлении (см. раздел "Добавление параметров контроля процесса для устройства вручную" на стр. [158](#)) или изменении (см. раздел "Изменение параметров контроля процесса для устройства" на стр. [159](#)) параметров при работе в таблице устройств.

7. При необходимости измените имя тега. По умолчанию задано имя по шаблону: **Tag <значение счетчика тегов устройства>**.

Вы можете использовать буквы латинского алфавита, цифры, пробел, а также следующие специальные символы: () . , : ; ? ! * + % - < > @ [] { } / \ _ \$ #. Имя тега должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

8. Настройте другие параметры тега (см. раздел "Параметры тегов" на стр. [345](#)).

Для тега должны быть указаны обязательные параметры (например, имя тега, тип данных). Также в зависимости от выбранного протокола и типа данных для настройки могут быть доступны дополнительные параметры (например, единица измерения, пределы масштабирования).

9. Нажмите на кнопку **Сохранить**.

Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

В таблице тегов появится новый тег.

Изменение параметров тега

Изменять параметры тегов могут только пользователи с ролью Администратор.

► *Чтобы изменить параметры тега, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Теги** выберите нужный тег.

В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Изменить**.
5. При необходимости измените имя тега.

Вы можете использовать буквы латинского алфавита, цифры, пробел, а также следующие специальные символы: () . , : ; ? ! * + % - < > @ [] { } / \ _ \$ #. Имя тега должно начинаться и заканчиваться любым допустимым символом, кроме пробела.

6. Настройте другие параметры тега (см. раздел "Параметры тегов" на стр. [345](#)).

Для тега должны быть указаны обязательные параметры (например, имя тега, тип данных). Также в зависимости от выбранного протокола и типа данных для настройки могут быть доступны дополнительные параметры (например, единица измерения, пределы масштабирования).

7. Нажмите на кнопку **Сохранить**.

Кнопка недоступна, если в параметрах указаны не все необходимые значения или есть недопустимые значения.

Добавление тегов в список избранных

Если вы хотите составить список наиболее важных тегов и быстро переходить к этому списку (например, для просмотра текущих значений этих тегов), вы можете добавлять теги в список избранных. Теги можно произвольно добавлять в список избранных и удалять из него. Количество тегов в списке избранных не ограничивается.

Для отображения списка избранных тегов вы можете использовать фильтрацию по графе **Избранное** при просмотре таблицы тегов (см. раздел "Просмотр таблицы тегов" на стр. [346](#)).

По умолчанию созданный тег не добавлен в список избранных.

► *Чтобы добавить в список избранных или удалить из списка один тег, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Теги** выберите тег, который вы хотите добавить в список избранных или удалить из списка.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Установите переключатель **Избранное** в нужное положение.
6. Нажмите на кнопку **Сохранить**.

В зависимости от установленного состояния переключателя, в таблице тегов для этого тега в графе **Избранное** отобразится признак **Да** или **Нет**.

► *Чтобы добавить в список избранных или удалить из списка несколько тегов, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Теги** выберите теги (см. раздел "Выбор тегов в таблице" на стр. [165](#)), которые вы хотите добавить в список избранных или удалить из списка.
В правой части окна веб-интерфейса появится область деталей.
4. Добавьте теги в список избранных или удалите из списка с помощью кнопок **Добавить теги в список избранных** и **Удалить теги из списка избранных**. Каждая из этих кнопок отображается, если среди выбранных тегов есть теги, с которыми можно выполнить соответствующую операцию.

Если выбраны все теги, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных тегов более 1000, программа не проверяет вхождение тегов в список избранных. В этом случае в области деталей отображаются обе кнопки для добавления и удаления тегов.

В зависимости от того, какая кнопка была нажата, в таблице тегов для всех выбранных тегов в графе **Избранное** отобразится признак **Да** или **Нет**.

Удаление тегов

Удалять теги могут только пользователи с ролью Администратор.

► *Чтобы удалить теги, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Теги** выберите теги (см. раздел "Выбор тегов в таблице" на стр. [165](#)), которые вы хотите удалить.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить**.
Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление тегов.

Просмотр правил контроля процесса, связанных с тегами

При работе с таблицей тегов вы можете просмотреть сведения о правилах контроля процесса, связанных с выбранными тегами. Для просмотра сведений доступны следующие возможности:

- Просмотр основных сведений о связанных правилах в окне деталей выбранного тега. Основные сведения выводятся для первых пяти правил, с которыми связан выбранный тег.
- Просмотр подробных сведений о связанных правилах в таблице правил контроля процесса. В таблице правил автоматически применяется фильтрация по идентификаторам выбранных тегов. Возможность загружать сведения о правилах в таблице правил доступна, если выбрано не более 200 тегов.

► *Чтобы просмотреть основные сведения о правилах контроля процесса, связанных с тегом, выполните следующие действия:*

1. Выберите раздел **Контроль процесса**.
2. На закладке **Теги** выберите тег, для которого вы хотите просмотреть основные сведения о правилах контроля процесса.

В правой части окна веб-интерфейса появится область деталей. Основные сведения о связанных правилах выводятся в разделе **Связанные правила контроля процесса** (раздел отсутствует, если с тегом не связано ни одного правила).

В блоках с основными сведениями отображаются имена правил и их текущие состояния. При необходимости вы можете перейти к подробным сведениям о правиле с помощью кнопки **Показать детали**. Подробные сведения о правиле будут показаны в области деталей на закладке **Правила** раздела **Контроль процесса**.

Также для пользователей с ролью Администратор доступны возможности изменения состояний и удаления правил с помощью соответствующих элементов интерфейса в блоках с основными сведениями о правилах.

- Чтобы просмотреть подробные сведения о правилах контроля процесса, связанных с тегами, выполните следующие действия:

1. Выберите раздел **Контроль процесса**.
2. На закладке **Теги** выберите теги (см. раздел "Выбор тегов в таблице" на стр. [165](#)), для которых вы хотите просмотреть сведения о правилах контроля процесса.
В правой части окна веб-интерфейса появится область деталей.
3. В зависимости от количества выбранных тегов, нажмите на одну из следующих кнопок:
 - **Показать правила (<количество правил> в таблице)** – отображается для одного выбранного тега в нижней части раздела **Связанные правила контроля процесса**.
 - **Показать правила контроля процесса** – отображается для нескольких выбранных тегов в нижней части области деталей. Кнопка недоступна, если количество выбранных тегов превышает 200.

Откроется закладка **Правила** раздела **Контроль процесса**. В таблице правил будет применена фильтрация по идентификаторам выбранных тегов.

Правила контроля процесса

Для контроля значений тегов в программе могут использоваться следующие правила контроля процесса:

- Правила с заданными условиями. Эти правила содержат условия для отслеживания значений тегов. Каждое правило может содержать условие одного из предусмотренных типов (см. раздел "Правила с заданными условиями для значений тегов" на стр. [171](#)). Если выполнено заданное в правиле условие, программа регистрирует событие. Параметры регистрируемого события также задаются в правиле.
- Правила с Lua-скриптами. Эти правила содержат описания алгоритмов для проверки значений тегов. Алгоритмы составляются на языке программирования Lua с использованием функций и переменных для Lua-скриптов (см. раздел "Правила с Lua-скриптами" на стр. [173](#)). При срабатывании алгоритма в правиле с Lua-скриптом программа регистрирует событие (параметры регистрируемого события задаются в правиле). Если вы используете Lua-скрипты для правил контроля процесса, то вы можете применить *глобальный Lua-скрипт*, в котором инициализируются глобальные переменные и функции Lua. Эти глобальные переменные и функции вы можете указать в Lua-скрипте любого правила. По умолчанию глобальный Lua-скрипт пустой и не содержит исполняемый код. В программе может существовать только один глобальный Lua-скрипт.

Правила контроля процесса могут быть включены или выключены. Включенные правила применяются при анализе трафика. Выключенные правила не применяются и не учитываются.

Программа может автоматически создавать правила контроля процесса с заданными условиями при работе контроля процесса в режиме обучения (см. раздел "Режим обучения правилам контроля процесса" на стр. [174](#)).

Вы можете просматривать и изменять правила контроля процесса на закладке **Правила** в разделе **Контроль процесса** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

В этом разделе

Правила с заданными условиями для значений тегов.....	171
Правила с Lua-скриптами.....	173
Режим обучения правилам контроля процесса	174
Включение и выключение контроля процесса по правилам.....	175
Просмотр таблицы правил контроля процесса.....	176
Выбор правил контроля процесса.....	180
Создание правила контроля процесса с параметрами условий	181
Создание правила контроля процесса с Lua-скриптом.....	182
Изменение параметров правила контроля процесса	183
Создание, просмотр и изменение глобального Lua-скрипта	183
Удаление правил контроля процесса	183
Просмотр сведений об устройствах, связанных с правилами контроля процесса	184
Просмотр тегов, связанных с правилами контроля процесса	184

Правила с заданными условиями для значений тегов

Для контроля значений тегов вы можете использовать правила контроля процесса, в которых заданы условия для значений тегов. Каждое правило может содержать условие одного из предусмотренных типов. Правило может быть связано только с одним тегом. При этом для тега можно создать до 20 правил с различными типами условий.

Правила с заданными условиями могут быть созданы автоматически программой при работе контроля процесса в режиме обучения (см. раздел "Режим обучения правилам контроля процесса" на стр. [174](#)). Также вы можете вручную создавать (см. раздел "Создание правила контроля процесса с параметрами условий" на стр. [181](#)) и изменять (см. раздел "Изменение параметров правила контроля процесса" на стр. [183](#)) правила с заданными условиями для значений тегов.

Для правила контроля процесса вы можете выбрать один из следующих типов условий:

- **Значение изменилось** – значение контролируемого тега изменилось целиком или в определенном бите.
Если выключен режим контроля определенного бита значения, с этим условием можно контролировать значение тегов любого типа. При этом вы можете указать количество сохраняемых (разрешенных) значений тега, при обнаружении которых не будет регистрироваться событие. Для правила можно указать количество сохраняемых значений от 1 до 10 (сохраняемые значения будут обновляться по мере обнаружения новых значений). По умолчанию сохраняется только последнее значение.
Если включен режим контроля определенного бита значения, с этим условием можно контролировать только теги типов int и unsigned int. Для контроля вам нужно указать порядковый номер отслеживаемого бита в теге (целое число в диапазоне, который соответствует типу данных выбранного тега: от 1 до 8, 16, 32 или 64).
- **Тег отсутствует** – контролируемый тег не обнаружен в отслеживаемом трафике в течение заданного времени.
С этим условием можно контролировать теги любого типа.

- **Обнаружение** – контролируемый тег обнаружен в отслеживаемом трафике.
С этим условием можно контролировать теги любого типа.
- **В диапазоне** – значение контролируемого тега входит в границы указанного диапазона.
С этим условием можно контролировать только теги типов int и float.
Вы можете задать значения для нижней и / или верхней границ диапазона. Заданные значения для границ могут быть включены в диапазон или исключены из него.
- **Вне диапазона** – значение контролируемого тега выходит за границы указанного диапазона.
С этим условием можно контролировать только теги типов int и float.
Вы можете задать значения для нижней и / или верхней границ диапазона. Заданные значения для границ могут быть включены в диапазон или исключены из него.
- **Равно** – значение контролируемого тега равно одному из заданных значений целиком или в определенном бите.
Если выключен режим контроля определенного бита значения, с этим условием можно контролировать значение тегов типов int, bool и string. Вы можете задать от 1 до 10 значений для сравнения.
Если включен режим контроля определенного бита значения, с этим условием можно контролировать только теги типов int и unsigned int. Для контроля вам нужно указать порядковый номер отслеживаемого бита в теге (целое число в диапазоне, который соответствует типу данных выбранного тега: от 1 до 8, 16, 32 или 64) и значение бита для сравнения (в виде одного из двух целых чисел: ноль или единица).
- **Не равно** – значение контролируемого тега не равно одному из заданных значений целиком или в определенном бите.
Если выключен режим контроля определенного бита значения, с этим условием можно контролировать значение тегов типов int, bool и string. Вы можете задать от 1 до 10 значений для сравнения.
Если включен режим контроля определенного бита значения, с этим условием можно контролировать только теги типов int и unsigned int. Для контроля вам нужно указать порядковый номер отслеживаемого бита в теге (целое число в диапазоне, который соответствует типу данных выбранного тега: от 1 до 8, 16, 32 или 64) и значение бита для сравнения (в виде одного из двух целых чисел: ноль или единица).
- **Нарушение монотонного изменения** – значение контролируемого тега нарушает последовательность монотонного возрастания или убывания значений.
С этим условием можно контролировать только теги типов int и float.

Для правил, контролирующих значения тегов, вам нужно учитывать особенности обработки программой значений, представленных денормализованными числами (числа малого порядка, приближенные к нулю – например, 2.22507e-308 в случае представления данного значения с двойной точностью). Программа преобразует денормализованные числа в нулевые значения.

Для любого условия вы можете выбрать операции, при выполнении которых программа будет контролировать значения тега. Предусмотрены следующие варианты контроля в зависимости от операций с тегом:

- **Контроль при чтении тега** – значение проверяется при чтении тега из устройства.
- **Контроль при записи тега** – значение проверяется при записи тега в устройство.

Правила с Lua-скриптами

Для описания алгоритмов проверки значений тегов в правилах контроля процесса могут использоваться скрипты на языке программирования Lua. Lua-скрипты предоставляют возможности не только для проверки значений тегов, но и для добавления различных сведений в регистрируемые события и журналы работы процессов.

Lua-скрипт должен состоять из одной или нескольких функций. Имена функций должны быть уникальны среди всех правил с Lua-скриптами. Функция, с помощью которой отслеживаются значения тегов, называется *триггерной функцией*. Для регистрации события триггерная функция должна возвращать значение `true`.

Если в скрипте указана переменная, она должна быть инициализирована либо в самом скрипте (для применения только в этом скрипте), либо в отдельном глобальном скрипте (для применения во всех правилах с Lua-скриптами). Глобальный скрипт также может содержать вспомогательные функции, которые можно использовать в правилах с Lua-скриптами.

Триггерная функция вызывается при изменении значения какого-либо тега, используемого в функции. Впервые функция вызывается при получении всех значений тегов, используемых в функции.

Для получения значений тега в коде функции используется запись вида:

```
tag'основные_параметры_тега[:имя_поля][@модификатор]' [.направление_передачи]
```

где:

- **основные_параметры_тега** – обязательные параметры, идентифицирующие тег в программе. Параметры разделяются двоеточием. Основные параметры представлены следующими параметрами из таблицы тегов:
 - **Устройство.**
 - **Имя тега.**
 - **Идентификатор тега.**
 - **имя_поля** – имя поля в структуре полей тега, представленной параметром **Структурные значения** в таблице тегов. Если поле является вложенным в другие поля, его имя указывается вместе с именами всех родительских полей, разделенных двоеточием. Если параметр **имя_поля** не указан, проверяется значение, которое является основным в структуре полей тега.
 - **модификатор** – определяет режим представления полученного значения. Предусмотрены следующие модификаторы:
 - `str` – полученное значение преобразуется в строковый тип.
 - `type` – в качестве значения передается название типа данных от полученного значения.
 - `loc` – в качестве значения передается закрепленное локализованное название для полученного значения (если локализованное название отсутствует, полученное значение преобразуется в строковый тип).
- Если модификатор не указан, передается само полученное значение. При этом тип данных значения не меняется.
- **направление_передачи** – задает направление передачи полученного значения. Направление передачи может быть задано одним из следующих параметров:
 - `R` – значение получено при чтении из устройства.
 - `W` – значение получено при записи в устройство.
 - `RW` – любое направление полученного значения.

Если направление передачи не задано, то передается значение, полученное с любого направления.

Записи для получения значений тегов могут использоваться в составе выражений (например, присвоение значений переменным или сравнение значений).

Для выполнения различных действий с помощью Lua-скрипта вы можете использовать *вспомогательные функции*, поддерживаемые Сервером. Имена вспомогательных функций начинаются с символа подчеркивания `_`.

Основные вспомогательные функции для добавления сведений через Lua-скрипты:

- Функция добавления параметров для использования их в качестве дополнительных переменных в событиях (см. раздел "Общие переменные для подстановки значений в Kaspersky Industrial CyberSecurity for Networks" на стр. [232](#)):

```
_AddEventParam('имя_параметра', значение_параметра)
```

Имя и значение параметра могут быть заданы произвольно. Для использования параметра и его значения в событиях этот параметр должен быть указан в параметрах типа события в виде `$extra.<имя_параметра>`.

- Функции для добавления записей в журнал работы процесса, в котором выполняется Lua-скрипт (обычно это процесс, имя которого начинается со слова `Filter`). В журнал вносится запись, заданная аргументом функции (переменной или константой):

- Для создания записи с уровнем *Ошибки*:

```
_WriteErrorLog(аргумент_функции)
```

- Для создания записи с уровнем *Важные*:

```
_WriteWarningLog(аргумент_функции)
```

- Для создания записи с уровнем *Инфо*:

```
_WriteInfoLog(аргумент_функции)
```

- Для создания записи с уровнем *Отладка*:

```
_WriteDebugLog(аргумент_функции)
```

- Для создания записи с уровнем *Отладка*, которая может содержать несколько аргументов функции:

```
print(аргумент_функции1, аргумент_функции2, ...)
```

Переменные или константы, заданные аргументами функции, разделяются в записи журнала символом табуляции.

Записи в журнале не создаются, если уровень записи ниже уровня ведения журнала, установленного для процесса.

Режим обучения правилам контроля процесса

В режиме обучения правилам контроля процесса программа автоматически формирует правила контроля процесса с условиями для значений тегов. Для формирования правил программа анализирует в трафике значения только тех тегов, которые добавлены в таблицу тегов (см. раздел «Теги» на стр. [163](#)).

Правила контроля процесса, которые были автоматически добавлены в режиме обучения, называются *системными*. У этих правил параметр **Источник** содержит значение **Система**.

Правила, созданные вручную, называются *пользовательскими*. У этих правил параметр **Источник** содержит значение **Пользователь**. Если в системное правило внесены изменения вручную, это правило

также становится пользовательским.

Правила, добавленные в режиме обучения, по умолчанию находятся в состоянии *Выключено*. Если системное правило было обновлено в режиме обучения, оно остается в том же состоянии, в котором было до обновления.

В режиме обучения правилам контроля процесса при добавлении или обновлении программа задает для каждого из них одно из следующих условий:

- **Не равно.**

Это условие задается при добавлении правила (если для обнаруженного значения тега не найдено другое системное правило) или при получении до десяти различных значений тега (кроме тегов с типом данных bool или float).

- **Вне диапазона.**

В правиле выполняется замена на это условие, если получено новое значение для тега с типом данных float или если получено более десяти различных значений для тега с типом данных int.

- **Нарушение монотонного изменения.**

В правиле выполняется замена на это условие, если обнаруженные значения тега изменялись только в сторону возрастания или только в сторону убывания. Замена на это условие выполняется в правилах для тегов с типом данных int или float по окончании режима обучения.

Также в режиме обучения программа удаляет системные правила контроля процесса в следующих случаях:

- если правило создано для тега с типом данных bool и обнаруженное и сохраненное значения не совпадают (сравнения выполняются только для первых десяти обнаруженных значений, остальные игнорируются);
- если правило создано для тега с типом данных string и получено более десяти различных значений.

Режим обучения правилам контроля процесса должен быть включен на время, достаточное для обнаружения всех возможных значений нужных тегов. Это время зависит от интенсивности появления тегов в трафике, периодичности работы устройств в промышленной сети и других особенностей технологического процесса. Рекомендуется включать режим обучения на время не менее одного часа. В крупных промышленных сетях, для накопления данных в максимальном объеме, режим обучения можно включить на период от одного до нескольких дней.

Включение и выключение контроля процесса по правилам

Включать и выключать контроль процесса по правилам могут только пользователи с ролью Администратор.

► *Чтобы включить или выключить контроль процесса по правилам, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Технологии**.
3. С помощью переключателя **Контроль процесса по правилам** включите или выключите контроль процесса 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.

5. Выберите нужный режим работы контроля процесса по правилам. 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.

Просмотр таблицы правил контроля процесса

Таблица правил контроля процесса отображается на закладке **Правила** в разделе **Контроль процесса** веб-интерфейса программы. В таблице представлены общие параметры правил а также тегов и устройств, к которым относятся правила.

При просмотре таблицы правил вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице правил

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

1. На закладке **Правила** в разделе **Контроль процесса** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
2. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр (см. ниже).
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 тегов.


Для выбора доступны следующие параметры:



- **ID правила** – уникальный идентификатор правила.
- **Группа устройств** – имя группы, в которую помещено связанное с тегом устройство (содержит имя самой группы и имена всех ее родительских групп в дереве групп устройств).
- **Устройство** – имя связанного с тегом устройства.
- **Протокол** – название протокола, по которому передается тег.

- **Имя тега** – заданное имя тега, для которого создано правило.
- **Правило** – заданное имя правила.
- **Состояние** – текущее состояние правила (*Включено* или *Выключено*).
- **Тип условия** – название выбранного типа условия для правила.
- **Создано** – дата и время создания правила.
- **Изменено** – дата и время последнего изменения правила.
- **Заголовок события** – заголовок события, регистрируемого при срабатывании правила.
- **Важность события** – уровень важности события, регистрируемого при срабатывании правила.
- **Описание события** – описание события, регистрируемого при срабатывании правила.
- **Источник** – сведения об источнике правила.

- Фильтрация по графам таблицы

► *Чтобы отфильтровать правила по графе **ID правила**, **Устройство**, **Имя тега** или **Правило**, выполните следующие действия:*

1. На закладке **Правила** в разделе **Контроль процесса** нажмите на значок фильтрации в нужной графе таблицы.
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 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 правила по графе **Группа устройств**, выполните следующие действия:*
1. На закладке **Правила** в разделе **Контроль процесса** нажмите на значок фильтрации в графе **Группа устройств**.
Откроется окно фильтрации.
 2. Нажмите на значок в правой части поля для указания группы устройств.
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 (ИЛИ)** 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 правила по графе **Протокол**, выполните следующие действия:*
1. На закладке **Правила** в разделе **Контроль процесса** нажмите на значок фильтрации в графе **Протокол**.
Откроется окно фильтрации.
 2. В поле **Протоколы** укажите нужный протокол из числа поддерживаемых протоколов прикладного уровня. Для этого начните вводить название протокола и выберите нужный протокол в раскрывшемся списке (список подходящих протоколов автоматически раскрывается при изменении значения в поле **Протоколы**).
Вы можете отсортировать открывшийся список протоколов по ссылке **Сортировка**.
 3. Если вы хотите добавить еще один протокол, нажмите на кнопку **Добавить протокол** и укажите другой протокол в открывшемся поле.
 4. Если вы хотите удалить один из указанных протоколов, в окне фильтрации нажмите на значок . Вы также можете удалить все указанные протоколы по ссылке **Фильтр по умолчанию** в окне фильтрации.
 5. Нажмите на кнопку **ОК**.

- ▶ *Чтобы отфильтровать правила по графе **Состояние**, **Важность события** или **Источник**, выполните следующие действия:*
 1. На закладке **Правила** в разделе **Контроль процесса** нажмите на значок фильтрации в нужной графе.

Для фильтрации по состояниям или источникам правил контроля процесса 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 **Создано** или **Изменено**, выполните следующие действия:*
 1. На закладке **Правила** в разделе **Контроль процесса** нажмите на значок фильтрации в нужной графе.

Откроется календарь.
 2. В календаре задайте дату начальной и конечной границ периода фильтрации. Для этого выберите дату в календаре (при этом будет указано текущее время) или введите значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс. Если указывать дату и время границы периода фильтрации не требуется, вы можете не выбирать дату или удалить текущее значение.
 3. Нажмите на кнопку **ОК**.

- Поиск правил

- ▶ *Чтобы найти нужные правила,*

на закладке **Правила** в разделе **Контроль процесса** введите поисковый запрос в поле **Поиск правил**. Поиск инициируется во время ввода символов.

В таблице правил контроля процесса отобразятся правила, которые удовлетворяют условиям поиска.

Поиск выполняется по всем графам, кроме граф **Состояние**, **Тип условия**, **Создано**, **Изменено**, **Заголовок события**, **Важность события**, **Описание события** и **Источник**.

- Сброс заданных параметров фильтрации и поиска

- ▶ *Чтобы сбросить заданные параметры фильтрации и поиска в таблице правил контроля процесса,*

в панели инструментов на закладке **Правила** в разделе **Контроль процесса** нажмите на кнопку **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации или поиска).

- Сортировка правил

► *Чтобы отсортировать правила контроля процесса, выполните следующие действия:*

1. На закладке **Правила** в разделе **Контроль процесса** 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.

- Обновление таблицы правил

Правила контроля процесса могут быть изменены на Сервере в то время, когда вы просматриваете таблицу правил. Например, таблица правил контроля процесса становится неактуальной, если пользователь программы в другом сеансе подключения изменил правила или программа выполнила преобразования правил в режиме обучения (см. раздел "Режим обучения правилам контроля процесса" на стр. [174](#)).

Для поддержания таблицы правил контроля процесса в актуальном состоянии вы можете включить автоматическое обновление правил.

► *Чтобы включить или выключить автоматическое обновление таблицы правил контроля процесса,*

на закладке **Правила** в разделе **Контроль процесса** используйте переключатель **Обновлять автоматически**.

Выбор правил контроля процесса

В таблице правил контроля процесса 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 процесса, 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**.
- 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.

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 преобразовании правил в режиме обучения (см. раздел "Режим обучения правилам контроля процесса" на стр. 174). 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 правила контроля процесса с параметрами условий

Для создания правил контроля процесса с параметрами условий предусмотрены следующие варианты:

- создание нового правила для тега;
 - создание дополнительного правила на основе имеющегося правила.
- *Чтобы создать новое правило для тега, выполните следующие действия:*
- Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
 - Выберите раздел **Контроль процесса**.
 - На закладке **Теги** выберите тег, для которого вы хотите создать правило контроля процесса. В правой части окна веб-интерфейса появится область деталей.
 - Нажмите на кнопку **Создать правило для тега**.
Откроется закладка **Правила** с областью деталей создаваемого правила контроля процесса.
 - Выполните следующие действия:
 - С помощью переключателя **Включить** задайте состояние правила: *Включено* или *Выключено*.
 - Введите имя и описание правила.
Вы можете использовать буквы латинского алфавита, цифры, пробел, а также следующие специальные символы: () . , : ; ? ! * + % - < > @ [] { } / \ _ \$ #. Имя правила должно начинаться и заканчиваться любым допустимым символом, кроме пробела.
 - Выберите тип условия и настройте параметры в зависимости от выбранного типа.
 - Настройте параметры регистрации события при срабатывании правила (заголовок и описание события, важность и параметры сохранения трафика).
 - Нажмите на кнопку **Сохранить**.

- *Чтобы создать дополнительное правило контроля процесса на основе имеющегося правила, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Правила** выберите правило, на основе которого вы хотите создать другое правило для того же самого тега.

В правой части окна веб-интерфейса появится область деталей.


4. Нажмите на кнопку **Создать другое правило для тега**.
Появится область деталей создаваемого правила контроля процесса. Для нового правила будут указаны сведения об устройстве, протоколе и теге, полученные из параметров выбранного правила.
5. Выполните следующие действия:
 - a. С помощью переключателя **Включить** задайте состояние правила: *Включено* или *Выключено*.
 - b. Введите имя и описание правила.
 - c. Выберите тип условия и настройте параметры в зависимости от выбранного типа.
 - d. Настройте параметры регистрации события при срабатывании правила (заголовок и описание события, важность и параметры сохранения трафика).
6. Нажмите на кнопку **Сохранить**.

Создание правила контроля процесса с Lua-скриптом

- *Чтобы создать правило с Lua-скриптом, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Правила** откройте область деталей по ссылке **Добавить Lua-скрипт**.
4. Выполните следующие действия:
 - a. С помощью переключателя **Включить** задайте состояние правила: *Включено* или *Выключено*.
 - b. Введите имя и описание правила.
 - c. Если вы хотите задать скрипт из шаблона, в области деталей нажмите на кнопку **Использовать шаблон Lua**, в открывшемся окне выберите нужный шаблон и нажмите на кнопку **Применить**.
 - d. В поле **Lua-скрипт для правила** введите код скрипта на языке Lua.

В поле ввода скрипта отображаются имена функций и комментарии, загруженные из шаблона. Вы можете формировать скрипт, изменяя и дополняя шаблонные строки. При вводе текста рядом с курсором автоматически появляются подсказки или доступные для выбора значения (например, подходящие имена устройств и тегов при вводе параметров, идентифицирующих тег (см. раздел "Правила с Lua-скриптами" на стр. [173](#))).

Если код скрипта не помещается в поле **Lua-скрипт для правила**, вы можете открыть отдельное окно для отображения кода с помощью кнопки .

- e. Настройте параметры регистрации события при срабатывании правила (заголовок и описание события, важность и параметры сохранения трафика).
5. Нажмите на кнопку **Сохранить**.

Изменение параметров правила контроля процесса

► *Чтобы изменить параметры правила контроля процесса, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Правила** выберите правило, которое вы хотите изменить.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Измените нужные параметры. Для изменения параметров вам доступны те же действия, что и при создании правил контроля процесса с параметрами условий (см. раздел "Создание правила контроля процесса с параметрами условий" на стр. [181](#)) или с Lua-скриптами (см. раздел "Создание правила контроля процесса с Lua-скриптом" на стр. [182](#)).

Создание, просмотр и изменение глобального Lua-скрипта

Переменные и функции, заданные в глобальном Lua-скрипте могут использоваться в правилах с Lua-скриптами (см. раздел "Правила с Lua-скриптами" на стр. [173](#)).

Создать и изменить глобальный Lua-скрипт для правил контроля процесса могут только пользователи с ролью Администратор. При этом просматривать содержимое глобального Lua-скрипта могут как пользователи с ролью Администратор, так и пользователи с ролью Оператор.

► *Чтобы создать или изменить глобальный Lua-скрипт, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Правила** откройте окно редактирования глобального Lua-скрипта по ссылке **Глобальный Lua-скрипт**.
4. Введите код скрипта на языке Lua.
5. Нажмите на кнопку **Сохранить**.

Удаление правил контроля процесса

► *Чтобы удалить правила контроля процесса, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Контроль процесса**.
3. На закладке **Правила** выберите правила (см. раздел "Выбор правил контроля процесса" на стр. [180](#)), которые вы хотите удалить.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить**.
Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление правил.

Просмотр сведений об устройствах, связанных с правилами контроля процесса

Вы можете просмотреть сведения об устройствах, с которыми связаны правила контроля процесса (правила контроля процесса связаны с устройствами через теги). Сведения об устройствах выводятся в таблице устройств. В таблице устройств автоматически применяется фильтрация по идентификаторам устройств, которые указаны в тегах.

Возможность загружать сведения доступна, если выбрано не более 200 правил.

► *Чтобы просмотреть сведения об устройствах в таблице устройств, выполните следующие действия:*

1. Выберите раздел **Контроль процесса**.
2. На закладке **Правила** выберите правила (см. раздел "Выбор правил контроля процесса" на стр. [180](#)), для которых вы хотите просмотреть сведения об устройствах.
В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Показать устройство** (если выбрано одно правило) или **Показать устройства** (если выбрано несколько правил).

Кнопка **Показать устройства** недоступна, если количество выбранных правил превышает 200.

Откроется раздел **Активы**. В таблице устройств на закладке **Устройства** будет применена фильтрация по идентификаторам устройств, с которыми связаны выбранные правила.

Просмотр тегов, связанных с правилами контроля процесса

Вы можете просмотреть сведения о тегах, с которыми связаны выбранные правила контроля процесса. В таблице тегов автоматически применяется фильтрация по идентификаторам тегов, указанных в правилах.

Возможность загружать сведения доступна, если выбрано не более 200 правил.

► *Чтобы просмотреть сведения о тегах, связанных с правилами контроля процесса, выполните следующие действия:*

1. Выберите раздел **Контроль процесса**.
2. На закладке **Правила** выберите правила (см. раздел "Выбор правил контроля процесса" на стр. [180](#)), для которых вы хотите просмотреть сведения о тегах.
В правой части окна веб-интерфейса появится область деталей.
3. Нажмите на кнопку **Показать тег** (если выбрано одно правило) или **Показать теги** (если выбрано несколько правил).

Кнопка **Показать теги** недоступна, если количество выбранных правил превышает 200.

Откроется закладка **Теги** раздела **Контроль процесса**. В таблице тегов будет применена фильтрация по идентификаторам тегов.

Настройка контроля взаимодействий

Kaspersky Industrial CyberSecurity for Networks может отслеживать сетевые взаимодействия устройств в промышленной сети. Для определения разрешенных и неразрешенных сетевых взаимодействий используются *правила контроля взаимодействий*. Все обнаруженные сетевые взаимодействия, которые не удовлетворяют действующим правилам контроля взаимодействий, считаются не разрешенными. При обнаружении таких взаимодействий программа регистрирует соответствующие события.

Сетевые взаимодействия между устройствами определяются по MAC- и / или IP-адресам устройств. Если для одной из сторон взаимодействия известен только IP-адрес устройства, этот IP-адрес проверяется на принадлежность известным программам подсетям (см. раздел "Просмотр подсетей для контроля активов" на стр. [270](#)). Для отправителей и получателей сетевых пакетов учитываются только те IP-адреса, которые принадлежат подсетям определенных типов (IP-адреса некоторых типов подсетей не контролируются программой).

Подсети IP-адресов для контроля взаимодействий

Таблица 2. Контролируемые взаимодействия в зависимости от подсетей IP-адресов

Подсеть отправителя	Подсеть получателя				
	Частная, IT	Частная, OT	Частная, DMZ	Публичная	Link-local
Частная, IT	нет	да	нет	нет	да
Частная, OT	да	да	да	да	да
Частная, DMZ	нет	да	нет	нет	да
Публичная	нет	да	нет	нет	да
Link-local	да	да	да	да	нет

Пример

При контроле взаимодействий программа проверяет все сетевые пакеты, в которых в качестве получателей указаны IP-адреса из подсетей с типом **Частная, OT**.

Правило контроля взаимодействий может относиться к одной из следующих технологий:

- Контроль целостности сети – правило описывает сетевое взаимодействие устройств, использующих заданный набор протоколов и параметров соединения.
- Контроль системных команд – правило описывает контролируемые системные команды при взаимодействии между устройствами по одному из поддерживаемых протоколов для контроля процесса (см. раздел "Поддерживаемые устройства и протоколы" на стр. [153](#)).

Правило контроля взаимодействий содержит следующую информацию о взаимодействии:

- стороны, принимающие участие в сетевом взаимодействии;
- разрешенный протокол или системные команды.

Правила контроля взаимодействий могут быть включены или выключены.

По умолчанию после создания правило включено и применяется для разрешения описанных взаимодействий. При обнаружении взаимодействий, описанных во включенных правилах, программа не регистрирует события.

Выключенные правила предназначены для описания нежелательных сетевых взаимодействий. В режиме обучения для технологий контроля взаимодействий (см. раздел "Режим обучения для технологий контроля взаимодействий" на стр. [187](#)) выключенные правила предотвращают автоматическое создание новых включенных правил, описывающих те же сетевые взаимодействия. В режиме наблюдения (см. раздел "Режим наблюдения для технологий контроля взаимодействий" на стр. [188](#)) выключенные правила не учитываются.

Программа обрабатывает правила контроля взаимодействий по технологиям Контроль целостности сети и Контроль системных команд, если включено применение этих технологий (см. раздел «Выбор применяемых технологий контроля взаимодействий» на стр. [189](#)).

Для создания списка правил контроля взаимодействий предусмотрены следующие способы:

- автоматическое формирование правил в режиме обучения (см. раздел "Автоматическое формирование правил контроля взаимодействий в режиме обучения" на стр. [189](#));
- создание правил вручную (см. раздел "Создание правил контроля взаимодействий вручную" на стр. [197](#)).

Вы можете настраивать правила контроля взаимодействий в разделе **Разрешающие правила** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks. Раздел содержит таблицу с правилами контроля взаимодействий по технологиям Контроль целостности сети и Контроль системных команд. Также в этой таблице правил могут быть представлены созданные разрешающие правила (см. раздел "Создание разрешающих правил для событий" на стр. [321](#)) для событий.

События, регистрируемые по технологиям Контроль целостности сети и Контроль системных команд, относятся к системным типам событий (см. раздел "Системные типы событий в Kaspersky Industrial CyberSecurity for Networks" на стр. [414](#)).

Вы можете просматривать события контроля взаимодействий в таблице зарегистрированных событий (см. раздел "Мониторинг событий и инцидентов" на стр. [305](#)). 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.

В этом разделе

Режим обучения для технологий контроля взаимодействий.....	187
Режим наблюдения для технологий контроля взаимодействий	188
Выбор применяемых технологий контроля взаимодействий	189
Автоматическое формирование правил контроля взаимодействий в режиме обучения	189
Просмотр правил контроля взаимодействий в таблице разрешающих правил	190
Выбор правил контроля взаимодействий в таблице разрешающих правил.....	196
Создание правил контроля взаимодействий вручную	197
Изменение параметров правила контроля взаимодействий	201
Включение и выключение правил контроля взаимодействий	201
Удаление правил контроля взаимодействий	202

Режим обучения для технологий контроля взаимодействий

В режиме обучения для технологий контроля взаимодействий программа выполняет следующие действия:

- Если включено применение технологии Контроль целостности сети, программа формирует правила по этой технологии. При обнаружении сетевых взаимодействий, которые удовлетворяют выключенным правилам, регистрируются события по технологии Контроль целостности сети. Для регистрации используется системный тип события (см. раздел "Системные типы событий по технологии Контроль целостности сети" на стр. [415](#)), которому присвоен код 4000002601.
- Если включено применение технологии Контроль системных команд, программа формирует правила по этой технологии. При обнаружении системных команд, которые удовлетворяют выключенным правилам, регистрируются события обнаружения неразрешенных системных команд по технологии Контроль системных команд. Для регистрации используется системный тип события (см. раздел "Системные типы событий по технологии Контроль системных команд" на стр. [415](#)), которому присвоен код 4000002602.

При формировании правил по технологиям контроля взаимодействий добавляются новые правила, полученные в результате анализа сетевых взаимодействий и системных команд в трафике промышленной сети. Для этих правил параметр **Источник** содержит значение **Система**. Если вы вручную измените параметры правила, параметр **Источник** примет значение **Пользователь**.

Сетевые взаимодействия, обнаруженные при анализе трафика, проверяются на соответствие текущим правилам контроля взаимодействий. Если обнаруженное взаимодействие не соответствует ни одному правилу, программа создает новое правило. Событие обнаружения взаимодействия в этом случае не регистрируется. При создании нового правила программа включает его и добавляет значения параметров на основании полученных данных о сетевом взаимодействии.

Если обнаруженное взаимодействие соответствует только выключенному правилу, программа регистрирует событие по технологии, соответствующей этому правилу. В этом случае новое правило не создается.

В процессе обучения программа может оптимизировать список правил контроля взаимодействий. Оптимизация заключается в объединении двух и более частных правил в одно общее правило либо в удалении частных правил при наличии общего правила. В оптимизации участвуют правила, для которых выполняются следующие условия:

- правила включены;
- параметр **Источник** содержит значение **Система**;
- правила относятся к одной технологии.

Объединение правил при оптимизации происходит, если полученное общее правило будет соответствовать только обнаруженным сетевым взаимодействиям и никаким другим. Например, после обнаружения системной команды при взаимодействии двух устройств было создано одно правило контроля взаимодействий. Затем была обнаружена другая системная команда при взаимодействии этих же устройств. В этом случае в результате оптимизации останется одно общее правило, описывающее обе системные команды при сетевом взаимодействии этих устройств.

Во время работы в режиме обучения программа периодически выполняет оптимизацию правил для соответствующей технологии контроля взаимодействий. Периодичность оптимизации – один раз в минуту. Оптимизация выполняется, если в трафике промышленной сети обнаружены новые взаимодействия. Для поддержания таблицы правил в актуальном состоянии требуется обновлять правила (см. раздел "Просмотр правил контроля взаимодействий в таблице разрешающих правил" на стр. [190](#)).

После выключения режима обучения (см. раздел "Выбор применяемых технологий контроля взаимодействий" на стр. [189](#)) оптимизация выполняется еще один раз.

Оптимизация правил контроля взаимодействий после выключения режима обучения может выполняться с задержкой. Длительность задержки зависит от интенсивности поступления данных в программу и может составлять до трех минут. В течение этого времени рекомендуется не вносить изменения в правила по технологиям Контроля целостности сети и Контроля системных команд, созданные в режиме обучения.

Режим обучения для технологий контроля взаимодействий должен быть включен на время, достаточное для получения всех необходимых данных о сетевых взаимодействиях. Это время зависит от количества устройств в промышленной сети, периодичности их работы и обслуживания. Рекомендуется включать режим обучения на время не менее одного часа. В крупных промышленных сетях, для накопления данных в максимальном объеме, режим обучения можно включить на период от одного до нескольких дней.

Режим наблюдения для технологий контроля взаимодействий

В режиме наблюдения для технологий контроля взаимодействий программа выполняет следующие действия:

- Если включено применение технологии Контроль целостности сети, программа проверяет сетевые взаимодействия устройств на соответствие правилам по этой технологии. При обнаружении сетевых взаимодействий, для которых отсутствуют включенные правила, регистрируются события обнаружения неразрешенных взаимодействий по технологии Контроль целостности сети. Для регистрации используется системный тип события (см. раздел "Системные типы событий по технологии Контроль целостности сети" на стр. [415](#)), которому присвоен код 4000002601.
- Если включено применение технологии Контроль системных команд, программа проверяет сетевые взаимодействия устройств на соответствие правилам по этой технологии. При обнаружении системных команд, для которых отсутствуют включенные правила, регистрируются события обнаружения неразрешенных системных команд по технологии Контроль системных команд. Для регистрации используется системный тип события (см. раздел "Системные типы событий по технологии Контроль системных команд" на стр. [415](#)), которому присвоен код 4000002602.

Правила, относящиеся к разным технологиям, применяются независимо друг от друга. Поэтому чтобы разрешить использование системной команды, в таблице разрешающих правил должны быть созданы правила (автоматически (см. раздел "Автоматическое формирование правил контроля взаимодействий в режиме обучения" на стр. [189](#)) или вручную (см. раздел "Создание правил контроля взаимодействий вручную" на стр. [197](#))) и для этой системной команды, и для сетевого пакета, в котором она передается.

См. также

Выбор применяемых технологий контроля взаимодействий [189](#)

Выбор применяемых технологий контроля взаимодействий

Управлять технологиями контроля взаимодействий могут только пользователи с ролью Администратор.

► Чтобы включить или выключить применение технологий контроля взаимодействий, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Технологии**.
3. Включите или выключите применение технологий контроля взаимодействий, 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.

5. Для каждой включенной технологии выберите нужный режим контроля взаимодействий. 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.

Процесс занимает некоторое время, при этом в раскрывающемся списке отображается статус *Изменение*.

Автоматическое формирование правил контроля взаимодействий в режиме обучения

В режиме обучения (см. раздел "Режим обучения для технологий контроля взаимодействий" на стр. [187](#)) Kaspersky Industrial CyberSecurity for Networks автоматически формирует правила контроля взаимодействий. Программа создает новое правило, если обнаруженное сетевое взаимодействие не соответствует ни одному правилу в таблице разрешающих правил.

При создании правила программа задает значения параметров, полученные из трафика и относящиеся к обнаруженному сетевому взаимодействию.

Если правило создается для взаимодействия, в котором IP-адрес одной из сторон принадлежит известной программе подсети (см. раздел "Просмотр подсетей для контроля активов" на стр. [270](#)), то программа может не добавить в параметры правила MAC-адреса, обнаруженные вместе с этим IP-адресом. Обнаруженные MAC-адреса для IP-адресов подсети добавляются в случае, если в параметрах подсети (см. раздел "Формирование списка подсетей для контроля активов" на стр. [133](#)) выключен режим пропуска MAC-адресов с помощью переключателя **Игнорировать MAC-адреса для правил NIC**.

В режиме обучения программа может автоматически создавать правила контроля взаимодействий, разрешающие отправку системных команд для Kaspersky Industrial CyberSecurity for Nodes. 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 (см. раздел "Выбор применяемых технологий контроля взаимодействий" на стр. 189) 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 правил контроля взаимодействий в таблице разрешающих правил

Правила контроля взаимодействий отображаются в таблице разрешающих правил в разделе **Разрешающие правила** веб-интерфейса программы. К правилам контроля взаимодействий относятся правила следующих типов:

- NIC – правила по технологии Контроль целостности сети.
- CC – правила по технологии Контроль системных команд.

Для просмотра нужных сведений о правилах контроля взаимодействий в таблице разрешающих правил вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице правил


► *Чтобы настроить параметры отображения таблицы разрешающих правил, выполните следующие действия:*

1. В разделе **Разрешающие правила** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
2. Для сторон сетевых взаимодействий **Сторона 1** и **Сторона 2** выберите отображаемые сведения в таблице. Для этого в раскрывающемся списке для каждой стороны выберите один из следующих вариантов:
 - **Адресная информация.** В графе таблицы отображается только адресная информация, представляющая сторону сетевого взаимодействия.
 - **Имена устройств.** Вместо адресной информации, которая соответствует известным программе устройствам, в графе таблицы отображаются имена этих устройств. Остальная адресная информация отображается в явном виде (например, диапазоны адресов).
3. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр (см. ниже).
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 разрешающих правил.


Для выбора доступны следующие параметры:

- **ID правила.**
Уникальный идентификатор правила.
- **Состояние** (значок )
Текущее состояние правила (*Включено* или *Выключено*).
- **Тип правила.**
Для правил контроля взаимодействий – технология, к которой относится правило (NIC или CC). Для правил, выключающих регистрацию событий, указан тип EVT.
- **Протоколы/Команды.**
Для правил, относящихся к технологии Контроль целостности сети (тип NIC) или выключающих регистрацию событий (тип EVT) – набор используемых протоколов. Для правил, относящихся к технологии Контроль системных команд (тип CC) – протокол и системные команды. Протоколы, которые определяются программой по содержимому сетевых пакетов, выделены курсивом.
- **Сторона 1.**
Имя устройства / адресная информация одной из сторон сетевого взаимодействия. Отображение адресов и портов адресной информации можно включать и выключать с помощью следующих параметров:
 - **MAC-адрес.**
 - **IP-адрес.**
 - **Номер порта.**
- **Сторона 2.**
Имя устройства / адресная информация другой стороны сетевого взаимодействия. Отображение адресов и портов адресной информации можно включать и выключать с помощью следующих параметров:
 - **MAC-адрес.**
 - **IP-адрес.**
 - **Номер порта.**
- **Комментарий.**
Дополнительная информация о правиле.

- **Создано.**
Дата и время создания правила.
- **Изменено.**
Дата и время последнего изменения правила.
- **Источник.**
Сведения об источнике правила.
- **Правило в событии.**
Имя правила контроля процесса или обнаружения вторжений, которое должно быть указано в событии (для правил типа EVT).
- **Точка мониторинга.**
Имя точки мониторинга, которое должно быть указано в событии (для правил типа EVT).
- **Тип события.**
Идентификатор и заголовок типа события (для правил типа EVT).

- Фильтрация по графам таблицы

► *Чтобы отфильтровать правила по графе **ID правила**, **Правило в событии** или **Тип события**, выполните следующие действия:*

1. В разделе **Разрешающие правила** нажмите на значок фильтрации в нужной графе.
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**, **Тип правила**, **Источник** или **Точка мониторинга**, выполните следующие действия:

1. В разделе **Разрешающие правила** нажмите на значок фильтрации в нужной графе.

При фильтрации по состояниям, типам правил и источникам 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 **Разрешающие правила** нажмите на значок фильтрации в графе **Протоколы/Команды**.

Фильтрация по графе **Протоколы/Команды** выполняется только по протоколам. Для фильтрации правил по названиям системных команд (правила по технологии Контроль 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 **Разрешающие правила** 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 **Создано** или **Изменено**, выполните следующие действия:

1. В разделе **Разрешающие правила** нажмите на значок фильтрации в нужной графе.

Откроется календарь.

2. В календаре задайте дату начальной и конечной границ периода фильтрации. Для этого выберите дату в календаре (при этом будет указано текущее время) или введите значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс. Если указывать дату и время границы периода фильтрации не требуется, вы можете не выбирать дату или удалить текущее значение.

3. Нажмите на кнопку **ОК**.

- Поиск правил

► Чтобы найти нужные разрешающие правила,

в разделе **Разрешающие правила** введите поисковый запрос в поле **Поиск правил**.

Поиск инициируется во время ввода символов.

В таблице разрешающих правил отобразятся правила, которые удовлетворяют условиям поиска.

Поиск выполняется по всем графам, кроме граф **ID правила**, **Состояние**, **Тип правила**, **Создано**, **Изменено**, **Источник** и **Точка мониторинга**.

- Сброс заданных параметров фильтрации и поиска

► Чтобы сбросить заданные параметры фильтрации и поиска в таблице разрешающих правил,

в панели инструментов в разделе **Разрешающие правила** нажмите на кнопку **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации или поиска).

- Сортировка правил

► Чтобы отсортировать правила в таблице разрешающих правил, выполните следующие действия:

1. В разделе **Разрешающие правила** нажмите на заголовок графы, по которой вы хотите выполнить сортировку.

Вы можете отсортировать таблицу правил по значениям любой графы, кроме граф **Комментарий**, **Источник**, **Точка мониторинга** или **Тип события**.

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

Состав разрешающих правил может быть изменен на Сервере в то время, когда вы просматриваете таблицу правил. Например, таблица правил становится неактуальной, если пользователь программы в другом сеансе подключения изменил правила или программа выполнила оптимизацию списка правил контроля взаимодействий в режиме обучения.

Для поддержания таблицы разрешающих правил 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 разрешающих правил,*

в разделе **Разрешающие правила** используйте переключатель **Обновлять автоматически**.

При включенном автоматическом обновлении таблица разрешающих правил обновляется через каждые пять секунд.

- ▶ *Чтобы вручную обновить таблицу разрешающих правил,*

в разделе **Разрешающие правила** запустите обновление таблицы правил по ссылке **Обновить** (ссылка отображается справа от переключателя **Обновлять автоматически**, если переключатель выключен).

Таблица разрешающих правил заново загрузится с Сервера.

Выбор правил контроля взаимодействий в таблице разрешающих правил

В таблице разрешающих правил вы можете выбирать правила контроля взаимодействий для просмотра сведений и для работы с этими правилами. При выборе правил в правой части окна веб-интерфейса появляется область деталей.

Перед выбором правил вы можете настроить таблицу разрешающих правил (см. раздел "Просмотр правил контроля взаимодействий в таблице разрешающих правил" на стр. [190](#)) для отображения правил контроля взаимодействий в нужном порядке.

- ▶ *Чтобы выбрать нужные правила контроля взаимодействий, 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 включенных и выключенных 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 (см. раздел "Режим обучения для технологий контроля взаимодействий" на стр. 187). 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 взаимодействий вручную

Вы можете создавать правила контроля взаимодействий вручную, используя следующие возможности:

- Создание правила с изначально пустыми значениями параметров или со значениями из шаблона

- Чтобы создать правило с изначально пустыми значениями параметров или со значениями из шаблона, выполните следующие действия:
1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
 2. В разделе **Разрешающие правила** откройте область деталей по ссылке **Добавить правило**.
 3. Если вы хотите задать значения параметров из шаблона, в области деталей нажмите на кнопку **Использовать шаблон**, в открывшемся окне выберите нужный шаблон и нажмите на кнопку **Применить**.
 4. В области деталей выберите тип правила, соответствующий нужной технологии контроля взаимодействий:
 - Если вы хотите создать правило по технологии Контроль целостности сети, нажмите на кнопку **НИС**.
 - Если вы хотите создать правило по технологии Контроль системных команд, нажмите на кнопку **СС**.
 5. В поле **Протокол** укажите протокол для взаимодействия устройств.
 При выборе поля **Протокол** откроется окно с таблицей поддерживаемых протоколов, отображаемых в виде дерева стека протоколов. Вы можете управлять отображением элементов дерева с помощью кнопок **+** и **-** рядом с названиями протоколов, которые содержат протоколы следующих уровней.
 При необходимости воспользуйтесь поисковой строкой над таблицей, чтобы найти нужные протоколы (см. ниже).
 6. Если для правила выбрана технология Контроль системных команд, в поле **Команды** укажите нужные системные команды.
 При выборе поля **Команды** открывается окно со списком системных команд, доступных для выбранного протокола (см. ниже).
 7. При необходимости введите дополнительную информацию о правиле в поле **Комментарий**.
 8. В блоках параметров **Сторона 1** и **Сторона 2** укажите доступную для изменения адресную информацию для сторон сетевого взаимодействия. В зависимости от выбранного протокола (или набора протоколов), адресная информация может содержать MAC-адрес, IP-адрес и / или номер порта.
 Для автоматического заполнения адресной информации стороны сетевого взаимодействия вы можете выбрать известные программе устройства (см. ниже).
 9. В области деталей нажмите на кнопку **Сохранить**.
 Программа проверит текущий состав правил контроля взаимодействий.
 10. Если среди правил контроля взаимодействий присутствует включенное правило, в котором совпадают все параметры, отобразится предупреждение о наличии совпадающего правила. В этом случае закройте предупреждение и измените параметры создаваемого правила.
 11. Если среди правил контроля взаимодействий присутствует включенное правило с более общими параметрами, отобразится предупреждение о наличии общего правила. При наличии общего правила новое частное правило не будет использоваться в программе. Предупреждение будет содержать запрос на сохранение нового частного правила. Для создания нового правила с заданными параметрами подтвердите решение в окне запроса (например, если вы хотите потом удалить общее правило).
 Новое правило будет добавлено в таблицу разрешающих правил.
 12. Если среди правил контроля взаимодействий присутствуют включенные правила с более частными параметрами, отобразится предупреждение о наличии более частных правил. После появления общего правила частные правила не будут использоваться в программе. Предупреждение будет содержать запрос на удаление частных правил. Для удаления частных правил подтвердите решение в окне запроса.

Если в таблице правил присутствуют выключенные правила с более частными или совпадающими параметрами, программа удаляет эти правила из списка. При удалении этих правил программа не отображает запрос.

Если для нового правила по технологии Контроль системных команд отсутствует включенное правило, которое разрешает сетевое взаимодействие между устройствами, отобразится запрос на создание соответствующего правила по технологии Контроль целостности сети. В этом случае рекомендуется создать дополнительное правило вместе с текущим создаваемым правилом. Для этого подтвердите решение в окне запроса и выполните действия по созданию нового правила по технологии Контроль целостности сети.

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 (см. раздел "Поддерживаемые устройства и протоколы" на стр. [153](#)).

- b. Нажмите на кнопку **ОК**.

Если выбран протокол, который программа может определять по содержимому сетевых пакетов, ниже поля **Протокол** появится пояснение об этом.

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**.

Для автоматического заполнения адресной информации стороны сетевого взаимодействия по сведениям об устройствах выполните следующие действия:

- a. Откройте окно выбора устройств по ссылке **Указать адреса устройств**.
- b. В окне выбора устройств установите флажки напротив тех устройств, которые вы хотите использовать.

Окно выбора устройств содержит таблицу, в которой можно настраивать отображение и порядок граф, выполнять фильтрацию, поиск и сортировку аналогично таблице устройств (см. раздел "Просмотр таблицы устройств" на стр. [265](#)) в разделе **Активы**.

- c. В окне выбора устройств нажмите на кнопку **ОК**.

- Создание нового правила на основе имеющегося правила

► *Чтобы создать новое правило контроля взаимодействий на основе имеющегося правила, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Разрешающие правила** выберите правило, на основе которого вы хотите создать новое правило.
3. По правой 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 4–9, описанные в процедуре создания правила с изначально пустыми значениями параметров.

- Создание правила на основе события, зарегистрированного по технологии Контроль целостности сети или Контроль системных команд

► *Чтобы создать новое правило контроля взаимодействий на основе зарегистрированного события, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **События**.
3. В таблице зарегистрированных событий выберите событие, на основе которого вы хотите создать правило контроля взаимодействий.

В правой части окна веб-интерфейса появится область деталей.

4. В области деталей нажмите на кнопку **Создать разрешающее правило**.

В окне браузера откроется раздел **Разрешающие правила**. В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила. Для параметров нового правила будут заданы значения, полученные из сохраненных сведений о событии.

5. При необходимости измените параметры нового правила. Для этого выполните пункты 4–9, описанные в процедуре создания правила с изначально пустыми значениями параметров. Если изменять параметры нового правила не требуется, сохраните правило с помощью кнопки **Сохранить**.

Изменение параметров правила контроля взаимодействий

Вы можете изменять параметры включенного правила контроля взаимодействий. Для выключенных правил возможность изменения недоступна.

- ▶ *Чтобы изменить параметры правила контроля взаимодействий, выполните следующие действия:*
 1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
 2. В разделе **Разрешающие правила** выберите нужное правило типа NIC или CC для изменения параметров.
В правой части окна веб-интерфейса появится область деталей.
 3. Нажмите на кнопку **Изменить**.
 4. Измените нужные параметры (см. раздел "Создание правил контроля взаимодействий вручную" на стр. [197](#)).

См. также

Создание правил контроля взаимодействий вручную[197](#)

Включение и выключение правил контроля взаимодействий

Правила контроля взаимодействий могут находиться в состояниях *Включено* или *Выключено*. По умолчанию после создания правила включены.

Вы можете выключить те правила, которые не должны использоваться при работе технологий контроля взаимодействий в режиме наблюдения (см. раздел "Режим наблюдения для технологий контроля взаимодействий" на стр. [188](#)).

- ▶ *Чтобы изменить состояние правил контроля взаимодействий, выполните следующие действия:*
 1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
 2. В разделе **Разрешающие правила** выберите правила контроля взаимодействий (см. раздел "Выбор правил контроля взаимодействий в таблице разрешающих правил" на стр. [196](#)), для которых вы хотите изменить состояние.
В правой части окна веб-интерфейса появится область деталей.
 3. Включите или выключите правила с помощью кнопок **Включить** и **Выключить**. Каждая из этих кнопок отображается, если среди выбранных правил есть правила, с которыми можно выполнить соответствующую операцию.

Если выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000, программа не проверяет состояние правил. В этом случае в области деталей отображаются обе кнопки для изменения состояния правил.

Удаление правил контроля взаимодействий

Вы можете выборочно удалить одно или несколько правил контроля взаимодействий. Удаленные правила перестают действовать при работе технологий контроля взаимодействий как в режиме наблюдения (см. раздел "Режим наблюдения для технологий контроля взаимодействий" на стр. [188](#)), так и в режиме обучения (см. раздел "Режим обучения для технологий контроля взаимодействий" на стр. [187](#)).

► *Чтобы удалить правила контроля взаимодействий, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Разрешающие правила**.
3. В таблице правил выберите правила контроля взаимодействий (см. раздел "Выбор правил контроля взаимодействий в таблице разрешающих правил" на стр. [196](#)), которые вы хотите удалить.

В правой части окна веб-интерфейса появится область деталей.

4. Нажмите на кнопку **Удалить**.

Откроется окно с запросом подтверждения. В зависимости от состояния выбранных правил, в запросе будут предложены следующие варианты действий:

- Если все выбранные правила включены, программа предлагает удалить выбранные правила, выключить их или отменить операцию. Это условие не проверяется, если выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000.
- Если среди выбранных правил присутствуют выключенные правила или выбраны все правила, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных правил более 1000, программа предлагает удалить выбранные правила или отменить операцию.

5. В окне запроса подтвердите удаление правил.

Настройка обнаружения вторжений

Для обнаружения вторжений в трафике промышленной сети вы можете использовать правила обнаружения вторжений и дополнительные методы обнаружения вторжений по встроенным алгоритмам. При обнаружении в трафике признаков атак Kaspersky Industrial CyberSecurity for Networks регистрирует события по технологии Обнаружение вторжений.

Настройка правил и методов обнаружения вторжений выполняется при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс. Список правил обнаружения вторжений отображается в разделе **Обнаружение вторжений**. Изменять состояния методов обнаружения вторжений вы можете в разделе **Параметры** → **Технологии** (см. раздел "**Управление технологиями**" на стр. [214](#)).

Настройка параметров регистрации событий обнаружения вторжений выполняется в разделе **Параметры** → **Типы событий**.

Вы можете просмотреть события обнаружения вторжений в таблице зарегистрированных событий (см. раздел "Мониторинг событий и инцидентов" на стр. [305](#)).

В этом разделе

Правила обнаружения вторжений.....	203
Дополнительные методы обнаружения вторжений.....	204
Включение и выключение обнаружения вторжений по правилам	205
Включение и выключение дополнительных методов обнаружения вторжений	206
Просмотр таблицы с наборами правил обнаружения вторжений.....	207
Выбор наборов правил обнаружения вторжений	208
Включение и выключение наборов правил обнаружения вторжений.....	209
Загрузка и замена пользовательских наборов правил обнаружения вторжений	209
Удаление пользовательских наборов правил обнаружения вторжений	210

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 (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).
- Пользовательские наборы правил. Эти наборы правил пользователь самостоятельно загружает в программу. Для загрузки нужно использовать файлы, в которых содержатся структуры данных, задающие правила обнаружения вторжений. Файлы для загрузки должны находиться в одной директории и иметь расширение rules. Имена пользовательских наборов правил совпадают с именами файлов, из которых были загружены эти наборы правил.

Программа поддерживает применение не более чем 50000 правил суммарно во всех загруженных наборах правил. Ограничение количества загруженных наборов правил – не более 100.

Правила, загружаемые из пользовательских наборов правил, могут содержать такие условия для анализа трафика, по которым программа будет регистрировать слишком большое количество событий срабатывания этих правил. При использовании таких правил учитывайте, что в некоторых случаях это может привести к снижению производительности системы обнаружения вторжений.

Наборы правил обнаружения вторжений могут быть включены или выключены. Правила из включенного набора применяются при анализе трафика, если включен метод обнаружения вторжений по правилам. Если набор правил выключен, правила из этого набора не применяются.

При загрузке набора правил программа выполняет проверку содержащихся в нем правил. Если в проверяемых правилах обнаружены ошибки, программа блокирует применение этих правил. Если обнаружены ошибки во всех правилах набора или набор не содержит правил, программа выключает этот набор правил.

Сведения о наборах правил и обнаруженных ошибках вы можете просмотреть в разделе **Обнаружение вторжений**.

При обнаружении в трафике условий, заданных в правиле из включенного набора, программа регистрирует событие срабатывания правила. Для регистрации используются системные типы событий (см. раздел "Системные типы событий по технологии Обнаружение вторжений" на стр. [416](#)), которым присвоены следующие коды:

- 4000003000 – для события при срабатывании правила из системного набора правил;
- 4000003001 – для события при срабатывании правила из пользовательского набора правил.

Пользовательские наборы правил могут содержать правила, полученные из других систем обнаружения и предотвращения вторжений. При обработке таких правил программа не выполняет заданные в них действия, применяющиеся по отношению к сетевым пакетам (например, действия `drop` и `reject`). В результате срабатывания правил обнаружения вторжений в Kaspersky Industrial CyberSecurity for Networks выполняется только регистрация событий.

Уровни важности событий Kaspersky Industrial CyberSecurity for Networks соответствуют значениям приоритетов в правилах обнаружения вторжений (см. таблицу ниже).

Таблица 3. 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 (см. раздел «Системные типы событий по технологии Обнаружение вторжений» на стр. [416](#)), 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 (см. раздел «Системные типы событий по технологии Обнаружение вторжений» на стр. [416](#)), 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 (см. раздел «Системные типы событий по технологии Обнаружение вторжений» на стр. [416](#)), 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

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **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

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **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

Таблица с наборами правил обнаружения вторжений отображается в разделе **Обнаружение вторжений** веб-интерфейса программы. При просмотре таблицы с наборами правил вы можете использовать следующие функции:

- Фильтрация по графам таблицы

► *Чтобы отфильтровать таблицу с наборами правил по графе **Имя набора правил**, выполните следующие действия:*

1. В разделе **Обнаружение вторжений** нажмите на значок фильтрации в графе **Имя набора правил**.
Откроется окно фильтрации.
2. В полях **Включая** и **Исключая** введите имена наборов 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 таблицу с наборами правил по графе **Источник, Состояние или Правила**, выполните следующие действия:*

1. В разделе **Обнаружение вторжений** нажмите на значок фильтрации в нужной графе.
Откроется окно фильтрации.
2. Установите флажки напротив значений, по которым вы хотите выполнить фильтрацию.
3. Нажмите на кнопку **ОК**.

- Поиск наборов правил

► *Чтобы найти нужные наборы правил обнаружения вторжений,*

*в разделе **Обнаружение вторжений** введите поисковый запрос в поле **Поиск наборов правил**. Поиск инициируется во время ввода символов.*

В таблице с наборами правил обнаружения вторжений отобразятся наборы, которые удовлетворяют условиям поиска.

*Поиск выполняется по графе **Имя набора правил**.*

- Сортировка наборов правил

► *Чтобы отсортировать наборы правил обнаружения вторжений, выполните следующие действия:*

1. В разделе **Обнаружение вторжений** 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.

Выбор наборов правил обнаружения вторжений

В таблице наборов правил обнаружения вторжений вы можете выбирать нужные наборы правил для выполнения действий с ними.

► *Чтобы выбрать нужные наборы правил обнаружения вторжений, выполните одно из следующих действий:*

- Если вы хотите выбрать один набор правил, установите флажок напротив этого набора или выберите набор с помощью мыши.
- Если вы хотите выбрать несколько наборов правил, установите флажки напротив нужных наборов или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**.
- Если вы хотите выбрать все наборы правил, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:
 - выберите любой набор правил в таблице и нажмите комбинацию клавиш **CTRL+A**;
 - установите флажок в заголовке левой крайней графы таблицы.

В заголовке левой крайней графы таблицы отображается флажок выбора наборов правил. В зависимости от количества выбранных наборов правил флажок может быть в одном из следующих состояний:

- – в таблице не выполнялся выбор всех наборов правил, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбран один набор или несколько наборов с помощью флажков напротив наборов правил или с использованием клавиш **CTRL** или **SHIFT**.
- – в таблице выбраны все наборы правил, удовлетворяющие текущим параметрам фильтрации и поиска.
- – в таблице были выбраны все наборы правил, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых наборов были сняты флажки. Это состояние сохраняется и в случае, если флажки сняты для всех наборов правил, выбранных таким способом (из-за того, что количество выбранных наборов может измениться).

Если выбраны все наборы правил, удовлетворяющие параметрам фильтрации и поиска, количество выбранных наборов может автоматически изменяться. Например, состав наборов правил в таблице может быть изменен пользователем программы в другом сеансе подключения.

Включение и выключение наборов правил обнаружения вторжений

Наборы правил обнаружения вторжений могут находиться в состояниях *Включено* или *Выключено*. Если набор правил выключен, все правила этого набора не используются при обнаружении вторжений.

При включении или выключении выбранных наборов правил на всех компьютерах с установленными компонентами программы (Сервере и сенсорах) выполняется перезапуск системы обнаружения вторжений. Перезапуск необходим для применения изменений.

Изменять состояния наборов правил обнаружения вторжений могут только пользователи с ролью Администратор.

► *Чтобы изменить состояние наборов правил обнаружения вторжений, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Обнаружение вторжений** выберите наборы правил (см. раздел "Выбор наборов правил обнаружения вторжений" на стр. [208](#)), для которых вы хотите изменить состояние.
3. По правой клавише мыши откройте контекстное меню.
4. В контекстном меню выберите один из следующих пунктов:
 - **Включить**, если вы хотите включить все выключенные наборы правил из числа выбранных.
 - **Выключить**, если вы хотите выключить все включенные наборы правил из числа выбранных.
 - **Переключить состояние выбранных наборов правил**, если для всех выбранных наборов правил вы хотите одновременно инвертировать их состояние. Этот вариант позволяет быстрее включить и выключить выбранные наборы правил с разными состояниями на всех компьютерах с установленными компонентами программы (так как для применения изменений будет выполнен только один перезапуск системы обнаружения вторжений на этих компьютерах).

Откроется окно с запросом подтверждения.

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

Загрузка и замена пользовательских наборов правил обнаружения вторжений

Вы можете загрузить в программу наборы правил обнаружения вторжений из файлов. Для загрузки в программу файлы с описаниями правил обнаружения вторжений должны находиться в одной папке и иметь расширение rules. Имена файлов не должны содержать следующие символы: \ / : * ? , " < > |.

После загрузки из файла правила обнаружения вторжений сохраняются в программе в качестве пользовательского набора правил. Имя набора правил совпадает с именем файла, из которого этот набор был загружен.

При загрузке наборов правил из файлов текущие пользовательские наборы правил удаляются из таблицы и заменяются новыми. При этом системные наборы правил (для которых в 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. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Обнаружение вторжений**.
3. По ссылке **Заменить пользовательские правила** в панели инструментов вызовите окно для выбора папки с файлами правил обнаружения вторжений.
4. При появлении окна запроса нажмите на кнопку **ОК**.
5. В стандартном окне используемого браузера выберите папку, в которой содержатся нужные файлы, и нажмите на кнопку пересылки файлов из этой папки.

В таблице с наборами правил отобразятся новые пользовательские наборы правил. Для этих наборов правил в графе **Источник** будет указано значение **Пользователь**. Все наборы правил, в которых не обнаружены ошибки, будут включены.

6. Проверьте наличие ошибок в правилах загруженных наборов правил.

Сведения об обнаруженных ошибках отображаются в графе **Правила**. При отсутствии ошибок отображается статус **ОК**. Если набор правил содержит ошибки, вы можете просмотреть подробные сведения о них по ссылке **Подробнее**. Вы можете изменить состояние (см. раздел "Включение и выключение наборов правил обнаружения вторжений" на стр. [209](#)) наборов правил, для которых отображается статус *Ошибки в некоторых правилах*.

Удаление пользовательских наборов правил обнаружения вторжений

Вы можете удалить все пользовательские наборы правил обнаружения вторжений, которые были загружены в программу из файлов. Возможность выборочного удаления пользовательских наборов правил недоступна. Если вы хотите использовать в программе только некоторые из имеющихся наборов правил, вы можете скопировать файлы с этими наборами в отдельную папку и заменить все пользовательские наборы правил (см. раздел "Загрузка и замена пользовательских наборов правил обнаружения вторжений" на стр. [209](#)) на наборы правил из этой папки.

Удалять пользовательские наборы правил обнаружения вторжений могут только пользователи с ролью Администратор.

► *Чтобы удалить пользовательские наборы правил обнаружения вторжений, выполните следующие действия:*

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

3. Запустите удаление пользовательских наборов правил по ссылке **Удалить пользовательские правила** в панели инструментов.

Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **ОК**.

Все пользовательские наборы правил обнаружения вторжений будут удалены из таблицы.

Управление журналами

Этот раздел содержит информацию об управлении журналами Kaspersky Industrial CyberSecurity for Networks.

Управлять журналами Kaspersky Industrial CyberSecurity for Networks могут только пользователи с ролью Администратор.

В этом разделе

Управление параметрами хранения журналов в базе данных Сервера	211
Управление параметрами сохранения трафика в базе данных Сервера	212
Включение и выключение аудита действий пользователей.....	213
Изменение уровней ведения журналов работы процессов	213

Управление параметрами хранения журналов в базе данных Сервера

Вы можете изменить параметры хранения записей журналов в базе данных Сервера (см. раздел “О журналах” на стр. [82](#)).

► *Чтобы изменить параметры хранения журналов в базе данных Сервера, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Развертывание**.
3. Выберите карточку Сервера.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.

5. В блоках параметров **События**, **Записи аудита** и **Сообщения программы** настройте следующие параметры:
 - а. С помощью параметра **Объем** задайте ограничение занимаемого объема для хранения записей. Вы можете выбрать единицу измерения для указанного значения: **МБ** или **ГБ**.

При изменении значения параметра обратите внимание на оцениваемое максимальное количество записей для указанного объема. Также вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.
 - б. При необходимости с помощью параметра **Время хранения (дней)** включите ограничение на минимальное время хранения записей и укажите нужное количество дней для хранения.
6. Нажмите на кнопку **Сохранить**.

См. также

Изменение параметров хранения данных программы на узле[88](#)

Управление параметрами сохранения трафика в базе данных Сервера

Программа может сохранять трафик, полученный на момент регистрации событий. Трафик сохраняется в базе данных Сервера при регистрации событий, для которых включено сохранение трафика (см. раздел "Настройка автоматического сохранения трафика для системных типов событий" на стр. [230](#)). Также программа может сохранять трафик в базе данных Сервера непосредственно при запросе на загрузку трафика (см. раздел "Загрузка трафика для событий" на стр. [328](#)), используя временные файлы дампа трафика.

Программа сохраняет данные о трафике блоками. Если блок трафика относится к нескольким событиям (когда события регистрируются в коротком промежутке времени), этот блок трафика не дублируется в базе данных.

► *Чтобы изменить параметры сохранения трафика в базе данных Сервера, выполните следующие действия:*

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

В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. В блоке параметров **Трафик для событий** задайте ограничение занимаемого объема для хранения трафика с помощью параметра **Объем**.

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

При изменении значения параметра вам нужно учитывать, что сумма всех ограничений по объему не может превышать заданный максимальный объем хранилища для узла.
6. Нажмите на кнопку **Сохранить**.

См. также

Изменение параметров хранения данных программы на узле[88](#)

Включение и выключение аудита действий пользователей

Вы можете включать и выключать аудит действий пользователей программы.

По умолчанию аудит действий пользователей включен.

► *Чтобы включить или выключить аудит действий пользователей, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Аудит**.
3. Включите или выключите аудит действий пользователей с помощью переключателя **Аудит действий пользователей** в панели инструментов.
4. Дождитесь применения изменений. До завершения перевода в другое состояние переключатель недоступен.

Изменение уровней ведения журналов работы процессов

На узлах с установленными компонентами программы выполняются служебные процессы, которые могут сохранять данные о своей работе в журналах в локальных директориях (см. раздел “Директории для хранения данных программы” на стр. [80](#)). Вы можете управлять сохранением данных в журналах работы следующих процессов программы:

- На компьютере, который выполняет функции Сервера:
 - EntityManager.
 - Filter.
 - KisClient.
 - NetworkDumper.
 - ProductServer.
 - Watchdog.
 - WebServer.
- На компьютере, который выполняет функции сенсора:
 - EntityManager.
 - Filter.
 - NetworkDumper.
 - Watchdog.

Для каждого процесса вы можете задать один из следующих уровней ведения журнала:

- **Выкл.** В журнале не сохраняются данные о работе процесса.
- **Ошибки.** В журнале сохраняются только данные об ошибках, возникших в работе процесса.
- **Важные.** В журнале сохраняются данные уровня **Ошибки** и данные, на которые нужно обратить внимание.
- **Инфо.** В журнале сохраняются данные уровня **Важные** и информация справочного характера.
- **Отладка.** В журнале сохраняются данные уровня **Инфо** и все данные о работе процесса, которые могут потребоваться в процессе отладки программы (например, сведения о производительности процесса).

Необходимость изменить уровни ведения журналов может возникнуть, например, при обращении в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. [370](#)).

Изменять уровни ведения журналов могут только пользователи с ролью Администратор.

► *Чтобы изменить уровни ведения журналов для процессов Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Ведение журналов**.
3. Измените уровни ведения журналов в зависимости от нужного результата:
 - Если вы хотите задать одинаковый уровень ведения журналов для всех процессов на всех узлах, нажмите на заголовок графы с названием нужного уровня.
 - Если вы хотите задать одинаковый уровень ведения журналов для всех процессов на одном из узлов, нажмите на ячейку графы с названием нужного уровня в строке с именем узла.
 - Если вы хотите для одного процесса задать уровень ведения журнала, отличающийся от заданных уровней для других процессов, раскройте список процессов нужного узла в графе **Узлы и процессы** и нажмите на ячейку графы с названием нужного уровня в строке с именем процесса.
4. Дождитесь применения изменений (до применения изменений отображается индикатор выполнения).

Управление технологиями

В Kaspersky Industrial CyberSecurity for Networks вы можете включать и выключать использование технологий и методов, относящихся к технологиям. Также вы можете изменять режим работы технологий и методов, для которых доступна такая возможность. Управлять технологиями могут только пользователи с ролью Администратор.

Включение и выключение поддерживается для следующих технологий и методов:

- Контроль активов (см. раздел "Настройка контроля активов" на стр. [120](#)):
 - Обнаружение активности устройств.
 - Обнаружение сведений об устройствах.

- Контроль проектов ПЛК.
- Обнаружение уязвимостей устройств.
- Контроль сети (см. раздел "Настройка контроля взаимодействий" на стр. [185](#)):
 - Контроль целостности сети.
 - Контроль системных команд.
- Контроль процесса (см. раздел "Настройка контроля процесса" на стр. [152](#)):
 - Контроль процесса по правилам.
 - Обнаружение неизвестных тегов.
 - Обнаружение устройств для контроля процесса.
- Обнаружение вторжений (см. раздел "Настройка обнаружения вторжений" на стр. [202](#)):
 - 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:

- Обнаружение активности устройств.
- Контроль системных команд.
- Контроль процесса по правилам.
- Контроль целостности сети.

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-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **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 (см. раздел "Просмотр статуса сервисов, обеспечивающих работу компонентов программы" на стр. [107](#)). Если сервис не активен, требуется его запустить.

3. Включите или выключите применение нужных технологий и / или методов с помощью переключателей слева. Вы можете включить или выключить все технологии и методы одновременно по ссылкам **Включить все** и **Выключить все**.
4. После включения или выключения технологии или метода дождитесь применения изменений. До завершения перевода в другое состояние переключатель недоступен.
5. Для технологий и методов, поддерживающих работу в режиме обучения (**Обнаружение активности устройств, Контроль системных команд, Контроль процесса по правилам и Контроль целостности сети**), выберите нужный режим. Если вы хотите выбрать одинаковый режим для всех этих технологий и методов, используйте раскрывающийся список **Режим**.

Если требуется выбрать разные режимы (**Обучение и Наблюдение**), используйте раскрывающийся список справа от названия технологии или метода. В этом случае раскрывающийся список **Режим** будет отображать значение **Смешанный**.

6. После выбора режима дождитесь применения изменений. До применения режима в раскрывающемся списке отображается статус *Изменение*.

Управление коннекторами

Этот раздел содержит информацию об управлении коннекторами в Kaspersky Industrial CyberSecurity for Networks. *Коннекторы* – это специальные программные модули, которые обеспечивают обмен данными Kaspersky Industrial CyberSecurity for Networks со сторонними системами, в том числе с Kaspersky Security Center.

С помощью коннекторов вы можете настроить отправку событий, сообщений программы или записей аудита в стороннюю систему (например, в SIEM-систему). Также коннекторы могут обеспечивать получение различных данных от сторонних систем (например, регистрировать события по технологии Внешние системы).

Максимальное количество коннекторов в программе – не более 20.

В программе могут использоваться системные и пользовательские типы коннекторов.

Системные типы коннекторов встроены в программу. Предусмотрены следующие системные типы коннекторов:

- **Syslog** – для отправки данных на сервер Syslog.
- **SIEM** – для отправки данных на сервер SIEM-системы.
- **Email** – для отправки данных в сообщениях электронной почты.
- **Generic** – для подключения приложений, использующих Kaspersky Industrial CyberSecurity for Networks API (см. раздел "Использование Kaspersky Industrial CyberSecurity for Networks API" на стр. [240](#)).

При необходимости в программу можно добавлять пользовательские типы коннекторов, которые будут обеспечивать обмен данными с другими сторонними системами. Для добавления пользовательских типов коннекторов вам нужно использовать скрипт `types_manager.py`, находящийся на компьютере Сервера в директории `/opt/kaspersky/kics4net-connectors/sbin/`.

Подключение сторонней системы через коннектор выполняется от имени одного из пользователей программы. Для каждого коннектора рекомендуется использовать отдельную учетную запись пользователя. За счет этого вам будет удобнее анализировать действия, которые выполнялись через коннекторы, по записям аудита.

В Kaspersky Industrial CyberSecurity for Networks действует ограничение на количество одновременно открытых сеансов подключения к Серверу для одного и того же пользователя программы. При подключении через коннектор пользователь, от имени которого выполнено подключение, не сможет подключаться к Серверу (и продолжать работу) через веб-интерфейс.

Также в программе предусмотрен специальный коннектор **Kaspersky Security Center Connector**. Этот коннектор обеспечивает взаимодействие программы с Kaspersky Security Center (на стр. [354](#)). Коннектор **Kaspersky Security Center Connector** создается в программе по умолчанию и не может быть удален. Для работы коннектора требуется добавить на Сервер Kaspersky Industrial CyberSecurity for Networks функциональность взаимодействия программы с Kaspersky Security Center.

Управлять коннекторами могут только пользователи с ролью Администратор.

В этом разделе

Об отправке событий, сообщений программы и записей аудита в сторонние системы.....	217
Добавление коннектора	218
Просмотр таблицы коннекторов	220
Включение и выключение коннекторов	223
Изменение параметров коннектора	223
Создание нового файла свертки для коннектора	224
Удаление коннекторов.....	225

Об отправке событий, сообщений программы и записей аудита в сторонние системы

Вы можете настроить отправку событий, сообщений программы или записей аудита (далее также "зарегистрированные уведомления") в стороннюю систему с помощью коннекторов. Для системных типов коннекторов (см. раздел "Управление коннекторами" на стр. [216](#)) **Syslog**, **SIEM** и **Email** возможность отправки зарегистрированных уведомлений включена по умолчанию. При использовании пользовательских типов коннекторов эта возможность доступна в зависимости от заданных параметров для типа коннектора.

Параметры отправки зарегистрированных уведомлений настраиваются для каждого коннектора. При настройке типов событий (см. раздел "Настройка передачи событий через коннекторы" на стр. [231](#)) вы можете выбрать нужные типы событий для передачи через коннекторы. При создании коннектора (см. раздел "Добавление коннектора" на стр. [218](#)) или при изменении (см. раздел "Изменение параметров коннектора" на стр. [223](#)) его параметров вы можете включить или выключить отправку всех сообщений программы и всех записей аудита через этот коннектор.

Некоторые типы коннекторов предоставляют возможность ограничения объема передаваемых данных. Ограничение действует в течение суток, начиная с нуля часов в часовом поясе Сервера. Вы можете задать ограничение объема передаваемых данных для следующих системных типов коннекторов:

- **Email.** Для этого типа коннектора можно задать максимальное количество сообщений электронной почты о новых зарегистрированных уведомлениях и максимальное количество зарегистрированных уведомлений в каждом сообщении. Если отправлено максимальное количество сообщений электронной почты, получателям отправляется ещё одно сообщение о превышении максимального количества. После этого новые сообщения не будут отправляться до конца текущих суток.
- **Kaspersky Security Center Connector.** Для этого типа коннектора можно задать максимальное количество передаваемых зарегистрированных уведомлений. Если зарегистрированных уведомлений больше, в Kaspersky Security Center не отправляются остальные уведомления, регистрируемые до конца текущих суток.

Передача событий, содержащих сведения о нескольких сетевых взаимодействиях, выполняется со следующей особенностью. При отправке через коннектор каждое такое событие учитывается как один элемент. Однако в процессе отправки событие преобразуется в несколько зарегистрированных уведомлений: по одному уведомлению на каждое сетевое взаимодействие. Поэтому список зарегистрированных уведомлений для коннектора может содержать больше уведомлений, чем задано параметром, который определяет максимальное количество уведомлений.

Содержание и порядок сведений о зарегистрированных уведомлениях, которые передаются через коннекторы типов **Syslog** и **SIEM**, могут отличаться в этих системах от содержания и порядка сведений, отображаемых на страницах веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Сообщения электронной почты, отправляемые через коннектор **Email**, формируются отдельно для каждого типа зарегистрированных уведомлений. То есть для отправки событий, сообщений программы и записей аудита формируются разные сообщения электронной почты.

Добавление коннектора

Перед добавлением коннектора рекомендуется создать отдельную учетную запись пользователя (см. раздел "Создание учетной записи пользователя программы" на стр. [118](#)), под которым сторонняя система будет подключаться к программе.

► *Чтобы добавить коннектор, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. Откройте область деталей по ссылке **Добавить коннектор**.
4. Укажите основные параметры коннектора:
 - Имя пользователя, под которым сторонняя система будет подключаться к программе через коннектор. Требуется указать имя одного из пользователей программы.
 - Адрес узла, на котором будет работать коннектор (для системных типов коннекторов совпадает с адресом компьютера Сервера, если коннектор работает на узле Сервера).

- Пароль для доступа к сертификату коннектора. С использованием заданного пароля будет зашифрован сертификат в файле свертки коннектора.
 - Имя коннектора.
 - Тип коннектора.
 - Описание коннектора.
 - Вариант отправки сообщений программы через коннектор: **Все** или **Не отправляются**.
 - Вариант отправки записей аудита через коннектор: **Все** или **Не отправляются**.
5. Укажите дополнительные параметры в зависимости от типа коннектора.

Для системных типов коннекторов вы можете настроить следующие параметры:

- **SIEM / Syslog:**
 - Адрес сервера.
 - Порт сервера.
 - Протокол передачи данных.
 - **Email:**
 - Адрес, указываемый в качестве отправителя сообщений электронной почты.
 - Адреса получателей сообщений электронной почты.
 - Темы сообщений электронной почты для событий, сообщений программы и записей аудита.
 - Шаблоны текстовых описаний для событий, сообщений программы, записей аудита описаний сетевых взаимодействий и для всего письма с уведомлениями. Шаблоны составляются с использованием переменных (см. раздел "Общие переменные для подстановки значений в Kaspersky Industrial CyberSecurity for Networks" на стр. [232](#)).
 - Тема и текст письма для сообщения электронной почты о достижении максимального количества отправленных уведомлений.
 - Максимальное количество отправляемых сообщений электронной почты в сутки.
 - Максимальное количество уведомлений в каждом сообщении. Определяет максимальное количество зарегистрированных уведомлений одного типа (событий, сообщений программы или записей аудита), которые можно поместить в одно сообщение электронной почты. Если зарегистрированных уведомлений больше, то формируется дополнительное сообщение электронной почты (в пределах суточного ограничения).
6. Нажмите на кнопку **Сохранить**.

Новый коннектор появится в таблице коннекторов. Также в таблице типов событий (см. раздел "Настройка передачи событий через коннекторы" на стр. [231](#)) появится новая графа с именем коннектора.

Одновременно Сервер сформирует файл свертки для нового коннектора, после чего браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

Содержимое полученного файла свертки вам нужно загрузить в приложение, которое будет использовать коннектор.

7. Создайте службу коннектора на Сервере с помощью скрипта `registrar.py`, который находится на компьютере Сервера в директории `/opt/kaspersky/kics4net-connectors/sbin/`. Запуск скрипта требуется выполнить с параметром `create` (для запуска введите команду: `sudo python3 registrar.py create`). По запросам скрипта последовательно укажите данные о коннекторе: имя коннектора, путь к файлу свертки, пароль для доступа к сертификату коннектора.

См. также

Управление коннекторами	216
Об отправке событий, сообщений программы и записей аудита в сторонние системы.....	217

Просмотр таблицы коннекторов

При просмотре таблицы коннекторов вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице коннекторов

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

1. В разделе **Параметры** → **Коннекторы** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
2. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр (см. ниже).
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 коннекторов.


Для выбора доступны следующие параметры:

- **Имя.**
Заданное имя коннектора.
- **ID коннектора.**
Идентификатор, присвоенный коннектору при его создании.
- **Включен.**
Признак включенного или выключенного состояния коннектора. Если коннектор выключен, подключение через этот коннектор невозможно.
- **Состояние.**
Состояние регистрации коннектора на Сервере. Предусмотрены следующие состояния:
 - *Ожидает регистрации* – после создания файла свертки для коннектора подключение через этот коннектор еще не выполнялось.
 - *Зарегистрирован* – после создания файла свертки для коннектора было выполнено успешное подключение через этот коннектор.Если коннектор выключен, для него отображается состояние *Выключен* независимо от текущего состояния регистрации этого коннектора.
- **Тип.**
Тип коннектора.

- **Последнее подключение.**
Дата и время последнего подключения через коннектор.
- **Изменен.**
Дата и время последнего изменения параметров коннектора.
- **Описание.**
Заданное описание коннектора.
- **Типы событий.**
Сведения об отправляемых типах событий через коннектор:
 - **Все** – для отправки через коннектор выбраны все типы событий.
 - **Выбранные** – для отправки через коннектор выбраны не все типы событий.
 - **Не отправляются** – нет выбранных типов событий для отправки через коннектор.
- **Сообщения программы.**
Сведения об отправляемых сообщениях программы через коннектор:
 - **Все** – все сообщения программы отправляются через коннектор.
 - **Не отправляются** – сообщения программы не отправляются через коннектор.
- **Записи аудита.**
Сведения об отправляемых записях аудита через коннектор:
 - **Все** – все записи аудита отправляются через коннектор.
 - **Не отправляются** – записи аудита не отправляются через коннектор.

- Фильтрация по графам таблицы

► Чтобы отфильтровать коннекторы по графе **Имя** или **ID коннектора**, выполните следующие действия:

1. В разделе **Параметры** → **Коннекторы** нажмите на значок фильтрации в нужной графе таблицы.
Откроется окно фильтрации.
2. В полях **Включая** и **Исключая** введите значения, 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 коннекторы по графе **Включен**, **Состояние**, **Тип**, **Типы событий**, **Сообщения программы** или **Записи аудита**, выполните следующие действия:

1. В разделе **Параметры** → **Коннекторы** нажмите на значок фильтрации в нужной графе таблицы.

Для фильтрации по состояниям или по типам коннекторов 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**.

- Поиск коннекторов

► Чтобы найти нужные коннекторы,

в разделе **Параметры** → **Коннекторы** введите поисковый запрос в поле **Поиск коннекторов**. Поиск инициируется во время ввода символов.

В таблице отобразятся коннекторы, которые удовлетворяют условиям поиска.

Поиск выполняется по графам **Имя**, **Описание** и **Тип**.

- Сброс заданных параметров фильтрации и поиска

► Чтобы сбросить заданные параметры фильтрации и поиска в таблице коннекторов,

в разделе **Параметры** → **Коннекторы** нажмите на кнопку **Фильтр по умолчанию** в панели инструментов (кнопка отображается, если заданы параметры фильтрации и / или поиска).

- Сортировка коннекторов

► *Чтобы отсортировать коннекторы, выполните следующие действия:*

1. В разделе **Параметры** → **Коннекторы** 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.

Включение и выключение коннекторов

Коннекторы могут быть включены или выключены. Если коннектор выключен, подключение через этот коннектор невозможно.

► *Чтобы включить или выключить коннекторы, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. В таблице коннекторов выберите коннекторы, которые вы хотите включить или выключить.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Включить** или **Выключить**.
Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.

Изменение параметров коннектора

► *Чтобы изменить параметры коннектора, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. В таблице коннекторов выберите нужный коннектор.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Измените нужные значения для основных и дополнительных параметров (см. раздел "Добавление коннектора" на стр. [218](#)) коннектора.
6. Нажмите на кнопку **Сохранить**.

Изменения отобразятся в соответствующих графах таблицы коннекторов. Если вы изменили имя коннектора, новое имя отобразится в заголовке графы в таблице типов событий (см. раздел "Настройка передачи событий через коннекторы" на стр. [231](#)).

При изменении некоторых параметров (например, адрес сервера для коннектора **Syslog**) Сервер сформирует новый файл свертки для коннектора. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла свертки.

Содержимое полученного файла свертки вам нужно загрузить в приложение, которое будет использовать коннектор. Иначе новое подключение через коннектор для этого приложения будет невозможно.

См. также

Об отправке событий, сообщений программы и записей аудита в сторонние системы.....	217
Управление коннекторами	216

Создание нового файла свертки для коннектора

При добавлении коннектора (см. раздел "Добавление коннектора" на стр. [218](#)) автоматически создается файл свертки для этого коннектора. При необходимости вы можете создать для коннектора новый файл свертки (например, если конфигурационный пакет из предыдущего файла свертки был скомпрометирован).

После создания нового файла свертки конфигурационный пакет из старого файла свертки становится недействительным. Поэтому для следующего подключения сторонней системы через коннектор вам потребуется использовать новый файл свертки.

► *Чтобы создать новый файл свертки для коннектора, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. В таблице коннекторов выберите коннектор, для которого вы хотите создать новый файл свертки.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Получить новый файл свертки**.
Откроется окно **Генерация нового файла свертки**.
5. Укажите параметры для создания файла свертки:
 - Имя пользователя, под которым сторонняя система будет подключаться к программе через коннектор. Требуется указать имя одного из пользователей программы.
Рекомендуется указать имя пользователя, которое было указано при добавлении коннектора. Если требуется указать имя другого пользователя, рекомендуется выбрать из учетных записей пользователей программы того пользователя, имя которого не указано для других коннекторов и не используется для подключения к Серверу через веб-интерфейс.
 - Адрес узла, на котором будет работать коннектор.
 - Пароль для доступа к сертификату коннектора. С использованием заданного пароля будет зашифрован сертификат в файле свертки коннектора.
6. Нажмите на кнопку **Создать файл свертки**.

Сервер сформирует новый файл свертки для выбранного коннектора, после чего браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

Содержимое полученного файла свертки вам нужно загрузить в приложение, которое будет использовать коннектор. Иначе новое подключение через коннектор для этого приложения будет невозможно.

Удаление коннекторов

Перед удалением коннекторов вам нужно остановить и удалить службы этих коннекторов на Сервере. Для этого используйте скрипт `registrar.py`, находящийся на компьютере Сервера в директории `/opt/kaspersky/kics4net-connectors/sbin/`. Запуск скрипта требуется выполнить с параметром `delete` (командой `sudo python3 registrar.py delete`). По запросам скрипта укажите имена коннекторов, которые вы хотите удалить.

► *Чтобы удалить коннекторы, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Коннекторы**.
3. В таблице коннекторов выберите коннекторы, которые вы хотите удалить.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Удалить**.
Откроется окно с запросом подтверждения.
5. В окне запроса нажмите на кнопку **ОК**.

Настройка типов событий

В Kaspersky Industrial CyberSecurity for Networks вы можете настраивать типы регистрируемых событий. *Типы событий* задают параметры, используемые при регистрации событий: заголовки, описания, уровни важности и параметры регистрации. Настройка типов событий выполняется при подключении к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс в разделе **Параметры** → **Типы событий**.

Таблица типов событий содержит *системные типы событий* (см. раздел "*Системные типы событий в Kaspersky Industrial CyberSecurity for Networks*" на стр. [414](#)). Эти типы событий создаются программой при установке и не могут быть удалены из списка. Для реализованных в программе технологий регистрации событий используются различные наборы системных типов событий.

На основе некоторых системных типов событий могут быть настроены *пользовательские параметры событий*, которые будут использоваться при регистрации событий в определенных случаях. В частности, пользовательские параметры могут быть заданы для регистрации событий по правилам контроля процесса (см. раздел "*Правила контроля процесса*" на стр. [170](#)), а также для регистрации событий с использованием Kaspersky Industrial CyberSecurity for Networks API (см. раздел "*Использование Kaspersky Industrial CyberSecurity for Networks API*" на стр. [240](#)).

Пользовательские параметры имеют приоритет при регистрации событий. Параметры, заданные в системных типах событий, используются в том случае, если не заданы пользовательские параметры.

Для типов событий предусмотрены следующие параметры:

- **Код** – уникальный номер типа события. В таблице типов событий номер отображается вместе с заголовком события. В таблице зарегистрированных событий номер типа события отображается в графе **Тип события**.
- **Важность** – уровень важности (см. раздел "Уровни важности событий" на стр. [307](#)) для регистрируемого события.
- **Технология** – технология регистрации события (см. раздел "Технологии регистрации событий" на стр. [307](#)).
- **Заголовок** – содержимое заголовка события, представленное текстом и / или переменными. В системных типах событий могут использоваться специфические переменные только для этих типов событий (например, переменная `$systemCommandShort` в типе события по технологии Контроль системных команд (см. раздел "Системные типы событий по технологии Контроль системных команд" на стр. [415](#))) или общие переменные (см. раздел "Общие переменные для подстановки значений в Kaspersky Industrial CyberSecurity for Networks" на стр. [232](#)), которые также можно использовать и в пользовательских параметрах (например, переменная `$stop_level_protocol` в типе события по технологии Контроль целостности сети (см. раздел "Системные типы событий по технологии Контроль целостности сети" на стр. [415](#))). В таблице типов событий содержимое заголовка отображается после номера типа события. В таблице зарегистрированных событий текст заголовка и / или полученные значения переменных отображаются в графе **Заголовок**.
- **Описание** – дополнительный текст, описывающий тип события. Аналогично заголовку, может содержать переменные. Этот параметр не отображается в таблице типов событий (вы можете посмотреть описание в области деталей выбранного типа события). В таблице зарегистрированных событий текст описания и / или полученные значения переменных отображаются в графе **Описание**.
- **<Имя коннектора-получателя>** – имя коннектора (см. раздел "Об отправке событий, сообщений программы и записей аудита в сторонние системы" на стр. [217](#)), через который программа передает события в стороннюю систему. Программа передает в сторонние системы события только тех типов, для которых включена передача событий через коннектор.
- **Время разрешения повтора** – максимальный период времени, по истечении которого разрешается повторная регистрация события. Если до истечения заданного периода времени повторяются условия для регистрации события, то новое событие не регистрируется, а увеличивается счетчик количества повторов ранее зарегистрированного события и обновляются дата и время последнего появления события. После окончания этого периода при повторении условий для регистрации события программа регистрирует новое событие такого типа. Период разрешения повтора отсчитывается от момента последней регистрации события такого типа. Например, если задано время 8 часов, то при обнаружении условий для регистрации этого события через два часа после предыдущего события, новое событие не будет зарегистрировано. Новое событие будет зарегистрировано при обнаружении условий для регистрации через 8 часов и более. Этот параметр не отображается в таблице типов событий (вы можете посмотреть и настроить этот параметр в области деталей выбранного типа события).

Для зарегистрированных событий время разрешения повтора может наступить раньше заданного периода. Повторная регистрация события разрешается раньше заданного периода, если событию присвоен статус *Обработано*, а также если был перезагружен компьютер, который выполняет функции Сервера.

- **Сохранять трафик** – параметр для включения / выключения автоматического сохранения трафика (см. раздел "Настройка автоматического сохранения трафика для системных типов событий" на стр. [230](#)) при регистрации события. Этот параметр не отображается в таблице типов событий (вы можете просмотреть и настроить этот параметр в области деталей выбранного типа события).

Если автоматическое сохранение трафика выключено, вы можете загружать трафик вручную (см. раздел "Загрузка трафика для событий" на стр. [328](#)) 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).

В этом разделе

Просмотр таблицы типов событий	227
Выбор типов событий в таблице	229
Изменение параметров системного типа события	230
Настройка автоматического сохранения трафика для системных типов событий.....	230
Настройка передачи событий через коннекторы	231
Общие переменные для подстановки значений в Kaspersky Industrial CyberSecurity for Networks.....	232

Просмотр таблицы типов событий

При просмотре таблицы типов событий вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице типов событий

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

1. В разделе **Параметры** → **Типы событий** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
2. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр (см. ниже).
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 типов событий.

Для выбора доступны следующие параметры:

- **Код и заголовок.**

Номер типа события и содержимое заголовка.

- **Важность.**

Уровень важности для типа события.

- **Технология.**

Технология для типа события.

- **<Имя коннектора-получателя>.**

Имя коннектора, через который программа передает события в стороннюю систему. Если графа с именем коннектора отображается в таблице типов событий, в этой графе отмечены те типы событий, для которых включена передача событий через этот коннектор (см. раздел "Настройка передачи событий через коннекторы" на стр. [231](#)).

- Фильтрация по графам таблицы

► *Чтобы отфильтровать типы событий по графе **Важность** или **Технология**, выполните следующие действия:*

1. В разделе **Параметры** → **Типы событий** нажмите на значок фильтрации в нужной графе таблицы.

Для 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. Вы можете снять или удалить все флажки по ссылке, которая отображается в верхней части окна фильтрации.

3. Нажмите на кнопку **ОК**.

- Поиск типов событий

► *Чтобы найти нужные типы событий,*

в разделе **Параметры** → **Типы событий** введите поисковый запрос в поле **Поиск типов событий**. Поиск инициируется во время ввода символов.

В таблице отобразятся типы событий, которые удовлетворяют условиям поиска.

Поиск выполняется по всем графам, кроме граф **Важность** и **Технология**.

- Сортировка типов событий

► *Чтобы отсортировать типы событий, выполните следующие действия:*

1. В разделе **Параметры** → **Типы событий** 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.

Выбор типов событий в таблице

В таблице типов событий вы можете выбирать типы событий для просмотра сведений и для настройки параметров. При выборе типов событий в правой части окна веб-интерфейса появляется область деталей.

► *Чтобы выбрать нужные типы событий в таблице, выполните одно из следующих действий:*

- Если вы хотите выбрать один тип события, установите флажок напротив этого типа события или выберите его с помощью мыши.
- Если вы хотите выбрать несколько типов событий, установите флажки напротив нужных типов событий или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**.
- Если вы хотите выбрать все типы событий, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:
 - выберите любой тип события в таблице и нажмите комбинацию клавиш **CTRL+A**;
 - установите флажок в заголовке левой крайней графы таблицы.

При выборе нескольких типов событий в области деталей отображается общее количество выбранных типов событий.

В заголовке левой крайней графы таблицы отображается флажок выбора типов событий. В зависимости от количества выбранных типов событий флажок может быть в одном из следующих состояний:

- – в таблице не выполнялся выбор всех типов событий, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбран один тип события или несколько типов событий с помощью флажков напротив типов событий или с использованием клавиш **CTRL** или **SHIFT**.
- – в таблице выбраны все типы событий, удовлетворяющие текущим параметрам фильтрации и поиска.
- – в таблице были выбраны все типы событий, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых типов событий были сняты флажки.

Изменение параметров системного типа события

► Чтобы изменить параметры системного типа события, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Типы событий**.
3. В таблице типов событий выберите тип события, который вы хотите изменить. Если тип события предусматривает регистрацию событий с несколькими уровнями важности, выберите в таблице строку типа события с нужным уровнем важности.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Настройте изменяемые параметры (см. раздел "Настройка типов событий" на стр. [225](#)): время разрешения повтора события и параметры сохранения трафика.
6. Нажмите на кнопку **Сохранить**.

См. также

Настройка типов событий[225](#)

Настройка автоматического сохранения трафика для системных типов событий

При изменении типов событий (см. раздел "Изменение параметров системного типа события" на стр. [230](#)) вы можете включать и выключать автоматическое сохранение трафика для событий при их регистрации. Если сохранение трафика включено, в базе данных сохраняется сетевой пакет, вызвавший регистрацию события, а также пакеты до и после регистрации события. Параметры сохранения трафика определяют количество сохраняемых сетевых пакетов и ограничения по времени.

Если автоматическое сохранение трафика выключено для типа события (и для этого типа события не заданы пользовательские параметры (см. раздел "Настройка типов событий" на стр. [225](#)), включающие автоматическое сохранение трафика), возможность загрузки трафика будет доступна только в течение некоторого времени после регистрации события этого типа. В этом случае для загрузки трафика (см. раздел "Загрузка трафика для событий" на стр. [328](#)) 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 (см. раздел "Системные типы событий по технологии Контроль целостности сети" на стр. [415](#)). Событие с кодом 4000002700 регистрируется при отсутствии трафика на точке мониторинга, поэтому для этого типа события наличие трафика не предполагается.

Если включено сохранение трафика для инцидентов (то есть для системного типа события, которому присвоен код 8000000001 (см. раздел “Системные типы событий по технологии Внешние системы” на стр. [425](#))), то при регистрации инцидента программа сохраняет трафик для всех вложенных событий инцидента. Для сохранения трафика вложенных событий применяются параметры, заданные для инцидента. При этом параметры сохранения трафика, заданные непосредственно для типов событий, вложенных в инцидент, имеют приоритет перед параметрами, заданными для инцидента. То есть трафик для вложенных событий инцидента будет сохранен в соответствии с параметрами, заданными для типов этих событий, а при отсутствии таких параметров – в соответствии с параметрами, заданными для инцидента.

► Чтобы включить и настроить параметры сохранения трафика для типа события, выполните следующие действия:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Типы событий**.
3. В таблице типов событий выберите тип события, который вы хотите изменить. Если тип события предусматривает регистрацию событий с несколькими уровнями важности, выберите в таблице строку типа события с нужным уровнем важности.
В правой части окна веб-интерфейса появится область деталей.
4. Нажмите на кнопку **Изменить**.
5. Установите переключатель **Сохранять трафик** в положение *Включено*.
6. Настройте сохранение трафика до момента регистрации события. Для этого укажите нужные значения в полях **Пакетов до события** и / или **Миллисекунд до 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.
7. Настройте сохранение трафика после момента регистрации события. Для этого укажите нужные значения в полях **Пакетов после события** и / или **Миллисекунд после 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.

8. Нажмите на кнопку **Сохранить**.

Настройка передачи событий через коннекторы

При настройке системных типов событий вы можете указать коннекторы (см. раздел "Об отправке событий, сообщений программы и записей аудита в сторонние системы" на стр. [217](#)), через которые Kaspersky Industrial CyberSecurity for Networks будет передавать зарегистрированные события в сторонние системы (например, в Kaspersky Security Center). Kaspersky Industrial CyberSecurity for Networks может передавать информацию о событиях одновременно через несколько коннекторов.

► *Чтобы настроить передачу событий через коннекторы в сторонние системы, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Типы событий**.
3. Убедитесь, что в таблице типов событий отображаются графы с нужными коннекторами.
Если графа с нужным коннектором отсутствует, проверьте настройку отображения граф (см. раздел "Просмотр таблицы типов событий" на стр. [227](#)). Если коннектор не был добавлен в список коннекторов, добавьте его (см. раздел "Добавление коннектора" на стр. [218](#)).
4. В таблице типов событий выберите типы событий (см. раздел "Выбор типов событий в таблице" на стр. [229](#)), для которых вы хотите включить или выключить передачу через коннекторы.
В правой части окна веб-интерфейса появится область деталей.
5. Нажмите на кнопку **Выбрать коннекторы**.
Откроется окно **Коннекторы-получатели событий**.
6. Установите флажки напротив тех коннекторов, через которые вы хотите передавать события в сторонние системы.
7. Нажмите на кнопку **ОК**.

Общие переменные для подстановки значений в Kaspersky Industrial CyberSecurity for Networks

Для подстановки текущих значений в Kaspersky Industrial CyberSecurity for Networks могут использоваться общие переменные. Вы можете использовать общие переменные в следующих параметрах:

- заголовки и описания событий в пользовательских параметрах (см. раздел "Настройка типов событий" на стр. [225](#)) для регистрации событий (например, в правилах контроля процесса (см. раздел "Правила контроля процесса" на стр. [170](#)));
- параметры передачи событий, сообщений программы или записей аудита через коннектор для электронной почты (см. раздел "Об отправке событий, сообщений программы и записей аудита в сторонние системы" на стр. [217](#)).

► *Чтобы вставить общую переменную в поле ввода,*

начните вводить имя переменной с символа \$ и выберите подходящую общую переменную в появившемся списке.

В зависимости от своего назначения, общие переменные могут использоваться для подстановки значений в различных параметрах (см. таблицу ниже).

Таблица 4. Общие переменные для подстановки значений

Переменная	Назначение	Где используется
<code>\$communications</code>	Строки описания сетевых взаимодействий (по одной строке на каждое сетевое взаимодействие) с указанием протокола и адресов отправителя и получателя сетевого пакета	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.
<code>\$dst_address</code>	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)	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.
<code>\$extra.<paramName></code>	Дополнительная переменная, добавленная с помощью функции <code>AddEventParam</code> для внешней системы или Lua-скрипта (см. раздел "Правила с Lua-скриптами" на стр. 173)	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.
<code>\$rule_max_value</code>	Заданное максимальное значение в правиле контроля процесса	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.
<code>\$rule_min_value</code>	Заданное минимальное значение в правиле контроля процесса	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.
<code>\$monitoring_point</code>	Имя точки мониторинга, трафик с которой вызвал регистрацию события	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.

<code>§occurred</code>	Дата и время регистрации	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
<code>§protocol</code>	Название протокола прикладного уровня, при отслеживании которого зарегистрировано событие	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.
<code>§src_address</code>	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)	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.
<code>§tags</code>	Список всех имен и значений тегов, указанных в правиле контроля процесса	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.
<code>§technology_rule</code>	Имя правила в событии	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий. • Параметры передачи событий через коннектор.
<code>§top_level_protocol</code>	Название протокола верхнего уровня	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.
<code>§type_id</code>	Код типа события, сообщения программы или записи аудита	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий (также может использоваться переменная <code>§event_type_id</code>). • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
<code>§rule_values</code>	Список значений правила контроля процесса (разрешенных или запрещенных)	<ul style="list-style-type: none"> • Пользовательские параметры для регистрации событий.

\$closed	Дата и время присвоения статуса <i>Обработано</i> или дата и время разрешения повтора события (для событий, не являющихся инцидентами), либо дата и время регистрации последнего события, включенного в инцидент (для инцидентов)	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор.
\$count	Количество срабатываний события или инцидента	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор.
\$description	Описание	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
\$id	Уникальный идентификатор зарегистрированного события, сообщения программы или записи аудита	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
\$message_category	Категория переданных данных (событие, сообщение программы или запись аудита)	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
\$message_count	Количество передаваемых событий, сообщений программы или записей аудита	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
\$messages	Шаблон, представляющий собой блок со списком данных	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.

\$node	Узел с установленным компонентом программы, от которого поступили данные	<ul style="list-style-type: none"> • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
\$result	Результат действия в записи аудита	<ul style="list-style-type: none"> • Параметры передачи записей аудита через коннектор.
\$severity	Уровень важности события	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор.
\$status	Статус сообщения программы	<ul style="list-style-type: none"> • Параметры передачи сообщений программы через коннектор.
\$system_process	Процесс программы, который вызвал регистрацию сообщения	<ul style="list-style-type: none"> • Параметры передачи сообщений программы через коннектор.
\$technology	Технология, к которой относится событие	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор.
\$title	Заголовок события, текст сообщения или зарегистрированное действие	<ul style="list-style-type: none"> • Параметры передачи событий через коннектор. • Параметры передачи сообщений программы через коннектор. • Параметры передачи записей аудита через коннектор.
\$user	Имя пользователя, который совершил зарегистрированное действие	<ul style="list-style-type: none"> • Параметры передачи записей аудита через коннектор.

Управление политикой безопасности

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

- пользовательские наборы правил обнаружения вторжений (см. раздел "Настройка обнаружения вторжений" на стр. [202](#));
- разрешающие правила для контроля взаимодействий (см. раздел "Настройка контроля взаимодействий" на стр. [185](#)) и для событий (см. раздел "Настройка типов событий" на стр. [225](#));
- параметры устройств и тегов, используемые при контроле активов (см. раздел "Настройка контроля активов" на стр. [120](#)) и контроле процесса (см. раздел "Настройка контроля процесса" на стр. [152](#));
- параметры отображения карты сети (см. раздел "Сохранение и загрузка параметров отображения карты сети" на стр. [297](#));
- параметры подсетей (см. раздел "Просмотр подсетей для контроля активов" на стр. [270](#));
- параметры типов событий (см. раздел "Настройка типов событий" на стр. [225](#)).

Остальные параметры работы программы не входят в политику безопасности и применяются отдельно от нее. К таким параметрам относятся параметры узлов с установленными компонентами, список

пользователей программы, объекты, связывающие события и устройства в таблице устройств, и другие параметры.

Политика безопасности хранится на Сервере и автоматически обновляется при каждом изменении параметров работы программы (например, при добавлении правил контроля взаимодействий).

Вы можете экспортировать политику безопасности в файлы и импортировать из файлов. Также вы можете очистить текущую политику безопасности на Сервере, чтобы удалить все ранее сохраненные параметры.

При экспорте, импорте или очистке политики безопасности вы можете выбирать нужные разделы политики, с которыми требуется выполнить операцию. Например, вы можете экспортировать только устройства и разрешающие правила.

В результате экспорта политики безопасности программа создает файл, содержащий информацию о выбранных параметрах работы программы. Для импорта параметров вы можете выбрать ранее экспортированный файл.

Изменение содержимого файла политики безопасности может привести к нарушению работы Kaspersky Industrial CyberSecurity for Networks при импорте политики безопасности из этого файла. Программа может перестать выполнять функции по защите промышленной сети.

В этом разделе

Экспорт политики безопасности в файл.....	237
Импорт политики безопасности из файла.....	238
Очистка текущей политики безопасности.....	239

Экспорт политики безопасности в файл

Вы можете экспортировать в файл параметры, входящие в политику безопасности (см. раздел "Управление политикой безопасности" на стр. [236](#)). Экспорт можно выполнить для всей политики безопасности или для ее отдельных разделов.


В дальнейшем при необходимости вы можете импортировать (см. раздел "Импорт политики безопасности из файла" на стр. [238](#)) нужные параметры работы программы из файла с сохраненной политикой безопасности.

► *Чтобы экспортировать текущую политику безопасности, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс.
2. Выберите раздел **Параметры** → **Политика безопасности**.
3. Нажмите на кнопку **Экспорт**.

Появится дерево разделов политики безопасности, в котором вы можете выбрать нужные разделы для экспорта.

4. Установите флажки для нужных разделов политики безопасности.
5. Нажмите на кнопку **Экспортировать**.

6. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:
 - a. Нажмите на кнопку  в меню веб-интерфейса программы.
Откроется список фоновых операций.
 - b. Дождитесь завершения операции формирования файла.
 - c. Нажмите на кнопку **Загрузить файл**.

Браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

Импорт политики безопасности из файла

Вы можете импортировать параметры работы программы из файла с сохраненной политикой безопасности. Для импорта можно использовать файл, полученный при экспорте политики безопасности (см. раздел "Экспорт политики безопасности в файл" на стр. [237](#)).

При импорте разделов политики безопасности программа предварительно очищает текущее содержимое этих разделов и затем импортирует данные в эти разделы.

Если файл содержит несколько разделов политики безопасности, вы можете выбрать нужные разделы для импорта.

Импорт политики безопасности невозможен, если в текущий момент выполняется установка обновлений или запущен другой процесс импорта.

Импортировать политику безопасности из файла могут только пользователи с ролью Администратор.

► *Чтобы импортировать политику безопасности из файла, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры** → **Политика безопасности**.
3. Нажмите на кнопку **Импорт**.
Откроется стандартное окно используемого браузера для выбора файла.
4. Укажите путь к файлу политики безопасности.
5. Нажмите на кнопку открытия файла.
После проверки содержимого файла появится дерево разделов политики безопасности, доступных для импорта.
6. Установите флажки для тех разделов политики безопасности, которые вы хотите импортировать в программу.
7. Нажмите на кнопку **Импортировать**.

Начнется процесс очистки политики безопасности. До окончания очистки Сервер программы недоступен для подключений. Во время очистки на странице веб-интерфейса программы отображается специальный раздел **Обслуживание программы**.

Очистка текущей политики безопасности

Вы можете очистить текущие параметры, входящие в политику безопасности (см. раздел "Управление политикой безопасности" на стр. [236](#)). Очистку можно выполнить для всей политики безопасности или для ее отдельных разделов.

После очистки политики безопасности некоторые данные будет невозможно восстановить, даже если предварительно был выполнен экспорт политики безопасности. Например, после очистки раздела, содержащего сведения об устройствах, безвозвратно удаляются все объекты, связывающие события и устройства в таблице устройств.

Очистка политики безопасности невозможна, если в текущий момент выполняется установка обновлений или запущен процесс импорта данных.

Очистить политику безопасности могут только пользователи с ролью Администратор.

► *Чтобы очистить политику безопасности, выполните следующие действия:*

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

Появится дерево разделов политики безопасности, в котором вы можете выбрать нужные разделы для очистки.

4. Установите флажки напротив разделов политики безопасности, которые вы хотите очистить.
5. Нажмите на кнопку **Очистить**.

Начнется процесс очистки политики безопасности. До окончания очистки Сервер программы недоступен для подключений. Во время очистки на странице веб-интерфейса программы отображается специальный раздел **Обслуживание программы**.

Использование Kaspersky Industrial CyberSecurity for Networks API

В Kaspersky Industrial CyberSecurity for Networks реализован интерфейс прикладного программирования (Application Programming Interface, далее API), который обеспечивает доступ к функциям программы для сторонних приложений.

В комплект поставки Kaspersky Industrial CyberSecurity for Networks входит пакет с описаниями спецификаций для представления данных в запросах к серверу REST API. *Сервер REST API* функционирует на компьютере Сервера Kaspersky Industrial CyberSecurity for Networks и обрабатывает запросы с использованием архитектурного стиля взаимодействия REST (Representational State Transfer). Обращения к серверу REST API выполняются по протоколу HTTPS. Вы можете настроить параметры сервера REST API в разделе **Параметры** → **Серверы подключений** (в том числе заменить используемый по умолчанию самоподписанный сертификат на доверенный).

Для представления данных в запросах и ответах используется формат JSON.

Документация с описанием запросов на основе архитектурного стиля REST представляет собой руководство разработчика на английском языке. В руководстве разработчика также представлены примеры кода и подробные описания вызываемых элементов, которые доступны в запросах к серверу REST API.

С помощью Kaspersky Industrial CyberSecurity for Networks API сторонние приложения могут выполнять следующие действия:

- получать данные об известных программе устройствах;
- добавлять, изменять и удалять устройства;
- получать данные о зарегистрированных событиях;
- отправлять события в Kaspersky Industrial CyberSecurity for Networks (для регистрации используется системный тип события (см. раздел "Настройка типов событий" на стр. [225](#)) с кодом 4000005400);
- получать данные о списке тегов и о параметрах тегов;
- подписываться на уведомления о полученных значениях тегов;
- получать данные об обнаруженных уязвимостях;
- получать сообщения программы и записи аудита;
- получать следующие данные о программе:
 - список точек мониторинга и их параметры;
 - список поддерживаемых стеков протоколов и их параметры;
 - список типов событий и их параметры;
 - версия программы и даты выпуска установленных обновлений;
 - язык локализации программы.

Сторонние приложения, использующие Kaspersky Industrial CyberSecurity for Networks API, подключаются к Серверу программы через коннекторы (см. раздел "Управление коннекторами" на стр. [216](#)). Коннекторы обеспечивают безопасное соединение с использованием сертификатов. Для каждого стороннего приложения, из которого вы хотите отправлять запросы на сервер REST API, вам нужно создать отдельный коннектор в Kaspersky Industrial CyberSecurity for Networks.

Для соединения с Kaspersky Industrial CyberSecurity for Networks стороннее приложение должно использовать токен аутентификации. Программа выдает токен аутентификации по запросу стороннего приложения и использует для токена сертификаты коннектора, который был создан для этого стороннего

приложения. По умолчанию время действия токена аутентификации составляет 10 часов (вы можете изменять время действия токенов аутентификации с помощью скрипта `kics4net-params.py` (см. раздел "Изменение времени действия для сеансов подключения и токенов аутентификации с помощью скрипта" на стр. [395](#)). Стороннее приложение может обновить токен аутентификации по специальному запросу.

В комплект поставки Kaspersky Industrial CyberSecurity for Networks входит пакет с документацией с описанием запросов для выполнения действий с токеном аутентификации. Документация представляет собой руководство разработчика на английском языке.

В Kaspersky Industrial CyberSecurity for Networks API предусмотрены следующие способы работы со сторонними приложениями:

- взаимодействие на основе архитектурного стиля REST;
- взаимодействие по протоколу WebSocket.

Сторонние приложения могут использовать способ взаимодействия по протоколу WebSocket в Kaspersky Industrial CyberSecurity for Networks API для создания подписок на изменяемые значения, которые получает программа. Например, этот способ взаимодействия позволяет подписываться на уведомления о полученных значениях определенного тега (см. раздел "Подписка на уведомления о значениях тега по протоколу WebSocket" на стр. [243](#)).

В этом разделе

Обеспечение безопасного взаимодействия при использовании Kaspersky Industrial CyberSecurity for Networks API	241
Создание и использование коннекторов для Kaspersky Industrial CyberSecurity for Networks API ...	242
Подписка на уведомления о значениях тега по протоколу WebSocket	243

Обеспечение безопасного взаимодействия при использовании Kaspersky Industrial CyberSecurity for Networks API

Сторонние приложения получают доступ к функциям программы с использованием Kaspersky Industrial CyberSecurity for Networks API, устанавливая зашифрованные соединения по протоколу HTTPS. Для обеспечения безопасности соединений используются сертификаты, выданные Сервером Kaspersky Industrial CyberSecurity for Networks. Сервер выдает сертификаты для коннекторов, через которые подключаются сторонние приложения.

Для каждого стороннего приложения в программе должен быть создан отдельный коннектор. Подключение через коннектор возможно с использованием только того сертификата, который был выдан Сервером и сохранен в файле свертки для этого коннектора. Подключение невозможно установить, если стороннее приложение предъявляет сертификат от другого коннектора, другого Сервера Kaspersky Industrial CyberSecurity for Networks, или сертификат, используемый для других подключений (например, сертификат сенсора).

После установки зашифрованного соединения стороннее приложение должно запросить *токен аутентификации* для коннектора, который будет указываться сторонним приложением в запросах к серверу REST API. Для выдачи токена аутентификации Сервер проверяет текущее состояние учетной записи пользователя программы, которая была указана при создании коннектора. Сервер не выдает токен аутентификации, если учетная запись пользователя программы удалена или заблокирована.

По умолчанию токен аутентификации действителен в течение 10 часов после выдачи Сервером (вы можете изменять время действия токенов аутентификации с помощью скрипта `kics4net-params.py` (см. раздел "Изменение времени действия для сеансов подключения и токенов аутентификации с помощью скрипта" на стр. [395](#))). При необходимости дальнейшего использования токена стороннее приложение должно запросить продление времени его действия до наступления момента прекращения действия.

Сведения о предусмотренных запросах и методах в Kaspersky Industrial CyberSecurity for Networks API см. в документации для Kaspersky Industrial CyberSecurity for Networks API.

В течение времени действия токена аутентификации при поступлении запросов от стороннего приложения Сервер проверяет наличие и текущие права доступа учетной записи пользователя программы, которая была указана при создании коннектора. Метод, указанный в запросе от стороннего приложения, не выполняется, если учетная запись не найдена (удалена из программы) или недостаточно прав для выполнения операции (роль учетной записи не соответствует выполняемой операции).

При обработке запросов от сторонних приложений программа сохраняет в журнале аудита сведения о попытках выполнения следующих операций:

- получение токена аутентификации;
- продление времени действия для токена аутентификации;
- добавление устройства в таблицу устройств;
- изменение сведений об устройстве;
- удаление устройства;
- запрос журнала аудита (при первом чтении записей аудита через коннектор после загрузки веб-сервера).

Создание и использование коннекторов для Kaspersky Industrial CyberSecurity for Networks API

Для взаимодействия стороннего приложения с программой с использованием Kaspersky Industrial CyberSecurity for Networks API вам нужно добавить коннектор (см. раздел "Добавление коннектора" на стр. [218](#)) для этого приложения. При создании коннектора для него требуется указать системный тип (см. раздел "Управление коннекторами" на стр. [216](#)) **Generic**.

При добавлении коннектора, а также при создании нового файла свертки (см. раздел "Создание нового файла свертки для коннектора" на стр. [224](#)) для этого коннектора Сервер формирует файл свертки, который вам нужно использовать для работы коннектора.

Файл свертки представляет собой архив, содержащий следующие файлы:

- `certificates.pfx` – содержит в зашифрованном виде открытый ключ сертификата Сервера, а также сертификат, выданный Сервером для коннектора (с закрытым ключом). Содержимое файла зашифровано с использованием пароля, который был указан при добавлении коннектора или при создании нового файла свертки для этого коннектора.
- `metadata.json` – содержит конфигурационные данные для коннектора. Данные представлены в формате JSON.

Перечисленные файлы вам нужно использовать для подключения стороннего приложения через коннектор. Для расшифровки файла `certificates.pfx` и применения содержащегося в нем сертификата с ключами вы можете использовать стандартные методы обработки файлов этого формата (например, команды `openssl`). Адреса, указанные в файле `metadata.json`, требуются для работы коннектора и отправки запросов к серверу REST API.

Сертификат и конфигурационные данные в файле свертке действительны до тех пор, пока не создан новый файл свертки или пока не удален коннектор в программе.

Подписка на уведомления о значениях тега по протоколу WebSocket

При использовании Kaspersky Industrial CyberSecurity for Networks API стороннее приложение может создавать подписку на уведомления об изменении значений определенного тега. Для создания подписки и получения уведомлений используется протокол WebSocket.

Сценарий подписки для стороннего приложения состоит из следующих этапов:

1. Стороннее приложение устанавливает соединение с Сервером Kaspersky Industrial CyberSecurity for Networks через коннектор для этого приложения с использованием сервера REST API.

После успешного соединения с Сервером коннектору отправляется токен аутентификации. Коннектор использует токен аутентификации для всех последующих взаимодействий с Сервером в этом сеансе (в частности для запроса своей конфигурации с Сервера).

2. Стороннее приложение подключается с использованием WebSocket и отправляет запрос для создания подписки на уведомления о получении значений нужного тега.

Сервер Kaspersky Industrial CyberSecurity for Networks принимает запрос и создает подписку. Для отправки запроса используются соответствующие функции, предусмотренные протоколом WebSocket.

3. Kaspersky Industrial CyberSecurity for Networks обнаруживает в трафике новое значение при чтении или записи тега.
4. Kaspersky Industrial CyberSecurity for Networks отправляет полученное значение тега стороннему приложению, для которого действует подписка на уведомления о получении значений этого тега.

Основные особенности реализации подписки:

- После того, как стороннее приложение указывает нужные теги Kaspersky Industrial CyberSecurity for Networks, Сервер отправляет подтверждение о возможности получать значения этих тегов. Далее стороннее приложение ожидает поступление значений этих тегов по установленному соединению.
- Для создания и сопровождения подписки используется протокол WebSocket и соединение по тому же адресу, который используется сервером REST API.
- Сервер Kaspersky Industrial CyberSecurity for Networks поддерживает не более одной активной подписки на значения тегов. Если активная подписка уже создана и используется, при попытке создания еще одной подписки возвращается ошибка о слишком большом количестве подключений.
- Стороннее приложение имеет возможность в любой момент закрыть установленное соединение по подписке для прекращения получения значений тега.
- Подписка прекращается либо после ее закрытия сторонним приложением, либо при разрыве соединения. Если Сервер Kaspersky Industrial CyberSecurity for Networks был временно недоступен (разорвано соединение) и отправка значений по подписке не выполнялась, то после восстановления соединения стороннему приложению потребуется заново подписаться на получение значений тегов.

Подключение с использованием WebSocket

Для получения тегов по подписке могут использоваться как стандартные функции WebSocket, так и библиотека SignalR Core. Пакеты для работы с библиотекой SignalR Core доступны для наиболее распространенных языков программирования: C++, C#, Java, Python, Go, JavaScript/TypeScript.

Для подключения с использованием WebSocket вам нужно указывать следующий адрес:

```
<адрес publicApi из файла свертки>/kics4net/api/ /v3/tag-values
```

При этом указываемый протокол в строке адреса зависит от используемой функциональности для подключения.

Если используется библиотека SignalR Core, строка адреса начинается с `https://`. Например:
`https://kics-server:8080/kics4net/api/ /v3/tag-values`

Если используются стандартные функции WebSocket, в строке адреса нужно заменить `https` на `wss`.
Например:

```
wss://kics-server:8080/kics4net/api/v3/tag-values
```

Если при подключении не предоставлен токен аутентификации (или предоставленный токен не прошел проверку), в ответ на открытие подключения сервер возвращает код 401.

Создание подписки на значения тегов

Для создания подписки требуется выполнить запрос с именем метода `GetTagValuesStream`.

Пример аргумента запроса:

```
{
  "tagIdentifiers": [
    { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
    { "tagName": "Asdu_1_object_1003", "assetName": "Asset 079" }
  ],
  "streamConfig": {
    "samplingRateHz": 1
  }
}
```

Аргумент запроса состоит из следующих полей:

- `tagIdentifiers` – массив идентификаторов тегов, значения которых нужно получать по подписке.
- `assetName`, `tagName` – значения, представляющие имя устройства и имя тега (используются для идентификации тега, на значения которого нужно создать подписку).
- `samplingRateHz` – частота сэмплирования значений тегов (используется для уменьшения объема передаваемых данных). Если для поля задано нулевое значение, сэмплирование не выполняется.

Если аргумент создания подписки не удовлетворяет требованиям к полям, возвращается ошибка с описанием проблемы.

Пример ошибки для аргумента создания подписки:

```
HubException: GetTagValuesStreamRequest has validation errors:
  TagIdentifiers:
    The TagName field is required.
    The StreamConfig field is required.
```

Подтверждение подписки

При подтверждении подписки сервер возвращает по одному результату подтверждения для каждого тега, подходящего под значения `tagIdentifiers` в запросе.

Пример подтверждения подписки:

```
{
  "confirmation": {
    "result": "ok",
    "tagIdentifier": { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079"
  },
  "tagId": 102
}
```

Ответ с подтверждением подписки состоит из следующих полей:

- `result` – статус подписки на значение тега. Может принимать значения:
 - `ok` – подписка успешно создана;
 - `notFound` – тег с указанными `assetName`, `tagName` не найден.
- `tagIdentifier` – идентификатор тега, аналогичный одному значению из массива `tagIdentifiers` аргументов запроса на создание подписки.
- `tagId` – уникальный идентификатор тега в программе. Может быть использован для получения информации о теге через Kaspersky Industrial CyberSecurity for Networks API, а также для идентификации тега в ответе с его значениями.

Значения тегов по подписке

Программа отправляет значения тегов по подписке в структуре полей. На верхнем уровне в структуре представлены следующие поля:

```
{
  "value": {
    "tagId": <уникальный идентификатор тега в программе>,
    "tagValue": "<JSON-объект с данными тега>"
  }
}
```

Информация о новом значении тега отправляется в стороннее приложение в формате JSON. Отправляемый объект с данными содержит следующие поля:

- `n` – тип данных тега, представленный именем из `TagStructure`.
- `ts` – время регистрации последнего обновления значений тега. Указывается в микросекундах от 01.01.1970.
- `dn` – направление передачи. Может принимать значения: `r`, `w`, `rw`.
- `mp` – идентификатор точки мониторинга.
- `d` – содержимое полей тега.

Атрибут `d` представляет словарь, в котором каждый ключ является именем поля тега нулевой иерархии. Значение каждого поля имеет следующие атрибуты:

- `t` – обязательный атрибут, указывающий один из следующих типов данных:
 - `u` – UINT64.
 - `i` – INT64.
 - `b` – BOOL.
 - `d` – DOUBLE.
 - `s` – строка UTF8.
 - `t` – время в микросекундах от 01.01.1970.
 - `e` – ENUM. Дополнительно поле содержит следующие атрибуты:
 - `n` – имя типа ENUM;
 - `v` – исходное значение ENUM;
 - `s` – строковое значение ENUM.
 - `st` – структура.
 - `un` – UNION.
- `v` – обязательный атрибут, указывающий значение поля тега.
- `n` – имя типа ENUM из `TagStructure` (только для типа `e` – ENUM).
- `s` – строковое значение ENUM (только для типа `e` – ENUM).

Пример:

- enum:

```
name: OpType # Имя типа ENUM (атрибут 'n')
data:
  0: NUL # 0 запишется в атрибут 'v', NUL запишется в 's'
  1: PULSE_ON
  2: PULSE_OFF
```

- `x` – идентифицирует основное значение тега.

Формат: "`x`": 1

Для всех остальных полей тега атрибут `x` отсутствует.

- `m` – специальный маркер параметра тега. Соответствует атрибуту `marker` со следующими полями:
 - `q` – значение атрибута качества.
 - `ts` – статус метки времени, отображающий её правильность, временное состояние или причину ошибки при проверке.
 - `ds` – статус данных.
 - `o` – источник, от которого пришло значение или команда.
 - `t` – время последнего обновления значений тега, взятое из трафика.
 - `ct` – причина передачи.

Формат: `"m": "q"`

Пример отправляемого значения тега в формате JSON:

```
{
  "n": "TagStructure1",
  "ts": 18446744073709551616,
  "dn": "r",
  "mp": 1,
  "d": {
    {
      "value": {
        {
          "t": "d",
          "v": 3.1415,
          "x": 1
        },
        "quality": {
          {
            "t": "s",
            "v": "good",
            "m": "q"
          },
          "mask": {
            {
              "t": "u",
              "v": 18446744073709551616
            },
            "enumfield": {
              {
                "t": "e",
                "n": "SwitchState",
                "v": 0,
                "s": "Off"
              },
            },
          },
        },
      },
    },
  },
}
```

```
"strucfield":
{
  "t": "st",
  "v":
  {
    "v1":
    {
      "t": "d",
      "v": 3.1415
    },
    "q2":
    {
      "t": "s",
      "v": "good",
      "m": "q"
    }
  }
},
"unionfield":
{
  "t": "un",
  "v":
  {
    "_":
    {
      "t": "u",
      "v": 42
    },
    "low4bits":
    {
      "t": "u",
      "v": 10
    },
    "high4bits":
    {
      "t": "u",
      "v": 2
    }
  }
}
}
```


Примеры получения значений тегов по подписке

Ниже представлен пример получения значений тегов по подписке с использованием стандартных функций WebSocket на языке Python.

Предварительно требуется выполнить команду:

```
pip install websocket_client
```

Пример подписки с использованием стандартных функций WebSocket:

```
import json, ssl, websocket

def on_message(ws, message):
    print(message)

def on_error(ws, error):
    print(f' error: {error}')

def on_close(ws):
    print("### closed ###")

def on_open(ws):
    print("connection opened and handshake received ready to send messages")

    # all sent messages must end with this character
    message_separator = chr(30)

    # setting up json as messages format
    protocol_selection_args = {
        'protocol': 'json',
        'version': 1
    }
    ws.send(json.dumps(protocol_selection_args) + message_separator)
```

```
# creating subscription
args = {
    'arguments': [
        {
            'tagIdentifiers': [
                {
                    'tagName': 'tag_01',
                    'assetName': 'asset_02'
                }
            ],
            'streamConfig': {
                'samplingRateHz': 5
            }
        }
    ],
    'invocationId': '0',          # will be included in response message
    'target': 'getTagValuesStream',
    'type': 4                    # must be equal to 4 for outgoing messages
}

ws.send(json.dumps(args) + message_separator)

def login():
    token = "you should get access token for API here"
    return token

if __name__ == "__main__":
    server_url = "wss://localhost:8091/kics4net/api/tag-values"
    auth = "Authorization: Bearer " + login()

    # for troubleshooting uncomment next line
    # websocket.enableTrace(True)
    ws = websocket.WebSocketApp(server_url,
                                on_message=on_message,
                                on_error=on_error,
                                on_close=on_close,
                                header=[auth])

    print(f'opening connection to {server_url}')
    ws.on_open = on_open
    ws.run_forever(
        # use it only if Server has self-signed certificate
        sslopt={"cert_reqs": ssl.CERT_NONE}
    )
```

Ниже представлен пример получения значений тегов по подписке с использованием библиотеки SignalR Core на языке Python.

Предварительно требуется выполнить команду:

```
pip install signalrcore
```

Пример подписки с использованием библиотеки SignalR Core:

```
import logging
from signalrcore.hub_connection_builder import HubConnectionBuilder

TOKEN = 'you should get access token for API here'
IP = '192.168.0.7'
PORT = '8080'
HUB = 'kics4net/api/v3/tag-values'

class WebsocketConnection(HubConnectionBuilder):
    def __init__(self, url: str = None, options: dict = None, verify_ssl: bool = False):
        super().__init__()
        self.with_url(url, options=options)
        self.configure_logging(logging.WARNING)
        self.with_automatic_reconnect({
            "type": "raw",
            "keep_alive_interval": 10,
            "reconnect_interval": 5,
            "max_attempts": 5
        })
        self.verify_ssl = verify_ssl

    def on_tag_stream_value(self, m):
        result.append(m)
        print(f'on_new_tag_value, {m}')

    def on_tag_stream_error(self, e):
        print(f'onError, {e}')

    def on_tag_stream_complete(self, q):
        print(f'onComplete, {q}')

    def subscribe_tags(self):
        print("connection opened and handshake received ready to send messages")
```

```
args = {
    'tagIdentifiers': [
        {
            'tagName': 'tag_01',
            'assetName': 'asset_02'}
    ],
    'streamConfig': {
        'samplingRateHz': 5
    }
}

self.stream("GetTagValuesStream", [args]) \
    .subscribe({
        "next": self.on_tag_stream_value,
        "complete": self.on_tag_stream_complete,
        "error": self.on_tag_strean_error
    })

def main():
    server_url = "Error! Hyperlink reference not valid., PORT, HUB)
    login = 'bearer {}'.format(TOKEN)

    conn = WebSocketConnection(url=server_url, options={"headers": {"authorization":
login}})
    conn.build()

    logging.info(f'opening connection to {server_url}')
    conn.on_open(conn.subscribe_tags)
    conn.start()

    logging.info('closing connection')
    conn.stop()

if __name__ == '__main__':
    main()
```

Решение типовых задач

Этот раздел содержит описание типовых пользовательских задач и инструкции по их выполнению.

В этом разделе

Мониторинг системы в онлайн-режиме	253
Контроль активов	262
Работа с картой сети	282
Мониторинг событий и инцидентов	305
Контроль уязвимостей устройств	331
Контроль технологического процесса	344
Обнаружение проблем безопасности в протоколах шифрования	352

Мониторинг системы в онлайн-режиме

Kaspersky Industrial CyberSecurity for Networks отображает данные для мониторинга текущего состояния системы в разделе **Мониторинг** веб-интерфейса программы. Обновление данных происходит автоматически в онлайн-режиме.

Данные в разделе **Мониторинг** представлены в виде отдельных блоков, называемых *виджетами*. В зависимости от назначения, виджет может содержать обновляемое значение, сообщение о текущем состоянии программы или предоставлять развернутую информацию о текущих и накопленных данных.

В разделе **Мониторинг** могут отображаться следующие виджеты:

- Виджеты с информацией о программе и аппаратных ресурсах Сервера и сенсоров:
 - **Трафик** – скорость поступления входящего трафика. Виджет может отображать данные по всем точкам мониторинга всех узлов с установленными компонентами программы, по точкам мониторинга выбранного узла или только по одной точке мониторинга.
 - **Процессор** – загруженность процессора на выбранном узле с установленным компонентом программы.
 - **Оперативная память** – объем потребления физической оперативной памяти на выбранном узле с установленным компонентом программы.
 - **Работоспособность** – информация о текущем состоянии работоспособности программы. Виджет может отображать следующие значения:
 - **ОК** – нет сообщений о нарушении работоспособности или все проблемы работоспособности устранены.
 - **Некритический сбой** – есть сообщения о некритических сбоях (отображается до момента устранения проблемы работоспособности).
 - **Нарушена работа** – есть сообщения о нарушении работы программы (отображается до момента устранения проблемы работоспособности).
 - **Режим обслуживания** – программа находится в режиме обслуживания.
 - **Теги** – скорость обработки тегов, обнаруженных программой. Виджет может отображать данные по всем точкам мониторинга всех узлов с установленными компонентами программы, по точкам мониторинга выбранного узла или только по одной точке мониторинга.

- **Хранилище** – данные о диске, который находится в локальной файловой системе на выбранном узле с установленным компонентом программы. В этом виджете вы можете выбрать следующие данные для отображения:
 - **Использование диска** – процентное значение времени на обработку операций чтения и записи данных.
 - **Занято на диске** – объем занятого дискового пространства.
 - **Чтение с диска** – скорость чтения данных с диска.
 - **Запись на диск** – скорость записи данных на диск.
- **Задержка обработки трафика** – текущее время задержки при обработке трафика с момента его поступления на точку мониторинга узла (выводится максимальное время задержки, полученное со всех включенных точек мониторинга). Виджет может отображать данные по всем точкам мониторинга всех узлов с установленными компонентами программы или по точкам мониторинга выбранного узла.
- **Состояние функций** – общая информация о текущем состоянии функций защиты в составе программы. Виджет может отображать следующие значения:
 - **Включены все** – работают все технологии и методы, предназначенные для постоянного использования, а также включены все созданные точки мониторинга.
 - **Не все включены** – некоторые функции защиты выключены или включены в режиме обучения, либо включены не все точки мониторинга.
- **Время работы** – время работы Kaspersky Industrial CyberSecurity for Networks. В этом виджете вы можете выбрать следующие данные для отображения:
 - **Эффективное время работы** – время нормальной работы программы (без сбоев) с последнего запуска до текущего момента.
 - **Общее время работы** – время работы с первого запуска программы до текущего момента (включает периоды нормальной работы программы и периоды работы со сбоями).
 - **С первого запуска программы** – общее время, прошедшее с первого запуска программы до текущего момента (включает периоды нормальной работы программы, периоды работы со сбоями и периоды неработоспособного состояния).
- Виджеты с информацией для контроля наиболее значимых изменений в системе:
 - **Устройства** – содержит информацию об устройствах в промышленной сети (см. раздел "Информация в виджете Устройства" на стр. [257](#)) (используется распределение по категориям устройств).
 - **События** – содержит информацию о событиях и инцидентах (см. раздел "Информация в виджете События" на стр. [259](#)), имеющих наиболее поздние значения даты и времени последнего появления.
- Виджеты без динамически изменяемой информации. Вы можете создавать виджеты с произвольно заданным содержанием. Такие виджеты называются *пользовательскими*. С помощью пользовательских виджетов вы можете, например, логически разделять группы виджетов в разделе **Мониторинг**.

Для виджетов предусмотрены различные средства привлечения внимания в зависимости от поступающих данных. Например, виджеты с информацией о программе и аппаратных ресурсах могут автоматически изменять цвет, если информация требует внимания (в частности, при нагрузке на аппаратный ресурс близкой к критической).

В виджетах отображается только основная информация, которая изменяется динамически. Если вам нужно просмотреть более подробную информацию (например, об устройствах, требующих внимания), вы можете перейти из раздела **Мониторинг** к другим разделам веб-интерфейса программы. Переходы можно выполнять путем выбора элементов интерфейса виджетов с помощью мыши.

В этом разделе

Добавление виджета	255
Настройка отображения виджетов	255
Информация в виджете Устройства	257
Информация в виджете События	259
Удаление виджета	261

Добавление виджета

► Чтобы добавить виджет, выполните следующие действия:

1. В разделе **Мониторинг** нажмите на кнопку **Виджеты**.
Откроется окно **Добавление виджетов**.
2. Добавьте нужный виджет (см. раздел "Мониторинг системы в онлайн-режиме" на стр. [253](#)) по ссылке **Добавить** справа от названия виджета.
Новый виджет займет свободное место в области отображения виджетов.
3. Нажмите на кнопку **Заккрыть** в окне **Добавление виджетов**.

После добавления вы можете настроить отображение виджета (см. раздел "Настройка отображения виджетов" на стр. [255](#)).

Настройка отображения виджетов

Для настройки отображения виджетов вы можете использовать следующие функции:

- Перемещение виджета

► Чтобы переместить виджет, выполните следующие действия:

1. В разделе **Мониторинг** наведите курсор на верхнюю часть нужного виджета (например, на название виджета).

Курсор примет вид .

2. Перетащите виджет (см. раздел "Мониторинг системы в онлайн-режиме" на стр. [253](#)) в нужную часть области отображения виджетов.

- Изменение размера виджета


► Чтобы изменить размер виджета, выполните следующие действия:

1. В разделе **Мониторинг** наведите курсор на нижний правый угол нужного виджета.
2. Удерживая нажатой левую клавишу мыши, задайте размер для рамки виджета.

- Изменение параметров отображения данных в виджете

После добавления виджета для отображения данных используются параметры, заданные по умолчанию. При необходимости вы можете изменить параметры отображения (например, чтобы указать нужный источник или выбрать другие данные для отображения в виджете **Хранилище** (см. раздел "**Мониторинг системы в онлайн-режиме**" на стр. [253](#))).

► *Чтобы настроить параметры отображения виджета, выполните следующие действия:*

1. В разделе **Мониторинг** откройте меню управления виджетом с помощью кнопки  в правом верхнем углу виджета.
2. В меню управления виджетом выберите пункт **Настроить**.
Откроется окно для настройки параметров отображения.
3. Настройте параметры виджета.

В зависимости от выбранного виджета окно может содержать следующие параметры:

- **Изменить название** – если установлен флажок **Изменить название**, вы можете задать произвольное название виджета (отличающееся от заданного по умолчанию) в поле **Название виджета**. Параметр **Изменить название** отсутствует для пользовательских виджетов.
 - **Название виджета** – поле для ввода названия виджета, отличающегося от названия по умолчанию.
 - **Изменить описание** – если установлен флажок **Изменить описание**, вы можете задать произвольное описание виджета (отличающееся от заданного по умолчанию) в поле **Описание виджета**. Параметр **Изменить описание** отсутствует для пользовательских виджетов.
 - **Описание виджета** – поле для ввода названия виджета, отличающегося от названия по умолчанию.
 - **Период обновления** – задает период времени в секундах, после которого обновляются отображаемые данные.
 - **Отображать** – задает тип отображаемых данных (для виджетов с возможностью выбора данных для отображения).
 - **Источник данных** – задает узел с установленными компонентами программы, данные от которого отображаются в виджете. Если выбран вариант **Вся программа**, виджет отображает данные со всех узлов.
 - **Точка мониторинга** – задает точку мониторинга выбранного узла для отображения данных. Если выбран вариант **Все точки мониторинга**, виджет отображает данные по всем точкам мониторинга выбранного узла.
 - **Изменять цвет по состоянию** – если флажок установлен, цвет фона виджета автоматически изменяется в зависимости от уровня важности поступивших данных. Критическому (максимальному) уровню важности данных соответствует красный цвет фона. Если флажок снят, закрашивание фона выключено.
 - **Заданный фон** – определяет цвет фона пользовательского виджета. Вы можете выбрать вариант закрашивания цветом, который соответствует одному из уровней важности (**Информационный**, **Важный**, **Критический**), или выключить закрашивание фона с помощью варианта **Бесцветный**.
4. Нажмите на кнопку **ОК**.

Информация в виджете Устройства

Виджет **Устройства** в разделе **Мониторинг** отображает информацию об устройствах, входящих в список известных программе устройств.

В виджете представлена следующая информация:

- Данные о количественном распределении известных программе устройств по категориям. Эти данные отображаются в верхней части виджета в виде значков категорий. Под значком каждой категории указано количество устройств этой категории. Если в списке известных программе устройств есть устройства, требующие внимания, на значках категорий этих устройств отображается значок предупреждения.
- Список категорий с устройствами, требующими внимания. Эти данные отображаются в средней части виджета при наличии таких устройств. Пространство для отображения графических элементов ограничено размером виджета.

Устройства, требующие внимания

Программа считает, что устройство требует внимания, в любом из следующих случаев:

- устройство имеет статус *Разрешенное* и состояние безопасности устройства отличается от *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 виджете. Количество графических элементов в строке зависит от текущего размера окна браузера. Если устройств, требующих внимания, больше, чем отображаемых графических элементов в строке, то справа отображается количество скрытых устройств в формате `+<количество устройств>`.

Графические элементы устройств

Графические элементы, представляющие устройства, содержат следующую информацию:

- Имя устройства.
- Статус устройства. Отображается в виде значка, если устройство имеет статус *Неразрешенное*.
- Состояние безопасности устройства. Отображается в виде цветной линии на левой границе графического элемента. Цвет линии соответствует состояниям *ОК*, *Важное* или *Критическое*.

Графические элементы отображаются в следующем порядке:

1. Устройства с присвоенным статусом *Неразрешенное*.
2. Устройства, имеющие состояние безопасности *Критическое*.
3. Устройства, имеющие состояние безопасности *Важное*.

Переходы к другим разделам из виджета Устройства

С помощью элементов интерфейса виджета **Устройства** вы можете выполнять переходы к таблице устройств для отображения подробных сведений об устройствах. Для этого предусмотрены следующие возможности:

- Переход к таблице устройств и фильтрация таблицы

► *Чтобы перейти к таблице устройств и просмотреть сведения о всех устройствах выбранной категории,*

в верхней части виджета **Устройства** нажмите на значок нужной категории.

Откроется раздел **Устройства** с таблицей устройств. В таблице будет применена фильтрация по выбранной категории устройств.

► *Чтобы перейти к таблице устройств и просмотреть сведения об устройствах, требующих внимания и относящихся к определенной категории,*

в списке категорий с устройствами, требующими внимания, нажмите на ссылку с количеством устройств нужной категории (ссылка отображается в конце строки со значком категории и текстовым комментарием **требующие внимания**).

Откроется раздел **Устройства** с таблицей устройств. В таблице будет применена фильтрация по идентификаторам устройств, требующих внимания и относящихся к определенной категории.

Фильтрация в таблице устройств выполняется по идентификаторам тех устройств, которые отображались в виджете **Устройства** на момент перехода к таблице устройств. После перехода к таблице устройств параметры фильтрации не обновляются. Если вы хотите просмотреть текущее количество устройств, требующих внимания, вы можете снова перейти в раздел **Мониторинг**.

► *Чтобы перейти к таблице устройств и просмотреть сведения об устройстве, требующем внимания,*

в виджете **Устройства** нажмите на графический элемент, представляющий нужное устройство.

Откроется раздел **Устройства** с таблицей устройств. В таблице будет применена фильтрация по идентификатору устройства.

► *Чтобы перейти к таблице устройств без изменений текущих параметров фильтрации таблицы,*

выполните переход по ссылке **Показать все устройства** в виджете **Устройства**.

Откроется раздел **Устройства** с таблицей устройств. В таблице отобразятся устройства, удовлетворяющие параметрам фильтрации, которые были заданы ранее в таблице устройств.

- Переход к таблице устройств и поиск в таблице

► Чтобы перейти к таблице устройств и найти нужные устройства, выполните следующие действия:

1. В виджете **Устройства** введите поисковый запрос в поле **Поиск устройств**.
2. Нажмите на кнопку **Поиск**.

Откроется раздел **Устройства** с таблицей устройств. В таблице отобразятся устройства, которые удовлетворяют условиям поиска.

Информация в виджете События

Виджет **События** в разделе **Мониторинг** отображает общую информацию о событиях и инцидентах, имеющих наиболее поздние значения даты и времени последнего появления.

В виджете отображаются следующие элементы:

- Гистограмма событий и инцидентов за выбранный период. Эти данные отображаются в верхней части виджета. Гистограмма отображает распределение событий и инцидентов по уровням важности.
- Список с информацией о зарегистрированных событиях и инцидентах, отсортированный по дате и времени последнего появления. Эти данные отображаются в средней части виджета.

Статистика событий и инцидентов

На гистограмме распределения событий и инцидентов столбцы соответствуют суммарному количеству событий за каждый интервал времени. Внутри столбцов цветом обозначены уровни 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.

Выбор периода для отображения гистограммы

► Чтобы построить гистограмму за нужный период,

в виджете **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.


Список событий и инцидентов

Список событий и инцидентов в виджете **События** обновляется в онлайн-режиме. События и инциденты с наиболее поздними значениями даты и времени последнего появления помещаются в начало списка.

Количество отображаемых элементов списка событий и инцидентов ограничено размером виджета.

Для каждого события или инцидента в списке представлены следующие сведения:

- заголовок события или инцидента;
- дата и время последнего появления;
- значок, обозначающий уровень важности события или инцидента: *Информационные*, *Важные*, или *Критические*.

Инциденты в списке обозначаются значком .

Переходы к другим разделам из виджета События

С помощью элементов интерфейса виджета **События** вы можете выполнять переходы к таблице событий для отображения подробных сведений о событиях и инцидентах. Для этого предусмотрены следующие возможности:

- Переход к таблице событий и фильтрация таблицы

► Чтобы просмотреть подробные сведения о событии или инциденте, отображаемом в списке виджета **События**,

нажмите на нужное событие или инцидент.

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 перейти к таблице событий без изменений текущих параметров фильтрации событий,

выполните переход по ссылке **Показать все события** в виджете **События**.

Откроется раздел **События**. В таблице событий отобразятся события и инциденты, удовлетворяющие параметрам фильтрации, которые были заданы ранее в таблице событий.

- Переход к таблице событий и поиск в таблице


► Чтобы найти нужные события и инциденты в таблице событий, выполните следующие действия:

1. В виджете **События** введите поисковый запрос в поле **Поиск событий**.
2. Нажмите на кнопку **Поиск**.

Откроется раздел **События**. В таблице событий отобразятся события и инциденты, которые удовлетворяют условиям поиска.

Удаление виджета

► Чтобы удалить виджет, выполните следующие действия:

1. В разделе **Мониторинг** вызовите меню управления виджетом с помощью кнопки  в правом верхнем углу виджета.
2. В меню управления виджетом выберите пункт **Удалить**.
Откроется окно с запросом подтверждения.
3. В окне запроса подтвердите удаление выбранного виджета.

Контроль активов

Kaspersky Industrial CyberSecurity for Networks позволяет контролировать устройства промышленной сети, представляющие активы предприятия. Для контроля активов вы можете просматривать таблицу устройств (см. раздел “Таблица устройств” на стр. [262](#)) в разделе **Активы** веб-интерфейса Kaspersky Industrial CyberSecurity for Networks. Также вы можете просматривать информацию о взаимодействиях устройств и выполнять различные действия с устройствами при работе с картой сети (см. раздел “Работа с картой сети” на стр. [282](#)).

В этом разделе

Таблица устройств.....	262
Просмотр таблицы устройств	265
Просмотр подсетей для контроля активов	270
Выбор устройств в таблице устройств	273
Выбор подсетей в таблице подсетей.....	274
Просмотр сведений об устройстве.....	275
Автоматическое добавление и обновление устройств	275
Автоматическое изменение статусов устройств	276
Дерево групп устройств.....	277
Контроль чтения и записи проектов ПЛК.....	277
Просмотр событий, связанных с устройствами	279
Экспорт устройств в файл.....	279
Экспорт подсетей в файл.....	281

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 100 тыс.
Если достигнуто ограничение максимального количества устройств со статусами *Разрешенное* и *Неразрешенное*, новые устройства с этими статусами не добавляются в таблицу. В этом случае, чтобы добавить новое устройство в таблицу, вам нужно удалить одно из ранее добавленных устройств.
- Количество устройств со статусом *Неиспользуемое* – не более 100 тыс.
Если достигнуто ограничение максимального количества устройств со статусом *Неиспользуемое*, новые устройства с этим статусом добавляются в таблицу вместо устройств, которые дольше всего не проявляли активность.

При переполнении таблицы устройств программа выводит соответствующее сообщение.

Таблица устройств содержит следующие сведения:

- **Имя** – имя, под которым устройство представлено в программе.
- **ID устройства** – идентификатор устройства, присвоенный в Kaspersky Industrial CyberSecurity for Networks.
- **Статус** – статус устройства, определяющий разрешение активности устройства в промышленной сети. Устройство может иметь один из следующих статусов:
 - *Разрешенное*. Этот статус присваивается устройству, которому разрешена активность в промышленной сети.
 - *Неразрешенное*. Этот статус присваивается устройству, которому не разрешена активность в промышленной сети.
 - *Неиспользуемое*. Этот статус присваивается устройству, если оно больше не используется или не должно использоваться в промышленной сети, либо если устройство длительное время не проявляло активность и не изменялись сведения об этом устройстве (30 дней и более).
- **Адресная информация** – MAC- и / или IP-адреса устройства. Если устройство имеет несколько сетевых интерфейсов, 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.
 - **Ноутбук** – переносные персональные компьютеры.
 - **HMI-панель** – устройства, использующие человеко-машинный интерфейс для управления отдельными устройствами или операциями технологического процесса.
 - **Принтер** – печатающие устройства.
 - **ИБП** – блоки бесперебойного питания, подключаемые к вычислительной сети.
 - **Сетевая камера** – устройства, выполняющие функции видеонаблюдения и передачи изображения в цифровом виде.
 - **Шлюз** – устройства для сопряжения сетей, преобразующие различные интерфейсы (например, Serial / Ethernet) в сетях с разнородной средой передачи данных и разными протоколами.
 - **Система хранения** – устройства для хранения информации внутри систем памяти.
 - **Брандмауэр** – устройства, выполняющие функции сетевого экрана для проверки и блокировки нежелательного трафика.
 - **Коммутатор** – устройства для физического соединения узлов локальной сети.

- **Виртуальный коммутатор** – устройства, логически объединяющие физические коммутаторы, или программно реализованные коммутаторы для систем виртуализации.
- **Маршрутизатор** – устройства, выполняющие функции перенаправления сетевых пакетов между сегментами вычислительной сети.
- **Виртуальный маршрутизатор** – устройства, логически объединяющие физические маршрутизаторы, или маршрутизаторы, использующие несколько независимых таблиц маршрутизации.
- **Wi-Fi** – точки доступа, обеспечивающие беспроводное подключение устройств из сетей Wi-Fi.
- **Сервер Historian** – серверы архивных данных.
- **Другое** – устройства, не относящиеся к вышеперечисленным категориям.
- **Группа** – имя группы, в которую помещено устройство в дереве групп устройств (содержит имя самой группы и имена всех ее родительских групп).
- **Состояние безопасности** – состояние безопасности устройства, определяемое по наличию связанных с устройством событий и актуальных уязвимостей. Предусмотрены следующие состояния безопасности:
 - *Критическое*. С устройством связаны необработанные события с уровнем важности *Критические* или актуальные уязвимости с уровнем критичности *Высокий*.
 - *Важное*. С устройством связаны необработанные события с уровнем важности *Важные* или актуальные уязвимости с уровнем критичности *Средний* (при этом нет необработанных событий с уровнем важности *Критические* или актуальных уязвимостей с уровнем критичности *Высокий*).
 - *ОК*. Все события, связанные с устройством, обработаны или имеют уровень важности *Информационные*. А также все уязвимости, связанные с устройством, переведены в состояние *Устранена* или *Принята* или имеют уровень критичности *Низкий*.
- **Последнее появление** – дата и время последней зафиксированной активности устройства.
- **Последнее изменение** – дата и время последнего изменения сведений об устройстве.
- **Создано** – дата и время добавления устройства в таблицу устройств.
- **ОС** – название операционной системы, установленной на устройстве.
- **Сетевое имя** – имя, под которым устройство представлено в сети.
- **Производитель оборудования** – название производителя аппаратного обеспечения устройства.
- **Модель оборудования** – название модели устройства.
- **Версия оборудования** – номер версии аппаратного обеспечения устройства.
- **Название ПО** – название программного обеспечения устройства.
- **Производитель ПО** – название производителя программного обеспечения устройства.
- **Версия ПО** – номер версии программного обеспечения устройства.
- **Метки** – список меток, назначенных устройству.
- **Уязвимости** – CVE-идентификаторы уязвимостей, связанных с устройством (уязвимости, обнаруженные по сведениям об устройстве).
- **Параметры контроля процесса** – признак наличия или отсутствия параметров контроля процесса, заданных для устройства.

Просмотр таблицы устройств

Таблица устройств отображается в разделе **Активы** на закладке **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

Вы можете настраивать следующие параметры отображения таблицы устройств:

- отображение CVE-идентификаторов уязвимостей в зависимости от состояния уязвимостей;
- состав и порядок граф, отображаемых в таблице.

► *Чтобы настроить параметры отображения таблицы устройств, выполните следующие действия:*

1. На закладке **Устройства** в разделе **Активы** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
2. Если вы хотите включить отображение CVE-идентификаторов всех обнаруженных уязвимостей (независимо от текущего состояния уязвимостей), установите флажок **Отображать устраненные и принятые уязвимости**.

Если флажок снят, в таблице отображаются только уязвимости в состоянии *Актуальна*.

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

Выбранные графы отобразятся в указанном вами порядке в таблице устройств.

- Фильтрация по графам таблицы

► *Чтобы отфильтровать устройства по графе **Статус**, **Категория**, **Состояние безопасности** или **Параметры контроля процесса**, выполните следующие действия:*


1. На закладке **Устройства** в разделе **Активы** 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 оборудования, Модель оборудования, Версия оборудования, Название ПО, Производитель ПО, Версия ПО или Сетевое имя**, выполните следующие действия:

1. На закладке **Устройства** в разделе **Активы** 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. На закладке **Устройства** в разделе **Активы** 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. На закладке **Устройства** в разделе **Активы** 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 (ИЛИ)** и укажите другую группу в открывшемся поле.

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

Вы также можете выключить фильтрацию в графе по ссылке **Фильтр по умолчанию**, которая отображается в верхней части окна фильтрации.

6. Нажмите на кнопку **ОК**.

► Чтобы отфильтровать устройства по графе **Последнее появление**, **Последнее изменение** или **Создано**, выполните следующие действия:

1. На закладке **Устройства** в разделе **Активы** 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. На закладке **Устройства** в разделе **Активы** 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.

Вы также можете выключить фильтрацию в графе по ссылке **Фильтр по умолчанию**, которая отображается в верхней части окна фильтрации.

5. Нажмите на кнопку **ОК**.

► Чтобы отфильтровать устройства по графе **Уязвимости**, выполните следующие действия:

1. На закладке **Устройства** в разделе **Активы** нажмите на значок фильтрации в графе **Уязвимости**.

Откроется окно фильтрации.

2. Если вы хотите задать параметры фильтрации устройств с уязвимостями, оставьте переключатель **Исключить устройства с уязвимостями** в состоянии *Выключено* и настройте параметры с помощью следующих элементов управления:

- **CVE** – позволяет ввести CVE-идентификатор для отображения устройств с этой уязвимостью.
- **Оценка CVSS** – позволяет задать диапазон значений оценок по системе CVSS для отображения устройств с уязвимостями, у которых значение оценки входит в указанный диапазон.
- **Состояние** – группирует кнопки для включения и выключения фильтрации по состояниям уязвимостей (кнопки отображаются, если в параметрах отображения таблицы устройств установлен флажок **Отображать устранимые и принятые уязвимости**).

3. Если вы хотите отобразить только устройства без уязвимостей, переведите переключатель **Исключить устройства с уязвимостями** в состояние *Включено*.
4. Нажмите на кнопку **ОК**.

- Поиск устройств

► *Чтобы найти нужные устройства,*

на закладке **Устройства** в разделе **Активы** 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**, **Создано** и **Параметры контроля процесса**. Поиск также выполняется по значениям пользовательских полей для устройств (см. раздел “Просмотр сведений об устройстве” на стр. [275](#)).

- Сброс заданных параметров фильтрации и поиска

► *Чтобы сбросить заданные параметры фильтрации и поиска в таблице устройств,*

в панели инструментов на закладке **Устройства** в разделе **Активы** нажмите на кнопку **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации или поиска).

- Сортировка устройств

► *Чтобы отсортировать устройства, выполните следующие действия:*

1. На закладке **Устройства** в разделе **Активы** 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 на закладке **Устройства** в разделе **Активы** используйте переключатель **Обновлять автоматически**.

Просмотр подсетей для контроля активов

Kaspersky Industrial CyberSecurity for Networks контролирует только те IP-адреса устройств, которые принадлежат подсетям из числа известных программе. По умолчанию в программе задан стандартный список подсетей, наиболее часто используемых на предприятиях.

Программа проверяет обнаруженные IP-адреса по списку известных подсетей и в зависимости от принадлежности IP-адресов определенным типам подсетей может выполнять следующие действия:

- добавлять устройство с обнаруженным IP-адресом в таблицу устройств и контролировать активность этого устройства;
- отображать устройство с обнаруженным IP-адресом на карте сети в виде узла соответствующего типа (см. раздел "Узлы на карте сети" на стр. [283](#)) (известное программе устройство, неизвестное или узел WAN);
- отображать соединение на карте сети (см. раздел "Соединения на карте сети" на стр. [286](#)), в котором одной из сторон взаимодействия является устройство с обнаруженным IP-адресом;
- проверять взаимодействия устройства с обнаруженным IP-адресом по заданным правилам (правила контроля взаимодействий, правила обнаружения вторжений и правила корреляции);
- игнорировать активность устройства с обнаруженным IP-адресом.

Вы можете просматривать сведения о подсетях на закладке **Подсети** в разделе **Активы**.

При просмотре сведений о подсетях вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице подсетей

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

1. На закладке **Подсети** в разделе **Активы** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
2. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр (см. ниже).
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 подсетей.

Для выбора доступны следующие параметры:

- **Подсеть** – адрес подсети в формате записи по методу бесклассовой адресации (Classless Inter-Domain Routing, CIDR): <базовый адрес подсети>/<количество бит в маске>. Адреса подсетей отображаются в виде дерева, которое показывает иерархию вложенности подсетей.
- **Тип** – тип подсети, определяющий ее назначение. Предусмотрены следующие типы:
 - **Частная, IT** – подсеть для устройств, относящихся к ресурсам информационных технологий (IT), например файловых серверов.
 - **Частная, OT** – подсеть для устройств, относящихся к операционным технологиям (OT), например ПЛК.
 - **Частная, DMZ** – подсеть для устройств, находящихся в сегменте сети демилитаризованной зоны (DMZ), например серверов для запросов из внешних сетей.
 - **Публичная** – подсеть, которая считается внешней (глобальной) сетью для устройств в подсетях других типов. IP-адреса из этой подсети представлены на карте сети узлом WAN.
 - **Link-local** – подсеть для сетевых взаимодействий в пределах одного сегмента локальной сети (немаршрутизируемая).
- **Диапазон** – диапазон IP-адресов, входящих в подсеть.
- **Игнорировать MAC-адреса** – признак включенного или выключенного режима пропуска обнаруженных MAC-адресов при создании разрешающих правил для сетевых взаимодействий с участием IP-адресов из подсети. Если режим включен, то MAC-адреса, обнаруженные вместе с IP-адресами из подсети, не будут добавляться в правила по технологии Контроль целостности сети в режиме обучения.

- Фильтрация по графам таблицы

При необходимости вы можете отфильтровать подсети по графам **Тип** или **Игнорировать MAC-адрес**.

► *Чтобы отфильтровать подсети, выполните следующие действия:*

1. На закладке **Подсети** в разделе **Активы** нажмите на значок фильтрации в графе **Тип** или **Игнорировать MAC-адрес**.

При фильтрации по типам вы также можете воспользоваться раскрывающимся списком **Типы** в панели инструментов.

Откроется окно фильтрации.

2. Установите флажки напротив значений, по которым вы хотите выполнить фильтрацию.
3. Нажмите на кнопку **ОК**.

- Поиск подсетей

► *Чтобы найти нужные подсети,*

на закладке **Подсети** в разделе **Активы** введите поисковый запрос в поле **Поиск подсетей**. Поиск инициируется во время ввода символов.

В таблице отобразятся подсети, которые удовлетворяют условиям поиска.

Поиск выполняется по графе **Подсеть**.

- Сброс заданных параметров фильтрации и поиска

► *Чтобы сбросить заданные параметры фильтрации и поиска в таблице подсетей,*

на закладке **Подсети** в разделе **Активы** нажмите на кнопку **Фильтр по умолчанию** в панели инструментов (кнопка отображается, если заданы параметры фильтрации или поиска).

- Сортировка подсетей

► *Чтобы отсортировать подсети, выполните следующие действия:*

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

Вы можете отсортировать таблицу подсетей по значениям любой графы, кроме графы **Диапазон**.

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.

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 (см. раздел "Автоматическое добавление и обновление устройств" на стр. [275](#)). 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).

Выбор подсетей в таблице подсетей

В таблице подсетей вы можете выбирать подсети для просмотра сведений и для работы с этими подсетями. При выборе подсети в правой части окна веб-интерфейса появляется область деталей.

► Чтобы выбрать нужные подсети в таблице, выполните одно из следующих действий:

- Если вы хотите выбрать одну подсеть, установите флажок напротив этой подсети или выберите подсеть с помощью мыши.
- Если вы хотите выбрать несколько подсетей, установите флажки напротив нужных подсетей или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**.
- Если вы хотите выбрать все подсети, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:
 - выберите любую подсеть в таблице и нажмите комбинацию клавиш **CTRL+A**;
 - установите флажок в заголовке левой крайней графы таблицы.

В заголовке левой крайней графы таблицы отображается флажок выбора подсетей. В зависимости от количества выбранных подсетей флажок может быть в одном из следующих состояний:

- – в таблице не выполнялся выбор всех подсетей, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбрана одна подсеть или несколько подсетей с помощью флажков напротив подсетей или с использованием клавиш **CTRL** или **SHIFT**.
- – в таблице выбраны все подсети, удовлетворяющие текущим параметрам фильтрации и поиска.
- – в таблице были выбраны все подсети, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых подсетей были сняты флажки. Это состояние сохраняется и в случае, если флажки сняты для всех подсетей, выбранных таким способом (из-за того, что количество выбранных подсетей может измениться).

Если выбраны все подсети, удовлетворяющие параметрам фильтрации и поиска, количество выбранных подсетей может автоматически изменяться. Например, состав подсетей в таблице может быть изменен пользователем программы в другом сеансе подключения. Рекомендуется настраивать параметры фильтрации и поиска таким образом, чтобы в выборку попали только нужные подсети.

Просмотр сведений об устройстве

Подробные сведения об устройстве включают информацию из таблицы устройств (см. раздел “Таблица устройств” на стр. [262](#)), а также следующие поля:

- **Маршрут. устройство** – признак маршрутизирующего устройства.


Если признак маршрутизирующего устройства не определен автоматически, то его требуется выставить вручную (например, для устройства, которое выполняет функции сетевого коммутатора между сегментами промышленной сети). В частности, если в различных сегментах находятся ПЛК и компьютер со SCADA-системой, взаимодействующий с этими ПЛК. В этом случае программа сможет автоматически добавлять в таблицу устройств все устройства, обнаруженные в сегменте с такими ПЛК.

- **Доп. сведения** – дополнительные сведения об устройстве, заданные пользователем программы (например, описание размещения устройства).
- **Пользовательские поля** – набор нестандартных сведений об устройстве, заданных пользователем программы (например, категории и классы защиты устройства). Для устройства может быть указано до 16 пользовательских полей.
- **Динамические поля** – набор расширенных сведений об устройстве, обнаруженных в трафике при работе метода обнаружения сведений об устройствах. Поле отображается, если расширенные сведения были обнаружены программой.

Если для устройства заданы параметры контроля процесса, они отображаются в отдельном блоке параметров (см. раздел “Параметры контроля процесса для устройств” на стр. [156](#)).

► *Чтобы просмотреть сведения об устройстве,*

на закладке **Устройства** в разделе **Активы** 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 .

Автоматическое добавление и обновление устройств

Программа может автоматически добавлять устройства в таблицу и обновлять сведения об устройствах. Для автоматического добавления и обновления устройств в Kaspersky Industrial CyberSecurity for Networks требуется включить следующие методы контроля активов:

- Обнаружение активности устройств. При использовании этого метода программа добавляет в таблицу новые обнаруженные устройства по полученным MAC- и / или IP-адресам устройств. Если обнаружена активность уже известного программе устройства, программа может изменить его статус в зависимости от текущего режима работы контроля активов (см. раздел “Методы и режимы контроля активов” на стр. [121](#)).
- Обнаружение сведений об устройствах. При использовании этого метода программа обновляет сведения об известных устройствах на основе полученных данных из трафика. Обновляются те сведения, для которых включено автоматическое изменение в параметрах устройства (см. раздел “Изменение сведений об устройстве” на стр. [150](#)) (включено по умолчанию до изменения значения вручную пользователем программы).

При добавлении устройства программа по умолчанию задает имя устройства по шаблону:

Устройство <значение внутреннего счетчика устройств>. При этом значение внутреннего счетчика в имени устройства может не совпадать с идентификатором устройства, который отображается в графе **ID устройства**.

С помощью метода обнаружения сведений об устройствах программа может обновить имя устройства после получения из трафика следующих сведений:

- название модели устройства;
- сетевое имя, под которым устройство представлено в сети (сетевое имя устройства имеет приоритет при актуализации).

Программа может автоматически обновлять сведения, относящиеся к производителям сетевого оборудования устройств, на основе MAC-адресов устройств. Для определения производителей по MAC-адресам программа сверяет MAC-адреса устройств с диапазонами адресов, которые были зарегистрированы в открытой базе данных (<http://standards-oui.ieee.org/>) международной организации Institute of Electrical and Electronics Engineers (IEEE). Если производитель сетевого оборудования определен по MAC-адресу, то в качестве названия производителя программа сохраняет такое же название, какое представлено в базе данных IEEE.

После установки программы используется копия базы данных IEEE, содержащая сведения о MAC-адресах и производителях на момент выпуска текущей версии программы. Вы можете поддерживать локальную копию базы данных IEEE в актуальном состоянии, устанавливая обновления (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).

Автоматическое изменение статусов устройств

При отслеживании активности устройств в промышленной сети программа может автоматически присваивать статусы обнаруженным устройствам по полученным MAC- и / или IP-адресам устройств. Статусы присваиваются в зависимости от текущего режима контроля активов (см. раздел "Методы и режимы контроля активов" на стр. [121](#)).

В режиме обучения программа присваивает статус *Разрешенное* всем обнаруженным устройствам (как новым устройствам, так и ранее добавленным в таблицу устройств). Статус обнаруженного устройства не изменяется, если устройству ранее был присвоен статус *Неразрешенное*.

В режиме наблюдения присваиваемый статус зависит от того, является ли устройство, проявившее активность, известным или неизвестным программе. В этом режиме присвоение статусов происходит по следующим правилам:

- Если устройство является новым (отсутствовало в таблице устройств на момент обнаружения), этому устройству присваивается статус *Неразрешенное*.
- Если устройство присутствует в таблице устройств со статусом *Разрешенное* или *Неразрешенное*, статус не меняется.
- Если устройство присутствует в таблице устройств со статусом *Неиспользуемое*, этому устройству присваивается статус *Неразрешенное*.

По умолчанию если устройство со статусом *Разрешенное* не проявляет активность более 30 дней и за это время не изменялись сведения об устройстве, этому устройству автоматически присваивается статус *Неиспользуемое*. Вы можете выключить автоматическое изменение статуса при изменении статуса устройства вручную (см. раздел "Изменение статусов устройств вручную" на стр. [130](#)) (например, чтобы статус *Разрешенное* не изменялся на статус *Неиспользуемое* для редко подключаемого устройства).

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 (см. раздел "Удаление устройств" на стр. [129](#)). Однако в этом случае также будут удалены все сведения, указанные для этого устройства. Если удаленное устройство снова будет обнаружено, в программе будут доступны только сведения, полученные с момента повторного добавления в таблицу устройств (в том числе обновится дата и время первого обнаружения устройства).

Дерево групп устройств

Дерево групп устройств предназначено для распределения устройств в соответствии с их назначением, размещением или по каким-либо другим произвольным признакам. Устройства могут быть распределены по группам вручную (например, для соответствия местоположению устройств в производственной структуре предприятия) или автоматически (по принадлежности IP-адресов устройств подсетям, по категориям устройств или по производителям).

Если устройство не включено ни в одну из групп, это устройство считается относящимся к верхнему уровню иерархии в дереве групп. Устройства, автоматически добавленные в таблицу, по умолчанию не включаются в группы.

Распределять устройства по группам могут только пользователи с ролью Администратор.

Узнать, в какие группы входят устройства, вы можете при просмотре таблицы устройств. Пути к группам указаны в графе **Группа**. Группы устройств также отображаются и на карте сети, однако входящие в эти группы устройства могут не отображаться, если они не удовлетворяют параметрам фильтрации объектов на карте сети (см. раздел "Фильтрация объектов на карте сети" на стр. [291](#)).

Контроль чтения и записи проектов ПЛК

Kaspersky Industrial CyberSecurity for Networks может обнаруживать в трафике промышленной сети информацию о проектах ПЛК и сравнивать эту информацию с ранее полученной информацией о проектах ПЛК.

Проект ПЛК – микропрограмма, написанная для ПЛК. Проект ПЛК хранится в памяти ПЛК и выполняется в рамках технологического процесса, использующего ПЛК. Проект ПЛК может состоять из блоков, которые по отдельности передаются и принимаются по сети при чтении или записи проекта.

Информация о проекте или блоке проекта ПЛК может быть получена программой при обнаружении операций чтения проекта / блока из ПЛК или записи проекта / блока в ПЛК. Полученная информация сохраняется в Kaspersky Industrial CyberSecurity for Networks. При следующем обнаружении операции чтения или записи проекта / блока программа сравнивает полученную информацию о проекте / блоке и сохраненную информацию. Если полученная информация о проекте / блоке не совпадает с последней сохраненной информацией об этом проекте / блоке (в том числе при отсутствии сохраненной информации), программа регистрирует соответствующее событие.

Получение информации о проектах ПЛК поддерживается для устройств следующих типов:

- Schneider Electric серии Modicon: M580, M340;
- Siemens SIMATIC серий S7-300, S7-400.

Для контроля чтения и записи проектов ПЛК не требуется добавлять параметры контроля процесса для устройств. Контроль чтения и записи проектов ПЛК осуществляется для всех обнаруженных устройств перечисленных типов.

Для каждого устройства программа сохраняет не более 100 различных вариантов проектов ПЛК. Если проект ПЛК передается или принимается отдельными блоками, сохраняется до 100 различных вариантов каждого блока.

Если для устройства достигнуто ограничение максимального количества сохраненных проектов ПЛК (или одноименных блоков проекта ПЛК), программа сохраняет новый обнаруженный проект / блок вместо самого старого обнаруженного проекта / блока.

При контроле чтения и записи проектов ПЛК программа регистрирует события по технологии Контроль активов. Для регистрации используются системные типы событий (см. раздел "Системные типы событий по технологии Контроль активов" на стр. [419](#)), 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 разделе **Параметры** → **Типы событий** (см. раздел "**Настройка типов событий**" на стр. [225](#)).

Сведения о зарегистрированных событиях вы можете просмотреть при подключении к Серверу через веб-интерфейс (см. раздел "Мониторинг событий и инцидентов" на стр. [305](#)).

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 **Активы**.
2. На закладке **Устройства** выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. [273](#)), 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**.

Экспорт устройств в файл

Вы можете экспортировать сведения об устройствах в файлы следующих форматов:

- **Формат CSV.**

При экспорте в этот формат в файле сохраняется информация из граф, отображаемых в таблице в текущий момент, а также дополнительные поля (см. раздел "Просмотр сведений об устройстве" на стр. [275](#)) и параметры контроля процесса в сведениях об устройствах.
- **Формат JSON.**


При экспорте в этот формат в файле сохраняется вся доступная информация об устройствах, включая служебную информацию из базы данных (например, сведения об событиях, с которыми связаны устройства). Файл можно использовать для загрузки подробных данных об устройствах в другие системы.

Экспорт можно выполнять для всех устройств, удовлетворяющих текущим параметрам фильтрации и поиска, или выборочно для устройств, отображаемых в таблице.

► Чтобы экспортировать информацию о всех устройствах, удовлетворяющих текущим параметрам фильтрации и поиска, выполните следующие действия:

1. Выберите раздел **Активы**.
2. По ссылке **Экспорт** в панели инструментов на закладке **Устройства** откройте меню для выбора формата сохраняемого файла.
3. В открывшемся меню выберите пункт с нужным форматом файла: **файл формата CSV** или **файл формата JSON**.
4. Если в меню выбран пункт **файл формата CSV**, отобразится запрос для выбора варианта сохранения параметров контроля процесса и тегов, связанных с устройствами. Если вы хотите сохранить в файле параметры контроля процесса и теги, установите флажок **С параметрами контроля процесса и тегами** и нажмите на кнопку **Экспортировать**.

Запустится процесс формирования файла.

5. Если формирование файла занимает длительное время (более 15 секунд), операция по формированию файла переводится в список фоновых операций. В этом случае для загрузки файла выполните следующие действия:
 - a. Нажмите на кнопку  в меню веб-интерфейса программы.
Откроется список фоновых операций.
 - b. Дождитесь завершения операции формирования файла.
 - c. Нажмите на кнопку **Загрузить файл**.

Браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

► Чтобы экспортировать информацию о выбранных устройствах, выполните следующие действия:

1. Выберите раздел **Активы**.
2. На закладке **Устройства** выберите устройства (см. раздел "Выбор устройств в таблице устройств" на стр. [273](#)), информацию о которых вы хотите экспортировать в файл.
3. По правой клавише мыши откройте контекстное меню одного из выбранных устройств.
4. В контекстном меню выберите пункт, в которой указан нужный формат файла для экспорта (**в CSV-файл** или **в JSON-файл**).
5. Если в меню выбран пункт для экспорта в файл формата CSV, отобразится запрос для выбора варианта сохранения параметров контроля процесса и тегов, связанных с устройствами. Если вы хотите сохранить в файле параметры контроля процесса и теги, установите флажок **С параметрами контроля процесса и тегами** и нажмите на кнопку **Экспортировать**.


Запустится процесс формирования файла. Если формирование файла занимает длительное время (более 15 секунд), выполните действия пункта 5, описанные в процедуре экспорта информации о всех устройствах.

Экспорт подсетей в файл

Вы можете экспортировать сведения о подсетях в файл формата JSON. В файле сохраняется основная информация о подсетях независимо от того, какие графы отображаются в таблице подсетей в текущий момент.

Экспорт можно выполнять для всех подсетей, удовлетворяющих текущим параметрам фильтрации и поиска, или выборочно для подсетей, отображаемых в таблице.

► *Чтобы экспортировать информацию о всех подсетях, удовлетворяющих текущим параметрам фильтрации и поиска, выполните следующие действия:*

1. Выберите раздел **Активы**.
2. По ссылке **Экспорт** в панели инструментов на закладке **Подсети** откройте меню для выбора формата сохраняемого файла.
3. В открывшемся меню выберите пункт **файл формата JSON**.
Запустится процесс формирования файла.
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**.

Браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

► *Чтобы экспортировать информацию о выбранных подсетях, выполните следующие действия:*

1. Выберите раздел **Активы**.
2. На закладке **Подсети** выберите подсети (см. раздел "Выбор подсетей в таблице подсетей" на стр. [274](#)), информацию о которых вы хотите экспортировать в файл.
После выбора подсетей в правой части окна веб-интерфейса появится область деталей.
3. В кнопке **Экспортировать в** нажмите на ту часть, в которой указан формат файла: **JSON-файл**.
Запустится процесс формирования файла. Если формирование файла занимает длительное время (более 15 секунд), выполните действия пункта 4, описанные в процедуре экспорта информации о всех устройствах.

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 (см. раздел "Узлы на карте сети" на стр. [283](#)). Эти объекты обозначают отправителей и получателей сетевых пакетов в обнаруженных взаимодействиях.
- Группы устройств (см. раздел "Группы устройств на карте сети" на стр. [285](#)). Эти объекты соответствуют группам в дереве групп устройств. Группы содержат узлы, представляющие включенные в эти группы устройства, и дочерние группы.
- Соединения (см. раздел "Соединения на карте сети" на стр. [286](#)). 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.

В этом разделе

Узлы на карте сети	283
Группы устройств на карте сети	285
Соединения на карте сети	286
Просмотр подробных сведений об объектах	286
Изменение масштаба карты сети.....	288
Позиционирование карты сети	289
Закрепление и открепление узлов и групп.....	289
Изменение местоположения узлов и групп вручную.....	290
Автоматическое распределение узлов и групп.....	290
Фильтрация объектов на карте сети	291
Сохранение и загрузка параметров отображения карты сети.....	297
Поиск узлов на карте сети.....	300
Просмотр событий, связанных с узлами известных программе устройств	301
Просмотр событий, связанных с соединением	302
Просмотр сведений в таблице устройств по выбранным узлам	303
Просмотр сведений в таблице устройств по выбранному соединению	304

Узлы на карте сети





Узлы на карте сети могут быть следующих типов:

- Известное программе устройство. Узел этого типа представляет устройство, входящее в таблицу устройств (см. раздел "Настройка контроля активов" на стр. [120](#)).
- 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. Устройствами глобальной сети считаются все устройства, у которых IP-адреса принадлежат только известным программе подсетям (см. раздел "Просмотр подсетей для контроля активов" на стр. [270](#)) с типом **Публичная**.

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, имеют серый цвет фона.

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 (см. раздел "Дерево групп устройств" на стр. [277](#)) могут отображаться на карте сети в свернутом или развернутом состояниях. Свернутые группы отображаются в виде значков, аналогичных узлам (см. раздел "Узлы на карте сети" на стр. [283](#)). Развернутые группы отображаются в виде окон с включенными в них узлами и другими группами.

Отображаемая информация на свернутых группах

Если группа свернута, при максимальном масштабе карты 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.


Сворачивание и разворачивание групп

Если группа свернута, вы можете ее развернуть двойным щелчком мыши на значке группы. Если группа развернута, вы можете ее свернуть двойным щелчком мыши на заголовке окна этой группы или с помощью кнопки  в заголовке.

► *Чтобы одновременно развернуть несколько свернутых групп, выполните следующие действия:*

1. На карте сети выберите несколько свернутых групп, выполнив одно из следующих действий:
 - Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными группами.
 - Удерживая нажатой клавишу **CTRL**, выберите нужные свернутые группы с помощью мыши.
2. Нажмите на кнопку  в панели инструментов, которая расположена в левой части области отображения карты сети (кнопка доступна, если выбрана хотя бы одна свернутая группа).

► *Чтобы одновременно свернуть все развернутые группы,*

нажмите на кнопку  в панели инструментов, которая расположена в левой части области отображения карты сети (кнопка доступна, если развернута хотя бы одна группа).

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 одного из типов (см. раздел "Узлы на карте сети" на стр. [283](#)):
 - известное программе устройство;
 - неизвестное программе устройство;
 - общий узел неизвестных устройств – если соединение показывает взаимодействие с одним или несколькими неизвестными устройствами этого узла;
 - узел WAN – если соединение показывает взаимодействие, в котором отправителем сетевых пакетов является устройство глобальной сети (IP-адрес принадлежит только известным программе подсетям (см. раздел "Просмотр подсетей для контроля активов" на стр. [270](#)) с типом **Публичная**);
- свернутая группа (см. раздел "Группы устройств на карте сети" на стр. [285](#)), если соединение показывает взаимодействие с одним или несколькими устройствами в этой группе.

В зависимости от уровня 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 (см. раздел "Фильтрация объектов на карте сети" на стр. [291](#)). 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 (см. раздел "Настройка контроля активов" на стр. [120](#)).
- Если узел представляет одно неизвестное программе устройство, в области деталей отображаются MAC- и / или IP-адреса устройства.

- Если выбран общий узел неизвестных устройств (см. раздел "Узлы на карте сети" на стр. [283](#)), 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 известным программе подсетям (см. раздел "Просмотр подсетей для контроля активов" на стр. [270](#)), для которых указан тип **Публичная** (внешние 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 (см. раздел "Фильтрация объектов на карте сети" на стр. [291](#)). 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 (см. раздел "Группы устройств на карте сети" на стр. [285](#)), в разделе отображается имя группы и количество устройств и дочерних групп в ней.
 - Если стороной взаимодействия является общий узел неизвестных устройств (см. раздел "Узлы на карте сети" на стр. [283](#)), 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 на закладку **Устройства** в разделе **Активы** 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 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.

► 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.


Позиционирование 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.

Закрепление и открепление узлов и групп


По умолчанию узлы и свернутые группы не закреплены на карте сети. Незакрепленные узлы и свернутые группы могут автоматически перемещаться для оптимального отображения остальных объектов.

Закрепление узлов и групп происходит при изменении их местоположения вручную (см. раздел "Изменение местоположения узлов и групп вручную" на стр. [290](#)) или при автоматическом распределении (см. раздел "Автоматическое распределение узлов и групп" на стр. [290](#)). Также вы можете закрепить текущее местоположение отображаемых объектов, не перемещая их.

Для закрепления и открепления объектов без их перемещения вы можете использовать следующие элементы интерфейса:

- Кнопки в панели инструментов, которая расположена в левой части области отображения карты сети. С помощью кнопок  и  вы можете закрепить и открепить все узлы и группы, отображаемые на карте сети (в том числе узлы в развернутых группах).
- Кнопки в заголовке окна развернутой группы. С помощью кнопок  и  вы можете закрепить и открепить только узлы и группы в окне развернутой группы (но не в окнах вложенных групп).

Кнопки доступны, если на карте сети есть объекты, к которым можно применить соответствующие действия.

После того, как местоположение узла или свернутой группы закреплено, в правом верхнем углу этого элемента отображается значок  (если для карты сети задан масштаб не менее 25%). Вы также можете использовать этот значок для открепления объекта.

Местоположение закрепленного узла или закрепленной группы сохраняется. Если закрепленный узел перестал отображаться на карте сети (например, после применения фильтрации), при следующем появлении этот узел отобразится на том же месте.

Изменение местоположения узлов и групп вручную

Вы можете вручную изменять местоположение узлов и групп на карте сети, распределяя их наиболее удобным для вас способом.

После перемещения узлы и группы закрепляются на новом местоположении. При необходимости вы можете откреплять эти объекты (см. раздел "Закрепление и открепление узлов и групп" на стр. [289](#)).

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 использовать алгоритмы автоматического распределения для следующих объектов:

- Все отображаемые узлы и группы, относящиеся к верхнему уровню иерархии в дереве групп. Автоматическое распределение выполняется с помощью кнопок  (для распределения по радиальному принципу) и  (для распределения с выравниванием по сетке) в панели инструментов, которая расположена в левой части области отображения карты сети.
- Все отображаемые узлы и группы внутри развернутой группы. Автоматическое распределение выполняется с помощью кнопок  (для распределения по радиальному принципу) и  (для распределения с выравниванием по сетке) в заголовке окна развернутой группы.
- Только выбранные узлы и свернутые группы. Перед автоматическим распределением вам нужно выбрать не менее трех узлов и / или свернутых групп внутри развернутой группы или на верхнем уровне иерархии. Для выбора нескольких объектов вы можете выделить мышью прямоугольную область с нужными объектами, удерживая нажатой клавишу **SHIFT**, или выбрать нужные объекты с помощью мыши, удерживая нажатой клавишу **CTRL**. Автоматическое распределение выполняется с помощью кнопок  (для распределения по радиальному принципу) и  (для распределения с выравниванием по сетке) в панели инструментов, которая расположена в левой части области отображения карты сети.

После автоматического распределения узлы и группы закрепляются на новом месте. В этих объектах появляется значок . При необходимости вы можете открепить эти объекты (см. раздел "Закрепление и открепление узлов и групп" на стр. [289](#)).

Фильтрация объектов на карте сети

Для ограничения количества узлов и соединений, отображаемых на карте сети, вы можете использовать следующие функции:

- Функции для комплексной фильтрации узлов и соединений:
 - Фильтрация с помощью периода на временной шкале

Для фильтрации узлов и соединений вы можете выбрать нужный период времени на временной шкале. Временная шкала отображается в нижней части раздела **Карта сети**.

Временная шкала содержит 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 границей временной шкалы, обозначающей текущий момент.
- Период без привязки к текущему моменту. Период этого типа может быть размещен в любой части временной шкалы.

► *Чтобы настроить фильтрацию объектов по периоду с привязкой к текущему моменту, выполните следующие действия:*

1. Нажмите на кнопку **Сейчас** справа от временной шкалы. Кнопка не отображается, если период уже привязан к текущему моменту.
2. Если требуется указать другую длительность периода, выполните одно из следующих действий:
 - Переместите левую границу желтой полосы периода в нужное положение (максимальная длительность периода – 7 дней).
 - Откройте окно настройки с помощью кнопки над желтой полосой периода, установите флажок **Прикреплять к границе**, выберите нужную длительность (**Час, День, 7 дней**) и нажмите на кнопку **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 период в нужную часть временной шкалы с помощью мыши.
 - Переместите одну или обе границы желтой полосы периода в нужную часть временной шкалы (максимальная длительность периода – 7 дней).
 - Откройте окно настройки с помощью кнопки над желтой полосой периода, выберите нужную длительность (**Час, День, 7 дней**) и нажмите на кнопку **ОК**.
3. Если для периода автоматически устанавливается привязка к текущему моменту (при перемещении периода в крайнее правое положение перестает отображаться кнопка **Сейчас** справа от временной шкалы), выключите режим автоматического прикрепления периода к границе шкалы. Для этого откройте окно настройки с помощью кнопки над желтой полосой периода, снимите флажок **Прикреплять к границе** и нажмите на кнопку **ОК**.

- Фильтрация по зарегистрированным событиям

Вы можете отобразить на карте сети узлы и соединения, информация о которых сохранена в событиях, связанных с выбранными узлами.

Возможность фильтрации по событиям доступна, если выбрано не более 200 узлов на карте 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.

Фильтрацию по событиям можно выполнить следующими способами:

- Начальная фильтрация по событиям. Этот способ применяется, если требуется отфильтровать объекты по событиям, связанным только с выбранными узлами.
- Дополнительная фильтрация по событиям. Этот способ применяется, если уже выполнена начальная фильтрация по событиям (например, при переходе на карту сети из таблицы событий (см. раздел "Переход на карту сети для отображения информации по событиям" на стр. [320](#))) и требуется добавить к фильтру события, связанные с дополнительно выбранными узлами из числа отображаемых на карте сети.

► *Чтобы отобразить узлы и соединения с использованием начальной фильтрации по событиям, выполните следующие действия:*

1. На карте сети выберите один или несколько объектов, представляющих узлы и / или свернутые группы.

Для выбора нескольких узлов и / или групп выполните одно из следующих действий:

- Удерживая нажатой клавишу **SHIFT**, выделите мышью прямоугольную область с нужными объектами.
- Удерживая нажатой клавишу **CTRL**, выберите нужные объекты с помощью мыши.

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. Нажмите на кнопку **Отфильтровать по событиям**.

На карте сети отобразятся только те узлы и соединения, информация о которых содержится в событиях, связанных с выбранными узлами. В панели инструментов, которая расположена над картой сети, появится список с идентификаторами событий (идентификаторы перечислены в порядке обнаружения связанных событий).

► Чтобы добавить к отображаемым объектам узлы и соединения с использованием дополнительной фильтрации по событиям, выполните следующие действия:

1. Убедитесь, что выполнена начальная фильтрация по событиям. Для этого проверьте наличие списка с идентификаторами событий в панели инструментов, которая расположена над картой сети.
2. Среди отображаемых узлов на карте сети выберите те узлы, для которых вы хотите добавить связанные события к фильтру.

В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Добавить фильтрацию по событиям**.

На карте сети дополнительно отобразятся те узлы и соединения, информация о которых содержится в событиях, связанных с выбранными узлами. Идентификаторы обнаруженных событий добавятся в список с идентификаторами в панели инструментов.

- **Функции для фильтрации узлов:**

- **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**, **Важное**, **Критическое**).

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 (см. раздел "Настройка контроля активов" на стр. [120](#)), 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.

- Включение и выключение отображения узлов, связанных с отфильтрованными узлами

После фильтрации узлов 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 (см. раздел "Узлы на карте сети" на стр. [283](#)), 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.

- Функции для фильтрации соединений:
 - 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.

- Сброс параметров фильтрации

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 **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации).

На карте сети отобразятся все узлы и соединения, для которых были обнаружены взаимодействия в течение времени заданного периода.

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:

- масштаб (см. раздел "Изменение масштаба карты сети" на стр. [288](#));
- позиционирование карты сети (на стр. [289](#));

- местоположение закрепленных узлов и групп (см. раздел "Закрепление и открепление узлов и групп" на стр. [289](#));
- фильтрация узлов и соединений (см. раздел "Фильтрация объектов на карте сети" на стр. [291](#)).

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-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** настройте параметры отображения карты сети.
3. Откройте окно **Настройка видов карты сети** по ссылке **Настроить виды**.
4. Нажмите на кнопку **Добавить**.
5. В поле ввода введите имя вида.

Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: ! @ # № \$ % ^ & () [] { } ' , . - _.

Имя вида должно удовлетворять следующим требованиям:

- начинается и заканчивается любым символом, кроме пробела;
 - содержит до 100 символов;
 - не совпадает с именем другого вида (регистр символов не учитывается).
6. Нажмите на значок  справа от поля ввода.

- Обновление вида с сохранением текущих параметров отображения карты 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-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** настройте параметры отображения карты сети.
3. Откройте окно **Настройка видов карты сети** по ссылке **Настроить виды**.
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-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** откройте окно **Настройка видов карты сети** по ссылке **Настроить виды**.
3. Выберите вид, который вы хотите переименовать.
4. Нажмите на значок  справа от текущего имени вида.
5. В поле ввода введите новое имя вида.

Вы можете использовать буквы, цифры, пробел, а также следующие специальные символы: ! @ # № \$ % ^ & () [] { } ' , . - _.

Имя вида должно удовлетворять следующим требованиям:

- начинается и заканчивается любым символом, кроме пробела;
 - содержит до 100 символов;
 - не совпадает с именем другого вида (регистр символов не учитывается).
6. Нажмите на значок  справа от поля ввода.

- Удаление вида карты сети

► *Чтобы удалить вид, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Карта сети** откройте окно **Настройка видов карты сети** по ссылке **Настроить виды**.
3. Выберите вид, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.
Откроется окно с запросом подтверждения.
5. В окне запроса подтвердите удаление выбранного вида.

- Применение на карте сети параметров, сохраненных в виде

► *Чтобы применить на карте сети параметры, сохраненные в виде, выполните следующие действия:*

1. В разделе **Карта сети** откройте окно **Настройка видов карты сети** по ссылке **Настроить виды**.
2. Выберите нужный вид в списке.
3. Нажмите на кнопку **Применить**.
Откроется окно с запросом подтверждения.
4. В окне запроса подтвердите применение вида.

Поиск узлов на 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 (см. раздел "Таблица устройств" на стр. [262](#)), кроме граф **Статус**, **Состояние безопасности**, **Последнее появление**, **Последнее изменение** и **Создано**. Поиск также выполняется по значениям пользовательских полей для устройств.

► *Чтобы найти нужные узлы на карте сети,*

в разделе **Карта сети** введите поисковый запрос в поле **Поиск узлов**. Поиск инициируется по мере ввода символов в строку поиска.

Если найдены узлы, удовлетворяющие поисковому запросу, контуры этих узлов подсвечиваются желтым цветом. Аналогично подсвечиваются контуры свернутых групп, в которых найдены узлы. При этом в правой части поля **Поиск узлов** появляются следующие элементы:

- Порядковый номер текущего выбранного объекта (узла или свернутой группы с найденными узлами) среди результатов поиска.
- Общее количество найденных объектов (узлов и / или свернутых групп с найденными узлами).

В общем количестве найденных объектов не учитывается количество узлов в свернутых группах. Если вы хотите, чтобы узлы в группах также учитывались в результатах поиска, разверните свернутые группы.

- Стрелки для переходов между найденными объектами. Переходы выполняются в алфавитном порядке имен найденных объектов. При переходе к очередному объекту карта 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*.

Открывается 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 (см. раздел "Узлы на карте сети" на стр. [283](#)).
- Загрузка событий, связанных с соединениями с узлами в свернутой группе (см. раздел "Группы устройств на карте сети" на стр. [285](#)).

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.

Открывается 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.

- Если выбранные объекты относятся к различным типам или категориям устройств, вы можете исключить объекты определенных типов (например, узлы неизвестных программ устройств) или категорий (например, ПЛК). Для этого снимите флажок рядом с названием типа или категории.
- В зависимости от количества выбранных объектов нажмите на кнопку **Показать устройство** или **Показать устройства** (кнопка **Показать устройства** недоступна, если общее количество известных программ устройств в выборке превышает 200).

Откроется раздел **Активы**. В таблице устройств на закладке **Устройства** 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 программ устройствах, участвовавших во взаимодействиях. Для загрузки сведений выполняется переход к таблице устройств. В таблице устройств автоматически применяется фильтрация по идентификаторам известных программ устройств.

Вы можете просматривать сведения в таблице устройств только для соединений с узлами в свернутых группах (см. раздел "Группы устройств на карте сети" на стр. [285](#)).

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:*

- 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.
- 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.
- Если общее количество известных программ устройств в выборке превысило 200, отобразится предупреждение о большом количестве устройств. Для загрузки устройств, относящихся к соединениям с наиболее высокими уровнями важности, подтвердите решение в окне запроса.

Откроется раздел **Активы**. В таблице устройств на закладке **Устройства** 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 используется системный тип события (см. раздел "Системные типы событий по технологии Внешние системы" на стр. [425](#)), которому присвоен код 8000000001.

Правила корреляции событий встроены в программу и применяются независимо от политики безопасности (см. раздел "Управление политикой безопасности" на стр. [236](#)).

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 (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).

Сервер Kaspersky Industrial CyberSecurity for Networks регистрирует события и инциденты в соответствии с параметрами, заданными для регистрации типов событий. Вы можете настроить эти параметры в разделе Типы событий (см. раздел "Настройка типов событий" на стр. [225](#)) (для всех типов событий) и при настройке правил контроля процесса (см. раздел "Настройка контроля процесса" на стр. [152](#)) (только для событий, регистрируемых при срабатывании правил контроля процесса).

Для сокращения количества часто повторяющихся событий, которые не требуют внимания оператора, предусмотрена возможность создания разрешающих правил на события. События, удовлетворяющие разрешающим правилам, не регистрируются. Например, с помощью разрешающего правила можно временно выключить регистрацию всех событий с определенной точки мониторинга. Вы можете просматривать разрешающие правила для событий в разделе **Разрешающие правила**. Для таких правил указан тип EVT.

Программа сохраняет события и инциденты в базе данных на Сервере. Вы можете настроить параметры хранения событий и инцидентов (см. раздел "Управление параметрами хранения журналов в базе данных Сервера" на стр. [211](#)). По умолчанию база данных хранит 100 000 записей в течение 365 дней. При этом

если количество записей или период хранения превышают предельные значения, самые старые записи удаляются.

Файлы базы данных сохраняются на Сервере в директориях СУБД (см. раздел "Директории для хранения данных программы" на стр. [80](#)). Удаление или изменение любого файла в этих директориях может привести к нарушению работоспособности программы.

Вы можете просматривать информацию о событиях и инцидентах в следующих разделах веб-интерфейса Kaspersky Industrial CyberSecurity for Networks:




- Раздел **Мониторинг** – отображает общую информацию о последних событиях и инцидентах, зарегистрированных программой.
- Раздел **События** – отображает подробную информацию о событиях и инцидентах и предоставляет возможность загрузки информации из базы данных Сервера за любой период.

В этом разделе

Уровни важности событий.....	307
Технологии регистрации событий	307
Статусы событий.....	308
Таблица зарегистрированных событий	308
Выбор событий в таблице событий.....	309
Просмотр событий, включенных в инцидент.....	311
Фильтрация событий	311
Поиск событий.....	315
Сброс заданных параметров фильтрации и поиска в таблице событий.....	316
Сортировка событий.....	316
Настройка таблицы зарегистрированных событий.....	317
Просмотр подробных данных о событии	319
Просмотр сведений об устройствах, связанных с событиями	319
Переход на карту сети для отображения информации по событиям	320
Изменение статусов событий	321
Создание разрешающих правил для событий	321
Установка меток.....	324
Копирование событий в текстовый редактор	325
Экспорт событий в файл	325
Загрузка трафика для событий.....	328
Создание директории для экспорта событий на сетевой ресурс.....	329

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 (см. раздел "Изменение параметров системного типа события" на стр. [230](#)). 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 сторонних систем с использованием методов Kaspersky Industrial CyberSecurity for Networks API.
- **Контроль активов (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 (см. раздел "Изменение параметров системного типа события" на стр. [230](#)). 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 (см. раздел "Просмотр таблицы устройств" на стр. [265](#)) и на карте сети (см. раздел "Узлы на карте сети" на стр. [283](#)).

Изменение статусов событий и инцидентов выполняется вручную (см. раздел "Изменение статусов событий" на стр. [321](#)). 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 (см. раздел "Настройка типов событий" на стр. [225](#)) 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 (см. раздел "Просмотр событий, включенных в инцидент" на стр. [311](#));
- фильтровать события (см. раздел "Фильтрация событий" на стр. [311](#));
- осуществлять поиск событий (см. раздел "Поиск событий" на стр. [315](#));
- сортировать события (см. раздел "Сортировка событий" на стр. [316](#));
- настраивать таблицу зарегистрированных событий (см. раздел "Настройка таблицы зарегистрированных событий" на стр. [317](#));
- просматривать подробные данные о событии (см. раздел "Просмотр подробных данных о событии" на стр. [319](#));
- изменять статусы событий (см. раздел "Изменение статусов событий" на стр. [321](#));
- просматривать в таблице устройств сведения по событиям (см. раздел "Просмотр сведений об устройствах, связанных с событиями" на стр. [319](#));
- просматривать на карте сети узлы и соединения по событиям (см. раздел "Переход на карту сети для отображения информации по событиям" на стр. [320](#));
- устанавливать метки (см. раздел "Установка меток" на стр. [324](#));
- копировать события в текстовый редактор (см. раздел "Копирование событий в текстовый редактор" на стр. [325](#));
- экспортировать события в файл (см. раздел "Экспорт событий в файл" на стр. [325](#));
- загружать трафик событий (см. раздел "Загрузка трафика для событий" на стр. [328](#)).

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, 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 могут быть свернуты и развернуты с помощью кнопок **+** и **-** рядом с заголовками инцидентов.

Вы можете изменить режим отображения при настройке таблицы событий (см. раздел "Настройка таблицы зарегистрированных событий" на стр. [317](#)).

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 от раскрывающегося списка отобразятся начальная и конечная дата и время периода фильтрации.
4. Нажмите на дату начала или окончания периода.
Откроется календарь.
5. В календаре задайте дату начальной и конечной границ периода фильтрации. Для этого выберите дату в календаре (при этом будет указано текущее время) или введите значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс. Если указывать дату и время конечной границы периода фильтрации не требуется, вы можете не выбирать дату или удалить текущее значение.
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 начальной и конечной границ периода фильтрации. Для этого выберите дату в календаре (при этом будет указано текущее время) или введите значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс. Если указывать дату и время границы периода фильтрации не требуется, вы можете не выбирать дату или удалить текущее значение.
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 (см. ниже).
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 **X**, который расположен справа от поля с раскрывающимся списком.
5. Нажмите на кнопку **ОК**.

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)**.

► 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 (см. раздел "Просмотр событий, включенных в инцидент" на стр. [311](#)) 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 (см. раздел "Настройка таблицы зарегистрированных событий" на стр. [317](#)).

Поиск событий

Вы можете выполнять поиск событий и инцидентов в таблице событий.

Поиск выполняется по графам, содержащим символные 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 (см. раздел "Просмотр событий, включенных в инцидент" на стр. [311](#)) 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 (см. раздел "Настройка таблицы зарегистрированных событий" на стр. [317](#)).

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 **Фильтр по умолчанию** (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** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
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 (см. раздел "Фильтрация событий" на стр. [311](#)) и поиска (см. раздел "Поиск событий" на стр. [315](#)), 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 (см. раздел "Настройка типов событий" на стр. [225](#)). 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 (см. раздел "Уровни важности событий" на стр. [307](#)).
- **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 (см. раздел "Технологии регистрации событий" на стр. [307](#)).
- **Всего появлений.**

Для события, не являющегося инцидентом – значение счетчика повторов после регистрации события в течение времени разрешения повтора события (см. раздел "Настройка типов событий" на стр. [225](#)). 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 (см. раздел "Статусы событий" на стр. [308](#)).
- **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 (см. раздел "Установка меток" на стр. [324](#)), 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 (см. раздел "Выбор событий в таблице событий" на стр. [309](#)), 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 **Активы**. В таблице устройств на закладке **Устройства** будет применена фильтрация по идентификаторам устройств, которые соответствуют выбранным событиям.

Переход на карту сети для отображения информации по событиям

Вы можете отобразить на карте сети узлы и соединения на основе информации, сохраненной в событиях. Узлы для отображения на карте сети определяются по адресной информации отправителей и получателей сетевых пакетов в выбранных событиях. Для отображения соединений применяется фильтрация по времени взаимодействий, начиная от даты и времени регистрации первого события из числа выбранных событий.

Возможность отображения узлов и соединений на карте сети доступна, если в таблице событий выбрано не более 200 событий (в том числе в составе выбранных инцидентов).

► Чтобы отобразить на карте сети узлы и соединения по информации в событиях, выполните следующие действия:

1. Выберите раздел **События**.
2. В таблице событий выберите события и / или инциденты (см. раздел "Выбор событий в таблице событий" на стр. [309](#)), для которых вы хотите отобразить узлы и соединения на карте сети.

В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Показать на карте сети** (кнопка недоступна, если количество выбранных событий превышает 200).

Откроется раздел **Карта сети**. На карте сети отобразятся узлы и соединения по информации в выбранных событиях (будет применена начальная фильтрация по событиям (см. раздел "Фильтрация объектов на карте сети" на стр. [291](#))). При этом если выбран инцидент, в который продолжают добавляться события, на карте сети также отобразятся узлы и соединения по информации в новых событиях.

Изменение статусов событий

Вы можете изменять следующие статусы (см. раздел "Статусы событий" на стр. [308](#)) 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 изменить статус событий или инцидентов, выполните следующие действия:*

1. Выберите раздел **События**.
2. В таблице событий выберите события и / или инциденты (см. раздел "Выбор событий в таблице событий" на стр. [309](#)), статус которых вы хотите изменить.

В правой части окна веб-интерфейса появится область деталей.

3. Присвойте событиям и / или инцидентам нужный статус с помощью кнопок **В обработке** или **Обработано**. Кнопки недоступны в следующих случаях:

- Кнопка **В обработке** недоступна, если среди выбранных элементов отсутствуют события или инциденты со статусом *Новое*.
- Кнопка **Обработано** недоступна, если среди выбранных элементов отсутствуют события или инциденты со статусами *Новое* или *В обработке*.

Если выбраны все события и инциденты, удовлетворяющие текущим параметрам фильтрации и поиска, и количество выбранных элементов более 1000, программа не проверяет их статусы. В этом случае доступны обе кнопки с названиями статусов **В обработке** и **Обработано**. При этом с помощью кнопки **В обработке** вы можете присвоить статус *В обработке* только событиям и инцидентам со статусом *Новое*.

Откроется окно с запросом подтверждения.

4. В окне запроса нажмите на кнопку **ОК**.

Создание разрешающих правил для событий

Если требуется выключить регистрацию событий с определенными признаками (например, все события с точки мониторинга), вы можете создавать разрешающие правила для событий.

Создавать разрешающие правила для событий могут только пользователи с ролью Администратор.

Для создания разрешающих правил для событий вы можете использовать следующие возможности:

- Создание правила с изначально пустыми значениями параметров или со значениями из шаблона

► *Чтобы создать правило с изначально пустыми значениями параметров или со значениями из шаблона, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Разрешающие правила** откройте область деталей по ссылке **Добавить правило**.
3. Если вы хотите задать значения параметров из шаблона, в области деталей нажмите на кнопку **Использовать шаблон**, в открывшемся окне выберите нужный шаблон и нажмите на кнопку **Применить**.
4. В области деталей нажмите на кнопку **EVT**.
5. В поле **Протокол** укажите протокол, который будет указан в событиях.

При выборе поля **Протокол** откроется окно с таблицей поддерживаемых протоколов, отображаемых в виде дерева стека протоколов. Вы можете управлять отображением элементов дерева с помощью кнопок **+** и **-** рядом с названиями протоколов, которые содержат протоколы следующих уровней.

При необходимости воспользуйтесь поисковой строкой над таблицей, чтобы найти нужные протоколы (см. ниже).

6. При необходимости введите дополнительную информацию о правиле в поле **Комментарий**.
7. В блоках параметров **Сторона 1** и **Сторона 2** укажите доступную для изменения адресную информацию для сторон сетевого взаимодействия. В зависимости от выбранного протокола (или набора протоколов), адресная информация может содержать MAC-адрес, IP-адрес и / или номер порта.

Для автоматического заполнения адресной информации стороны сетевого взаимодействия вы можете выбрать известные программе устройства (см. ниже).

8. В поле **Тип события** укажите тип события (см. раздел "Настройка типов событий" на стр. [225](#)), числовой код которого указывается в событиях.

При выборе поля **Тип события** откроется окно со списком типов событий, которые могут быть указаны в разрешающих правилах. При необходимости воспользуйтесь поисковой строкой над списком, чтобы найти нужный тип события. Чтобы указать тип события, выберите его в списке и нажмите на кнопку **Применить**.

9. В поле **Точка мониторинга** укажите имя точки мониторинга, которое указывается в событиях.

При выборе поля **Точка мониторинга** откроется окно со списком всех точек мониторинга на всех узлах с установленными компонентами программы. При необходимости воспользуйтесь поисковой строкой над списком, чтобы найти имя нужной точки мониторинга. Чтобы указать имя точки мониторинга, выберите его в списке и нажмите на кнопку **Применить**.

10. В поле **Правило в событии** введите имя (или часть имени) правила, которое указывается в событиях в качестве сработавшего правила.
11. В области деталей нажмите на кнопку **Сохранить**.

Новое правило будет добавлено в таблицу разрешающих правил.

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.
- b. Нажмите на кнопку **ОК**.

Если выбран протокол, который программа может определять по содержимому сетевых пакетов, ниже поля **Протокол** появится пояснение об этом.

Для автоматического заполнения адресной информации стороны сетевого взаимодействия по сведениям об устройствах выполните следующие действия:

- a. Откройте окно выбора устройств по ссылке **Указать адреса устройств**.
- b. В окне выбора устройств установите флажки напротив тех устройств, которые вы хотите использовать.

Окно выбора устройств содержит таблицу, в которой можно настраивать отображение и порядок граф, выполнять фильтрацию, поиск и сортировку аналогично таблице устройств (см. раздел "Просмотр таблицы устройств" на стр. [265](#)) в разделе **Активы**.

- c. В окне выбора устройств нажмите на кнопку **ОК**.

- Создание нового правила на основе имеющегося правила

► *Чтобы создать новое разрешающее правило для событий на основе имеющегося правила, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. В разделе **Разрешающие правила** выберите правило, на основе которого вы хотите создать новое правило.
3. По правой 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 4–11, описанные в процедуре создания правила с изначально пустыми значениями параметров.

- Создание правила на основе зарегистрированного события

► *Чтобы создать новое разрешающее правило для событий на основе зарегистрированного события, выполните следующие действия:*

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **События**.
3. В таблице зарегистрированных событий выберите событие, на основе которого вы хотите создать разрешающее правило для событий.

В правой части окна веб-интерфейса появится область деталей.

4. В области деталей нажмите на кнопку **Создать разрешающее правило**.

В окне браузера откроется раздел **Разрешающие правила**. В правой части окна веб-интерфейса появится область деталей в режиме изменения параметров правила. Для параметров нового правила будут заданы значения, полученные из сохраненных сведений о событии.

5. При необходимости измените параметры нового правила. Для этого выполните пункты 4–11, описанные в процедуре создания правила с изначально пустыми значениями параметров. Если изменять параметры нового правила не требуется, сохраните правило с помощью кнопки **Сохранить**.

Установка меток

Вы можете присваивать событиям и инцидентам определенные метки в разделе **События** веб-интерфейса программы.

Метка – значок, который позволяет легко находить события и инциденты по критерию, отсутствующему в таблице.

► *Чтобы установить метку для события или инцидента, 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 копирования доступна, если выбрано не более 200 событий и инцидентов.

► *Чтобы скопировать события и / или инциденты в текстовый редактор, выполните следующие действия:*

1. Выберите раздел **События**.
2. В таблице событий выберите события и / или инциденты (см. раздел "Выбор событий в таблице событий" на стр. [309](#)), 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 выбрано одно событие или инцидент.
 - **Копировать детали выбранных событий**, если выбрано несколько событий и / или инцидентов.
5. Откройте любой текстовый редактор.
6. В окне текстового редактора выполните вставку (например, с помощью комбинации клавиш **CTRL+V**).

Скопированная информация о событии будет доступна для изменения в текстовом редакторе. Информация о нескольких событиях будет разделена пустой строкой.

Экспорт событий в файл


Экспорт событий при подключении к Серверу через веб-интерфейс

При подключении к Серверу через веб-интерфейс вы можете экспортировать информацию о событиях (в том числе об инцидентах) в файлы следующих форматов:

- **Формат CSV.**
При экспорте в этот формат в файле сохраняется информация из граф, отображаемых в таблице в текущий момент.
- **Формат JSON.**
При экспорте в этот формат в файле сохраняется вся доступная информация о событиях, включая служебную информацию из базы данных (например, сведения об устройствах, с которыми связаны события). Файл можно использовать для загрузки подробных данных о событиях в другие системы.

Экспорт в файлы форматов CSV и JSON можно выполнять для всех событий, удовлетворяющих текущим параметрам фильтрации и поиска, или выборочно для событий, отображаемых в таблице.

► Чтобы экспортировать информацию о всех событиях, удовлетворяющих текущим параметрам фильтрации и поиска, выполните следующие действия:

1. Выберите раздел **События**.
2. По ссылке **Экспорт** в панели инструментов откройте меню для выбора формата сохраняемого файла.
3. В открывшемся меню выберите пункт с нужным форматом файла: **файл формата CSV** или **файл формата JSON**.
Запустится процесс формирования файла.
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**.

Браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

► Чтобы экспортировать информацию о выбранных событиях, выполните следующие действия:

1. Выберите раздел **События**.
2. В таблице событий выберите события (см. раздел "Выбор событий в таблице событий" на стр. [309](#)), информацию о которых вы хотите экспортировать в файл.
После выбора событий в правой части окна веб-интерфейса появится область деталей.
3. В кнопке **Экспортировать в: CSV-файл или JSON-файл** нажмите на ту часть, в которой указан нужный формат файла.
Запустится процесс формирования файла. Если формирование файла занимает длительное время (более 15 секунд), выполните действия пункта 4, описанные в процедуре экспорта информации о всех событиях.

Экспорт событий с помощью утилиты экспорта

В Kaspersky Industrial CyberSecurity for Networks вы можете экспортировать события и инциденты в файлы формата XML с помощью утилиты экспорта событий. Утилита предназначена для использования на компьютерах под управлением операционной системы Astra Linux SE 1.6. Файл для запуска утилиты export.xml входит в комплект поставки Kaspersky Industrial CyberSecurity for Networks.

Утилита экспорта событий сохраняет файлы с информацией о событиях и инцидентах в указанной директории. Информация о каждом событии или инциденте сохраняется в виде отдельного файла, в имени которого указан идентификатор события или инцидента. Файл содержит всю доступную информацию о событии или инциденте, включая служебную информацию из базы данных (например, сведения об устройствах, с которыми связаны события).

С помощью утилиты экспорта событий выполняется экспорт всех событий и инцидентов, зарегистрированных в течение указанного промежутка времени.

Утилита экспорта событий подключается к Серверу программы через коннектор, который должен быть предварительно добавлен в программу.

► *Чтобы подготовить программу к использованию утилиты экспорта событий, выполните следующие действия:*

1. Добавьте в программу коннектор (см. раздел "Добавление коннектора" на стр. [218](#)), через который утилита экспорта событий будет подключаться к Серверу программы. Для коннектора укажите системный тип **Generic** (см. раздел "**Управление коннекторами**" на стр. [216](#)).
2. На компьютере, на котором будет использоваться утилита, создайте произвольную директорию для сохранения экспортированных файлов. В качестве такой директории вы можете использовать специально созданную директорию для сохранения файлов на сетевой ресурс (см. раздел "Создание директории для экспорта событий на сетевой ресурс" на стр. [329](#)).
3. Скопируйте на компьютер файл для запуска утилиты export-xml из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.
4. Перейдите в директорию с файлом export-xml и введите команду для предоставления прав на запуск файла:

```
sudo chmod +x ./export-xml
```
5. Если файл свертки, полученный при выполнении пункта 1, отсутствует на компьютере, на котором будет использоваться утилита, скопируйте этот файл на компьютер (например, в директорию, в которой находится файл export-xml).

► *Чтобы экспортировать информацию о событиях с помощью утилиты экспорта событий, выполните следующие действия:*

1. На компьютере, на котором будет использоваться утилита, откройте консоль операционной системы и перейдите в директорию с файлом export-xml.
2. В командной строке введите команду:

```
./export-xml -p <пароль для доступа к сертификату коннектора> \  
-c <путь к файлу свертки> \  
-f <дата и время начала периода регистрации событий> \  
-t <дата и время окончания периода регистрации событий> \  
-d <имя директории для сохранения файлов> \  
-m <идентификатор производителя программы> \  
-i <идентификатор экземпляра программы> \  
-z <смещение относительно времени UTC>
```

где:

- <пароль для доступа к сертификату коннектора> – пароль, заданный при добавлении коннектора, через который утилита экспорта событий подключается к Серверу программы (обязательный параметр).
- <путь к файлу свертки> – полный путь и имя файла свертки, созданного при добавлении коннектора, через который утилита экспорта событий подключается к Серверу программы (обязательный параметр).
- <дата и время начала периода регистрации событий>, <дата и время окончания периода регистрации событий> – начальная и конечная дата и время периода, в течение которого были зарегистрированы события для экспорта (обязательные параметры). Формат записи значения: ГГГГ-ММ-ДДТч:мм:сс (например: 2021-05-23T13:45:21).

- `<имя директории для сохранения файлов>` – полный путь к директории для сохранения экспортированных файлов (обязательный параметр).
- `<идентификатор производителя программы>` – идентификатор в диапазоне 0–9999, представляющий производителя программы (по умолчанию 55).
- `<идентификатор экземпляра программы>` – идентификатор в диапазоне 0–9999, представляющий экземпляр программы (по умолчанию 1).
- `<смещение относительно времени UTC>` – положительное или отрицательное смещение относительно времени UTC для заданных границ периода регистрации событий, выражается в минутах (по умолчанию 180 минут, что соответствует положительному смещению 3 часа).

Пример:

```
./export-xml -p Password1234 -c ./connectorXML.zip -f 2021-05-23T13:45:21 -t 2021-05-23T14:45:21 -d ./output -i 12
```

После завершения работы утилиты проверьте наличие файлов экспортированных событий в заданной директории.

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 (см. раздел "Настройка автоматического сохранения трафика для системных типов событий" на стр. [230](#)). 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 (см. раздел "Управление параметрами сохранения трафика в базе данных Сервера" на стр. [212](#)) 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 (см. раздел "Выбор событий в таблице событий" на стр. [309](#)), 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**.

Браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

Создание директории для экспорта событий на сетевой ресурс

Вы можете экспортировать события в файл (см. раздел "Экспорт событий в файл" на стр. [325](#)) с сохранением файла на сетевом ресурсе компьютера, который выполняет функции Сервера. Для этого вы можете использовать протокол Network File System (NFS), с помощью которого выполняется монтирование общего сетевого ресурса другого компьютера (например, точки экспорта сервера NFS) в локальной файловой системе компьютера Сервера. Создание директории и монтирование общего сетевого ресурса выполняется с помощью стандартных средств операционной системы.

При использовании протокола NFS в операционной системе активируется программный пакет `grsecbind`. Следует учитывать, что злоумышленники могут попытаться использовать этот программный пакет для проведения некоторых типов DDoS-атак. Для устранения угрозы проникновения требуется выполнить настройку сетевого экрана. В операционной системе Astra Linux SE 1.6 рекомендуется использовать программу настройки сетевой защиты UFW.

Создание директории и монтирование общего сетевого ресурса вручную

► Чтобы создать директорию для сохранения файлов на сетевой ресурс, выполните следующие действия:

1. Откройте консоль операционной системы.
2. Создайте локальную директорию для монтирования общего сетевого ресурса. Для этого введите команду:

```
mkdir <полный путь локальной директории>
```

Например:

```
mkdir ~/nfsshare
```

3. После создания директории введите команду монтирования сетевого ресурса:

```
sudo mount -t nfs <имя или IP-адрес удаленного компьютера>:\
<полный путь общего сетевого ресурса>\
<полный путь локальной директории>
```

Например:

```
sudo mount -t nfs nfs-server.example:/nfsshare ~/nfsshare
```

4. Проверьте результат монтирования с помощью команды:

```
mount | grep <полный путь локальной директории>
```

Например:

```
mount | grep ~/nfsshare
```

При успешном монтировании будут выведены данные, содержащие имя или IP-адрес удаленного компьютера, имя общего сетевого ресурса и имя родительской директории.

Автоматическое монтирование общего сетевого ресурса

- Чтобы настроить автоматическое монтирование общего ресурса в операционной системе Astra Linux SE 1.6, выполните следующие действия:

1. Проверьте наличие пакета `libpam-mount`. В операционной системе Astra Linux SE 1.6 этот пакет может быть не установлен по умолчанию.

Для проверки наличия пакета введите в командной строке команду:

```
dpkg -l libpam-mount
```

Если пакет `libpam-mount` не обнаружен в операционной системе, установите этот пакет с помощью команды:

```
sudo apt install libpam-mount
```

После ввода команды выполните необходимые действия по запросам системы.

2. Откройте файл `/etc/security/pam_mount.conf.xml` для редактирования с `root`-правами и отредактируйте или добавьте строку тега `volume` в пределах тега `pam_mount`:

```
<volume fstype="nfs" server="<имя или IP-адрес удаленного компьютера>"
path="<полный путь общего сетевого ресурса>" mountpoint="<полный путь
локальной директории>" user="<имя пользователя>" options="defaults" />
```

Пример значений для строки тега `volume`:

```
<volume fstype="nfs" server="nfs-server.example" path="/nfsshare"
mountpoint="/home/%(USER)/nfsshare" user="user1" options="defaults" />
```

где `user1` – имя пользователя, для которого при входе в систему сетевой ресурс `nfs-server.example/nfsshare` будет подключен как директория `/home/user1/nfsshare`.

Контроль уязвимостей устройств

Kaspersky Industrial CyberSecurity for Networks может обнаруживать уязвимости в контролируемых устройствах промышленной сети. *Уязвимость* – это недостаток в программном или аппаратном обеспечении устройства, используя который злоумышленник может повлиять на работу информационной системы или получить несанкционированный доступ к информации.

Программа обнаруживает уязвимости, анализируя имеющиеся сведения об устройствах. Сведения, по которым можно найти известную уязвимость для устройства, сравниваются с определенными полями в базе данных известных уязвимостей. Например, для сравнения могут использоваться сведения о версиях программного обеспечения на устройствах. Kaspersky Industrial CyberSecurity for Networks сравнивает сведения об устройствах с теми полями в базе данных, которые описывают подверженные уязвимостям устройства. При выявлении соответствия программа регистрирует событие об обнаружении уязвимости устройства, после чего загружает информацию об этой уязвимости из базы данных известных уязвимостей.

База данных известных уязвимостей встроена в программу. Эту базу данных формируют специалисты "Лаборатории Касперского", размещая в ней сведения о наиболее актуальных или часто встречающихся уязвимостях устройств в промышленных сетях. База данных содержит описания уязвимостей и устройств, которые подвержены этим уязвимостям, а также рекомендации для защиты системы (в виде текстов или ссылок на общедоступные ресурсы). В базу данных могут быть загружены описания и рекомендации из различных источников (например, от производителей устройств или программного обеспечения). Описания и рекомендации приводятся на английском языке.

После установки программы используется исходная база данных известных уязвимостей. Вы можете поддерживать базу данных в актуальном состоянии, устанавливая обновления (см. раздел "Обновление баз и программных модулей" на стр. 110).

Основным параметром, который идентифицирует уязвимость в базе данных программы, является идентификационный номер, присвоенный этой уязвимости в списке общеизвестных уязвимостей и рисков (Common Vulnerabilities and Exposures – CVE). Этот идентификационный номер называется *CVE-идентификатором*.

Вы можете просматривать информацию об уязвимостях устройств на странице веб-интерфейса Сервера (см. раздел "О веб-интерфейсе Сервера в основном режиме работы программы" на стр. 64) в следующих разделах:

- **Уязвимости** – отображает подробную информацию обо всех уязвимостях, обнаруженных программой.
- **Активы** – на закладке **Устройства** отображает списки CVE-идентификаторов обнаруженных уязвимостей в графе **Уязвимости** и в области деталей выбранного устройства.

В этом разделе

Сценарий реализации для процесса непрерывного управления уязвимостями	332
Сведения об устройствах, используемые для проверки уязвимостей	334
Просмотр устройств с обнаруженными уязвимостями	334
Просмотр таблицы уязвимостей	335
Выбор уязвимостей в таблице уязвимостей	340
Просмотр сведений об уязвимости	341
Автоматическое изменение состояний уязвимостей	341
Изменение состояний уязвимостей вручную	342
Просмотр сведений об устройствах с обнаруженной уязвимостью	342
Просмотр событий, связанных с уязвимостью	343
Экспорт уязвимостей в файл	343

Сценарий реализации для процесса непрерывного управления уязвимостями

С помощью функциональности контроля активов и обнаружения уязвимостей вы можете реализовать непрерывное (циклическое) управление уязвимостями в устройствах промышленной сети. Для управления уязвимостями Kaspersky Industrial CyberSecurity for Networks предоставляет информацию об обнаруженных уязвимостях, на основе которой вы можете предпринять соответствующие меры по устранению уязвимостей и минимизации рисков. Непрерывность процесса управления уязвимостями обеспечивается за счет автоматического обновления сведений об устройствах и уязвимостях в программе.

Сценарий реализации для процесса непрерывного управления уязвимостями состоит из следующих этапов:

1. Инвентаризация устройств и отслеживание сведений об устройствах

Этот этап реализуется с использованием методов обнаружения активности устройств и обнаружения сведений об устройствах (применение методов должно быть включено (см. раздел "Выбор применяемых методов и изменение режима контроля активов" на стр. [123](#))). На этом этапе программа автоматически обнаруживает новые устройства и обновляет сведения об устройствах. Для всех сведений, определяющих классификацию и эксплуатационные особенности устройств (например, информация о модели и версии программного обеспечения на устройстве), требуется включить автоматическое изменение в параметрах устройств (см. раздел "Изменение сведений об устройстве" на стр. [150](#)). Если автоматическое изменение таких сведений не может выполняться по каким-либо причинам, эти сведения следует актуализировать вручную.

2. Сканирование устройств на наличие уязвимостей

Этот этап реализуется с использованием метода обнаружения уязвимостей (применение метода должно быть включено (см. раздел "Выбор применяемых методов и изменение режима контроля активов" на стр. [123](#))). Сканирование выполняется по имеющимся сведениям об устройствах. Запуск сканирования происходит автоматически после обновления базы данных известных уязвимостей в программе или после добавления / изменения тех сведений об устройствах, которые используются для сравнения с полями в базе данных (например, после сохранения информации о модели и версии программного обеспечения на устройстве).

3. Оценка обнаруженных уязвимостей и классификация рисков

Для каждой обнаруженной уязвимости указано значение оценки ее критичности по общей системе оценки уязвимостей (Common Vulnerability Scoring System – CVSS). В зависимости от числового значения этой оценки уязвимость может относиться к уровням критичности *Низкий* (оценки 0.0–3.9), *Средний* (оценки 4.0–6.9) или *Высокий* (оценки 7.0–10.0). Уровни критичности обнаруженных уязвимостей влияют на состояния безопасности связанных с ними устройств (так же, как и необработанные события, относящиеся к этим устройствам).

На основании уровней критичности со значениями оценок, а также с учетом факторов, связанных с особенностями работы устройств, можно классифицировать риски эксплуатации обнаруженных уязвимостей. Если риск, связанный с эксплуатацией уязвимости, оценивается как незначительный, эту уязвимость можно перевести (см. раздел "Изменение состояний уязвимостей вручную" на стр. 342) из состояния *Актуальна* (в котором уязвимость находится по умолчанию после обнаружения) в состояние *Принята*. Например, в случае, если условия для эксплуатации уязвимости не могут быть воспроизведены. Все уязвимости, по которым требуется выполнить какие-либо дополнительные действия, следует оставить в состоянии *Актуальна*.

4. Устранение уязвимостей и минимизация рисков

На этом этапе вам нужно устранить актуальные уязвимости или минимизировать риски, связанные с их эксплуатацией. Действия по устранению уязвимостей и минимизации рисков могут включать получение, проверку и установку необходимых исправлений или обновлений для устройств, организационные меры (например, изоляция уязвимых устройств от внешних сетей) или замену уязвимых устройств.

Вы можете получить информацию о рекомендуемых действиях, просматривая сведения об обнаруженных уязвимостях. Рекомендации для защиты системы представлены в виде текстов или ссылок на общедоступные ресурсы.

Действия по устранению уязвимостей и минимизации рисков выполняются без участия Kaspersky Industrial CyberSecurity for Networks.

5. Проверка устранения уязвимостей

Этот этап аналогичен этапу сканирования устройств на наличие уязвимостей. При изменении сведений об устройстве программа автоматически переводит связанную с ним уязвимость из состояния *Актуальна* в состояние *Устранена*, если сведения об устройстве больше не соответствуют полям в базе данных, которые описывают уязвимость с тем же CVE-идентификатором (например, после изменения сведений о версии программного обеспечения на устройстве). Также в состояние *Устранена* переводятся те уязвимости, для которых больше нет связанных устройств (в случае удаления (см. раздел "Удаление устройств" на стр. 129) этих устройств) или больше нет описания в базе данных известных уязвимостей (в случае удаления описания из базы данных после загрузки обновлений (см. раздел "Обновление баз и программных модулей" на стр. 110)).

Если сведения об устройстве, с которым связана уязвимость, не изменились (например, минимизация рисков была выполнена путем изоляции уязвимого устройства от внешних сетей), вы можете вручную перевести эту уязвимость из состояния *Актуальна* в состояние *Принята*.

6. Возвращение устройств в состояние безопасности ОК

При регистрации события об обнаружении уязвимости изменяется состояние безопасности устройства, для которого обнаружена уязвимость. Состояние безопасности устройства изменяется в зависимости от уровня важности события.

Устройство возвращается в состояние безопасности **ОК** после присвоения статуса *Обработано* всем событиям, которые связаны уязвимостями этого устройства. При переводе уязвимости в состояние *Устранена* или *Принята* программа автоматически присваивает статус *Обработано* соответствующим событиям. Аналогично, если вы присвоили статус *Обработано* событию об обнаружении уязвимости, которая находится в состоянии *Актуальна*, эта уязвимость переводится в состояние *Принята*.

Сведения об устройствах, используемые для проверки уязвимостей

При сканировании устройств на наличие уязвимостей, как и при проверке устранения уязвимостей, программа использует следующие сведения об устройствах:

- **Производитель оборудования.**
- **Модель оборудования.**
- **Версия оборудования.**
- **Производитель ПО.**
- **Название ПО.**
- **Версия ПО.**

Программа сравнивает эти сведения с описаниями устройств в соответствующих полях базы данных известных уязвимостей. В базе данных описания устройств хранятся в формате языка CPE (Common Platform Enumeration). Программа сравнивает сведения с этими описаниями, автоматически преобразовывая сведения в формат языка CPE.

Для каждой уязвимости содержимое совпавших описаний приводится в области деталей в разделе **Совпавшие CPE**. В зависимости от того, какой тип сведений об устройстве совпал с описанием устройства в базе данных, в разделе **Совпавшие CPE** могут отображаться следующие сведения:

- **CPE-код оборудования, Описание оборудования** – если с описаниями в базе данных совпали сведения об устройстве **Производитель оборудования, Модель оборудования и Версия оборудования**.
- **CPE-код ПО, Описание ПО** – если с описаниями в базе данных совпали сведения об устройстве **Производитель ПО, Название ПО и Версия ПО**.

Просмотр устройств с обнаруженными уязвимостями

В таблице устройств (см. раздел "Таблица устройств" на стр. [262](#)) отображаются CVE-идентификаторы уязвимостей, которые находятся в состоянии *Актуальна* (сведения об уязвимостях в других состояниях не отображаются в таблице устройств). CVE-идентификаторы отображаются в графе **Уязвимости** и в области деталей при выборе устройства. Вы можете использовать CVE-идентификатор для вызова окна деталей уязвимости.

Для обозначения уровней критичности уязвимостей CVE-идентификаторы могут быть окрашены одним из следующих цветов:

- Красный – уязвимость с уровнем критичности *Высокий*.
- Желтый – уязвимость с уровнем критичности *Средний*.
- Синий – уязвимость с уровнем критичности *Низкий*.

По умолчанию в графе **Уязвимости** отображаются CVE-идентификаторы уязвимостей в состоянии *Актуальна* с любыми значениями оценок по системе CVSS. При этом внутри ячеек CVE-идентификаторы отсортированы в порядке убывания значений оценок.

При просмотре таблицы устройств (см. раздел "Просмотр таблицы устройств" на стр. [265](#)) вы можете настроить параметры фильтрации, сортировки или поиска устройств по CVE-идентификаторам уязвимостей.

Просмотр таблицы уязвимостей

Таблица уязвимостей отображается в разделе **Уязвимости** веб-интерфейса программы. В таблице могут отображаться сведения как об уязвимостях в состоянии *Актуальна*, так и об уязвимостях в состояниях *Устранена* или *Принята*.

При просмотре таблицы уязвимостей вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице уязвимостей

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

1. В разделе **Уязвимости** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
2. Установите флажки напротив тех параметров, которые вы хотите просматривать в таблице. Требуется выбрать хотя бы один параметр (см. ниже).
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 уязвимостей.

Для выбора доступны следующие параметры:

- **CVE.**

CVE-идентификатор обнаруженной уязвимости.

- **Группа устройств.**

Имя группы, в которую помещено устройство с обнаруженной уязвимостью (содержит имя самой группы и имена всех ее родительских групп).

- **Устройство.**

Имя и IP-адрес устройства (если IP-адрес не задан, отображается MAC-адрес).

- **Оценка CVSS.**

Значение оценки критичности уязвимости по системе CVSS. Числовое значение определяет, к какому уровню критичности относится уязвимость. В зависимости от уровня критичности, значение оценки может быть окрашено одним из следующих цветов:

- Красный – уязвимость с уровнем критичности *Высокий*.
- Желтый – уязвимость с уровнем критичности *Средний*.
- Синий – уязвимость с уровнем критичности *Низкий*.

Для уязвимостей в состоянии *Актуальна* значение оценки окрашено ярким цветом. Если уязвимость переведена в состояние *Устранена* или *Принята*, ее значение оценки окрашено бледным цветом.

- **Состояние.**

Текущее состояние уязвимости. Предусмотрены следующие состояния:

- *Актуальна* – автоматически установленное состояние уязвимости при ее первом обнаружении (а также при повторном обнаружении, если уязвимость находилась в состоянии *Устранена*). Также уязвимость можно вручную перевести в состояние *Актуальна* из состояния *Принята*.
- *Устранена* – автоматически установленное состояние уязвимости, если сведения об устройстве больше не соответствуют полям в базе данных, которые описывают уязвимость с тем же CVE-идентификатором (в том числе если удалено само устройство или удалено описание уязвимости из базы данных известных уязвимостей).
- *Принята* – в это состояние можно вручную перевести уязвимость из состояния *Актуальна*, если риск, связанный с эксплуатацией уязвимости, оценивается как незначительный или минимизирован организационными мерами.

- **Опубликовано.**

Дата и время публикации информации об уязвимости производителем оборудования или программного обеспечения (VendorAdvisory).

- **Первое обнаружение.**

Дата и время первого обнаружения уязвимости по сведениям об устройстве.

- **Последнее обнаружение.**

Дата и время последнего обнаружения уязвимости по сведениям об устройстве.

- **Условия эксплуатации.**

Описание условий эксплуатации уязвимости.

- **Возможные последствия.**

Описание возможных последствий при эксплуатации уязвимости.

- **Совпавшие CVE.**

Описания устройств, хранящиеся в базе данных известных уязвимостей. Приводятся описания, которые совпали со сведениями об устройстве в таблице устройств. Описания представлены в формате языка CPE (**CPE-код оборудования / CPE-код ПО**) и в текстовом виде (**Описание оборудования / Описание ПО**).

- **Вектор.**

Запись метрик для вычисления оценки уязвимости по системе CVSS.

- **Описание.**

Текстовое описание уязвимости из базы данных известных уязвимостей.

- Фильтрация по стандартным периодам

► Чтобы настроить фильтрацию уязвимостей по стандартному периоду, выполните следующие действия:

1. В разделе **Уязвимости** выполните одно из следующих действий:
 - откройте раскрывающийся список **Период обнаружения** в панели инструментов;
 - нажмите на значок фильтрации в графе **Последнее обнаружение**.
2. В раскрывающемся списке выберите один из стандартных периодов:
 - **Последние 24 часа.**
 - **Последняя неделя.**
 - **Последний месяц.**
 - **Последний год.**

В таблице отобразятся уязвимости за указанный вами период.

- Фильтрация по заданному периоду


► Чтобы настроить фильтрацию уязвимостей по заданному периоду, выполните следующие действия:

1. В разделе **Уязвимости** выполните одно из следующих действий:
 - откройте раскрывающийся список **Период обнаружения** в панели инструментов;
 - нажмите на значок фильтрации в графе **Последнее обнаружение**.
2. В раскрывающемся списке выберите **Задать период**.
Справа от раскрывающегося списка отобразятся начальная и конечная дата и время периода фильтрации.
3. Нажмите на дату начала или окончания периода.
Откроется календарь.
4. В календаре задайте дату начальной и конечной границ периода фильтрации. Для этого выберите дату в календаре (при этом будет указано текущее время) или введите значение вручную в формате ДД.ММ.ГГГГ чч:мм:сс. Если указывать дату и время конечной границы периода фильтрации не требуется, вы можете не выбирать дату или удалить текущее значение.
5. Нажмите на кнопку **ОК**.

В таблице отобразятся уязвимости за указанный вами период.

- Фильтрация по графам таблицы



► Чтобы отфильтровать уязвимости по графе **CVE, Устройство, Условия эксплуатации, Возможные последствия, Вектор или Совпавшие CVE**, выполните следующие действия:

1. В разделе **Уязвимости** нажмите на значок фильтрации в нужной графе таблицы.
Откроется окно фильтрации.
2. В полях **Включая** и **Исключая** введите значения для уязвимостей, 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 уязвимости по графе **Оценка CVSS или Состояние**, выполните следующие действия:

1. В разделе **Уязвимости** нажмите на значок фильтрации в нужной графе таблицы.
Для фильтрации по оценкам CVSS или по состояниям 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 уязвимости по графе **Группа устройств**, выполните следующие действия:

1. В разделе **Уязвимости** нажмите на значок фильтрации в графе **Группа устройств**.
Откроется окно фильтрации.
2. Нажмите на значок  в правой части поля, чтобы указать группу.
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 (ИЛИ)** 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 **Опубликовано** или **Первое обнаружение**, выполните следующие действия:

1. В разделе **Уязвимости** 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**.

- Поиск уязвимостей

► Чтобы найти нужные уязвимости,

в разделе **Уязвимости** введите поисковый запрос в поле **Поиск уязвимостей**. Поиск инициируется во время ввода символов.

В таблице отобразятся уязвимости, которые удовлетворяют условиям поиска.

Поиск выполняется по всем графам, кроме граф **Оценка CVSS**, **Состояние**, **Опубликовано**, **Первое обнаружение** и **Последнее обнаружение**.

- Сброс заданных параметров фильтрации и поиска

► Чтобы сбросить заданные параметры фильтрации и поиска в таблице уязвимостей,

в панели инструментов в разделе **Уязвимости** нажмите на кнопку **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации или поиска).

- Сортировка уязвимостей

Вы можете отсортировать уязвимости, отображаемые в таблице уязвимостей. Сортировку можно выполнить по значениям любой графы, кроме графы **Описание**.

► Чтобы отсортировать уязвимости, выполните следующие действия:

1. В разделе **Уязвимости** 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.

Выбор уязвимостей в таблице уязвимостей

В таблице уязвимостей вы можете выбирать уязвимости для просмотра сведений и для работы с этими уязвимостями. При выборе уязвимостей в правой части окна веб-интерфейса появляется область деталей.

► Чтобы выбрать нужные уязвимости в таблице, выполните одно из следующих действий:

- Если вы хотите выбрать одну уязвимость, установите флажок напротив этой уязвимости или выберите уязвимость с помощью мыши.
- Если вы хотите выбрать несколько уязвимостей, установите флажки напротив нужных уязвимостей или выберите их, удерживая нажатой клавишу **CTRL** или **SHIFT**. При выборе нескольких уязвимостей программа проверяет состояние выбранных уязвимостей и определяет наличие актуальных, устаревших и принятых уязвимостей среди выбранных.
- Если вы хотите выбрать все уязвимости, удовлетворяющие текущим параметрам фильтрации и поиска, выполните одно из следующих действий:
 - выберите любую уязвимость в таблице и нажмите комбинацию клавиш **CTRL+A**;
 - установите флажок в заголовке левой крайней графы таблицы.

При выборе нескольких уязвимостей в области деталей отображается общее количество выбранных уязвимостей. Если вы выбрали все уязвимости, удовлетворяющие текущим параметрам фильтрации и поиска, в области деталей отображается одно из следующих значений:

- Если выбрано до 2000 уязвимостей включительно, отображается точное количество. В этом случае программа проверяет состояние выбранных уязвимостей, как и при других способах выбора нескольких уязвимостей.
- Если выбрано более 2000 уязвимостей, отображается 2000+. В этом случае программа не проверяет состояние выбранных уязвимостей.

В заголовке левой крайней графы таблицы отображается флажок выбора уязвимостей. В зависимости от количества выбранных уязвимостей флажок может быть в одном из следующих состояний:

- – в таблице не выполнялся выбор всех уязвимостей, удовлетворяющих текущим параметрам фильтрации и поиска. При этом в таблице может быть выбрана одна уязвимость или несколько уязвимостей с помощью флажков напротив уязвимостей или с использованием клавиш **CTRL** или **SHIFT**.
- – в таблице выбраны все уязвимости, удовлетворяющие текущим параметрам фильтрации и поиска.
- – в таблице были выбраны все уязвимости, удовлетворяющие текущим параметрам фильтрации и поиска, и после этого для некоторых уязвимостей были сняты флажки. Это состояние сохраняется и в случае, если флажки сняты для всех уязвимостей, выбранных таким способом (из-за того, что количество выбранных уязвимостей может измениться).

Если выбраны все уязвимости, удовлетворяющие параметрам фильтрации и поиска, количество выбранных уязвимостей может автоматически изменяться. Например, в результате действий пользователя программы в другом сеансе подключения или при обнаружении новых уязвимостей. Рекомендуется настраивать параметры фильтрации и поиска таким образом, чтобы в выборку попали только нужные уязвимости.

Просмотр сведений об уязвимости

Подробные сведения об уязвимости включают информацию из таблицы уязвимостей (см. раздел “Просмотр таблицы уязвимостей” на стр. [335](#)), а также следующие поля:

- **Рекомендации** – рекомендации по устранению уязвимости (например, сведения о том, какую версию программного обеспечения рекомендуется установить на устройстве).
- **Ссылки** – ссылки на общедоступные ресурсы с дополнительными сведениями об уязвимости.
- **История CVE** – даты этапов выявления, подтверждения и публикации уязвимости в общедоступных источниках.
- **События** – список событий, связанных с уязвимостью (если событий больше 10, под списком отображается количество непоказанных событий).
- **Другие устройства с этой уязвимостью** – список устройств, в которых также обнаружена эта уязвимость (если устройств больше 10, под списком отображается количество непоказанных устройств).

► *Чтобы просмотреть сведения об уязвимости в разделе **Уязвимости**,*

выберите нужную уязвимость в таблице уязвимостей.

В правой части окна веб-интерфейса появится область деталей с подробными сведениями об уязвимости.

► *Чтобы просмотреть сведения об уязвимости на закладке **Устройства** в разделе **Активы**,*

нажмите на CVE-идентификатор уязвимости в графе **Уязвимости** или в области деталей устройства с уязвимостью.

Появится окно с подробными сведениями об уязвимости.

Автоматическое изменение состояний уязвимостей

Программа может автоматически переводить состояния обнаруженных уязвимостей из состояния *Актуальна* в состояние *Устранена* и обратно.

Уязвимость переводится в состояние *Устранена* в одном из следующих случаев:

- сведения об устройстве больше не соответствуют полям, которые описывают уязвимость с тем же CVE-идентификатором в базе данных известных уязвимостей (например, после изменения сведений о версии программного обеспечения на устройстве);
- удалено (см. раздел “Удаление устройств” на стр. [129](#)) устройство, в котором ранее была обнаружена уязвимость;
- удалено описание уязвимости из базы данных известных уязвимостей (после загрузки обновлений (см. раздел “Обновление баз и программных модулей” на стр. [110](#))).

Автоматическое возвращение уязвимости в состояние *Актуальна* происходит в случае, если уязвимость с тем же CVE-идентификатором снова обнаружена на том же устройстве.

Изменение состояний уязвимостей вручную

При работе в разделе **Уязвимости** вы можете вручную переводить уязвимости из состояния *Актуальна* в состояние *Принята* и обратно. При работе в разделе **Активы** вы можете переводить уязвимости только из состояния *Актуальна* в состояние *Принята*.

Также вы можете перевести уязвимость из состояния *Актуальна* в состояние *Принята* при присвоении статуса (см. раздел "Изменение статусов событий" на стр. [321](#)) *Обработано* событиям, которые связаны с этой уязвимостью (например, событие об обнаружении уязвимости). При этом статус *Обработано* будет также присвоен и всем остальным событиям, которые связаны с этой уязвимостью.

► *Чтобы изменить состояние уязвимости вручную, выполните следующие действия:*

1. Откройте область деталей или окно с подробными сведениями об уязвимости (см. раздел "Просмотр сведений об уязвимости" на стр. [341](#)).
2. В зависимости от того, в какое состояние вы хотите перевести уязвимость, нажмите на одну из следующих кнопок:
 - **Принята** – если вы хотите перевести уязвимость из состояния *Актуальна* в состояние *Принята*.
 - **Актуальна** – если вы хотите вернуть уязвимость из состояния *Принята* в состояние *Актуальна*.Откроется окно с запросом подтверждения.
3. Нажмите на кнопку **ОК**.

Просмотр сведений об устройствах с обнаруженной уязвимостью

Если уязвимость была обнаружена в нескольких устройствах, вы можете просмотреть сведения об этих устройствах в таблице устройств.

► *Чтобы просмотреть сведения об одном из устройств с обнаруженной уязвимостью, выполните следующие действия:*

1. Откройте область деталей или окно с подробными сведениями об уязвимости (см. раздел "Просмотр сведений об уязвимости" на стр. [341](#)).
2. В блоке **Другие устройства с этой уязвимостью** нажмите на строку с именем нужного устройства. Откроется раздел **Активы**. На закладке **Устройства** будет применена фильтрация по идентификатору устройства.

► *Чтобы просмотреть сведения обо всех устройствах с обнаруженной уязвимостью, выполните следующие действия:*

1. Откройте область деталей или окно с подробными сведениями об уязвимости (см. раздел "Просмотр сведений об уязвимости" на стр. [341](#)).
2. По ссылке **Перейти к таблице устройств** в блоке **Другие устройства с этой уязвимостью** перейдите к таблице устройств.

Откроется раздел **Активы**. На закладке **Устройства** будет применена фильтрация по CVE-идентификатору уязвимости.

Просмотр событий, связанных с уязвимостью

При мониторинге уязвимостей программа регистрирует события по технологии Контроль активов. Для регистрации используются системные типы событий (см. раздел "Системные типы событий по технологии Контроль активов" на стр. [419](#)), которым присвоены следующие коды:

- 4000005300 – обнаружена уязвимость устройства в первый раз или если уязвимость ранее была переведена в состояние *Устранена* (например, если измененные сведения об устройстве снова совпали с описанием устройства в уязвимости с тем же CVE-идентификатором);
- 4000005303 – обнаружены изменения в уязвимости, которые не повлияли на ее текущее состояние (например, если при обновлении базы данных известных уязвимостей были добавлены дополнительные рекомендации по защите системы).

Вы можете просмотреть события, связанные с уязвимостью, в таблице событий.

► *Чтобы просмотреть сведения об одном из событий, связанных с обнаруженной уязвимостью, выполните следующие действия:*

1. Откройте область деталей или окно с подробными сведениями об уязвимости (см. раздел "Просмотр сведений об уязвимости" на стр. [341](#)).
2. В блоке **События** нажмите на строку с заголовком нужного события.

Откроется раздел **События**. В таблице событий будет применена фильтрация по идентификатору выбранного события.

► *Чтобы просмотреть сведения обо всех событиях, связанных с обнаруженной уязвимостью, выполните следующие действия:*

1. Откройте область деталей или окно с подробными сведениями об уязвимости (см. раздел "Просмотр сведений об уязвимости" на стр. [341](#)).
2. По ссылке **Перейти к таблице событий** в блоке **События** перейдите к таблице событий.

Откроется раздел **События**. В таблице событий будет применена фильтрация по идентификаторам событий, связанных с уязвимостью.

Экспорт уязвимостей в файл


Вы можете экспортировать информацию об уязвимостях в файл формата CSV. Информация экспортируется из граф, отображаемых в таблице в текущий момент.

► *Чтобы экспортировать информацию об уязвимостях, выполните следующие действия:*

1. Выберите раздел **Уязвимости**.
2. В таблице уязвимостей выберите уязвимости (см. раздел "Выбор уязвимостей в таблице уязвимостей" на стр. [340](#)), информацию о которых вы хотите экспортировать в файл.

Для экспорта информации о всех уязвимостях, удовлетворяющих текущим параметрам фильтрации и поиска, вы можете выбрать все уязвимости в таблице или использовать ссылку **Экспорт** в панели инструментов раздела **Уязвимости**. По ссылке **Экспорт** сразу запускается процесс формирования файла формата CSV.

После выбора уязвимостей в правой части окна веб-интерфейса появится область деталей.

3. В зависимости от количества выбранных элементов, нажмите на кнопку **Экспортировать уязвимость** или **Экспортировать выбранные уязвимости**.
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**.

Браузер сохранит загруженный файл. В зависимости от используемого браузера на экране может появиться окно для изменения пути и имени сохраняемого файла.

Контроль технологического процесса

Kaspersky Industrial CyberSecurity for Networks позволяет контролировать технологический процесс, предоставляя информацию о параметрах технологического процесса и полученных системных командах, передаваемых в трафике промышленной сети. Программа отслеживает эти данные для устройств, представленных в таблице устройств (см. раздел "Таблица устройств" на стр. [262](#)) и имеющих заданные параметры контроля процесса (см. раздел "Параметры контроля процесса для устройств" на стр. [156](#)).

Вы можете просматривать контролируемые теги и имеющиеся правила контроля процесса на странице веб-интерфейса Сервера (см. раздел "О веб-интерфейсе Сервера в основном режиме работы программы" на стр. [64](#)) в разделе **Контроль процесса**. Параметры контроля процесса для устройств доступны при выборе устройств в разделах **Активы** и **Карта сети**.

В этом разделе

Мониторинг значений параметров технологического процесса	344
Параметры тегов.....	345
Просмотр таблицы тегов	346
Просмотр сведений об устройствах, связанных с тегами.....	350
Обнаружение паролей по умолчанию при подключении к устройствам	350

Мониторинг значений параметров технологического процесса

Kaspersky Industrial CyberSecurity for Networks может отображать значения параметров технологического процесса (тегов) в онлайн-режиме.

Для отображения значений требуется добавить нужные теги в программу. Добавление тегов выполняется при настройке контроля процесса (см. раздел "Настройка контроля процесса" на стр. [152](#)).

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 событиях сохраняются значения тегов, полученные на момент регистрации события). Для сохранения имен и

значений тегов необходимо наличие переменной \$tags в параметрах типов событий (см. раздел "Настройка типов событий" на стр. [225](#)).

► *Чтобы просматривать значения параметров технологического процесса,*

подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс и в разделе **Контроль процесса** выберите закладку **Теги**.

В окне браузера отобразится таблица с тегами и их текущими значениями. Оперативно изменяемые значения отображаются в следующих параметрах тегов:

- **Значение.**
- **Тип данных основного значения.**
- **Структурные значения.**
- **Чтение/запись.**
- **Получено.**
- **Метка времени.**
- **Статус метки времени.**
- **Статус данных.**
- **Инициатор.**
- **Причина передачи.**
- **Источник.**

Для мониторинга значений тегов вы можете использовать все функции, доступные при просмотре таблицы тегов (см. раздел "Просмотр таблицы тегов" на стр. [346](#)).

Параметры тегов

Параметры тегов, используемые при контроле процесса, отображаются в таблице тегов и в области деталей при выборе тега.

В зависимости от того, какие графы выбраны для отображения, в таблице тегов могут отображаться следующие параметры:

- **Группа устройств** – имя группы, в которую помещено связанное с тегом устройство (содержит имя самой группы и имена всех ее родительских групп в дереве групп устройств).
- **Устройство** – имя связанного с тегом устройства.
- **Протокол** – название протокола, по которому передается тег.
- **Имя тега** – заданное имя тега.
- **Значение** – оперативно изменяемое значение тега.
- **Единица измерения** – единица измерения параметра технологического процесса, который представлен тегом.
- **Тип данных** – тип данных тега.
- **Тип данных основного значения** – тип данных для значения, которое является основным в структуре полей тега.

- **Чтение/запись** – направление передачи, при котором получено значение тега (R – при чтении из устройства, W – при записи в устройство, RW – любое направление).
- **Получено** – дата и время последнего получения значения тега программой.
- **Метка времени** – дата и время последнего изменения / обновления значения тега (полученное из трафика).
- **Статус метки времени** – текущий статус для даты и времени последнего изменения / обновления значения тега.
- **Статус данных** – текущий статус для полученного значения тега.
- **Инициатор** – название источника, от которого получено значение тега или передана команда.
- **Причина передачи** – причина изменения или отправки значения тега (полученная из трафика).
- **Избранное** – признак включения тега в список избранных.
- **Описание** – дополнительные сведения о теге.
- **Адрес тега** – физический адрес тега в памяти устройства.
- **Идентификатор тега** – порядковый номер тега. Идентификатор тега задается автоматически.
- **Масштабируемый тег** – признак масштабирования тега в пределах минимумов и максимумов для входных и выходных значений.
- **Вход (минимально)** – минимальный предел для входного значения.
- **Вход (максимально)** – максимальный предел для входного значения.
- **Выход (минимально)** – минимальный предел для выходного значения.
- **Выход (максимально)** – максимальный предел для выходного значения.
- **Структурные значения** – список имен и значений всех полей тега. Элементы списка разделяются запятой с пробелом (например: `field1: <значение1>, field2: <значение2>`). Имена вложенных полей состояются из имен всех родительских полей, и имени самого поля, разделенных двоеточием (например: `parent1:parent2:field: <значение>`). Строковые значения должны быть заключены в кавычки.
- **Источник** – сведения об источнике создания тега.

В области деталей для выбранного тега дополнительно могут отображаться другие параметры, определяемые в зависимости от устройства и протокола (например: **Номер блока, Область памяти**).

Для контроля технологического процесса на устройствах, которые взаимодействуют по протоколам стандартов IEC 60870-5-104 и IEC 60870-5-101, поддерживаются типы кадров, представляющие блоки данных прикладного уровня (ASDU). Сведения о поддерживаемых типах кадров ASDU в этих протоколах см. в Приложении (см. раздел "Поддерживаемые типы кадров ASDU в протоколах стандартов IEC 60870-5-104 и IEC 60870-5-101" на стр. [382](#)).

Просмотр таблицы тегов

Таблица тегов отображается на закладке **Теги** в разделе **Контроль процесса** веб-интерфейса программы. В таблице представлены общие параметры тегов, а также устройств, к которым относятся теги.

При просмотре таблицы тегов вы можете использовать следующие функции:

- Настройка отображения и порядка граф в таблице тегов

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


1. На закладке **Теги** в разделе **Контроль процесса** откройте окно для настройки отображения таблицы по ссылке **Настроить таблицу**.
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 тегов.


- Фильтрация по графам таблицы

Вы можете отфильтровать таблицу тегов по значениям граф **Группа устройств**, **Устройство**, **Протокол**, **Имя тега**, **Единица измерения**, **Избранное** и **Идентификатор тега**.


► *Чтобы отфильтровать теги по графе **Устройство**, **Имя тега**, **Единица измерения** или **Идентификатор тега**, выполните следующие действия:*

1. На закладке **Теги** в разделе **Контроль процесса** нажмите на значок фильтрации в нужной графе таблицы.
Откроется окно фильтрации.
2. В полях **Включая** и **Исключая** введите значения для тегов, 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 теги по графе **Группа устройств**, выполните следующие действия:

1. На закладке **Теги** в разделе **Контроль процесса** нажмите на значок фильтрации в графе **Группа устройств**.
Откроется окно фильтрации.
2. Нажмите на значок в правой части поля для указания группы устройств.
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 (ИЛИ)** 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 теги по графе **Протокол**, выполните следующие действия:

1. На закладке **Теги** в разделе **Контроль процесса** нажмите на значок фильтрации в графе **Протокол**.
Откроется окно фильтрации.
2. В поле **Протоколы** укажите нужный протокол из числа поддерживаемых протоколов прикладного уровня. Для этого начните вводить название протокола и выберите нужный протокол в раскрывшемся списке (список подходящих протоколов автоматически раскрывается при изменении значения в поле **Протоколы**).
Вы можете отсортировать открывшийся список протоколов по ссылке **Сортировка**.
3. Если вы хотите добавить еще один протокол, нажмите на кнопку **Добавить протокол** и укажите другой протокол в открывшемся поле.
4. Если вы хотите удалить один из указанных протоколов, в окне фильтрации нажмите на значок . Вы также можете удалить все указанные протоколы по ссылке **Фильтр по умолчанию** в окне фильтрации.
5. Нажмите на кнопку **ОК**.

► Чтобы отфильтровать теги по графе **Избранное**, выполните следующие действия:

1. На закладке **Теги** в разделе **Контроль процесса** нажмите на значок фильтрации в графе **Избранное**.

Для фильтрации по графе **Избранное** вы также можете воспользоваться раскрывающимся списком **Избранные** в панели инструментов.

Откроется окно фильтрации.

2. Выберите один из следующих вариантов:
 - **Только избранные** – для отображения только тегов с признаком **Да** в графе **Избранное**.
 - **Без избранных** – для отображения только тегов с признаком **Нет** в графе **Избранное**.
3. Нажмите на кнопку **ОК**.

- Поиск тегов

► Чтобы найти нужные теги,

на закладке **Теги** в разделе **Контроль процесса** введите поисковый запрос в поле **Поиск тегов**. Поиск инициируется во время ввода символов.

В таблице тегов отобразятся теги, которые удовлетворяют условиям поиска.

Поиск выполняется по графам **Группа устройств**, **Устройство**, **Протокол**, **Имя тега**, **Единица измерения**, **Избранное**, **Описание**, **Адрес тега** и **Идентификатор тега**.

- Сброс заданных параметров фильтрации и поиска

► Чтобы сбросить заданные параметры фильтрации и поиска в таблице тегов,

в панели инструментов на закладке **Теги** в разделе **Контроль процесса** нажмите на кнопку **Фильтр по умолчанию** (кнопка отображается, если заданы параметры фильтрации или поиска).

- Сортировка тегов

Вы можете отсортировать таблицу тегов по значениям граф **Группа устройств**, **Устройство**, **Протокол**, **Имя тега**, **Единица измерения**, **Избранное** и **Источник**.

► *Чтобы отсортировать теги, выполните следующие действия:*

1. На закладке **Теги** в разделе **Контроль процесса** 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 сведений об устройствах, связанных с тегами

Вы можете просмотреть сведения об устройствах, с которыми связаны теги, в таблице устройств. В таблице устройств автоматически применяется фильтрация по идентификаторам устройств, которые указаны в тегах.

Возможность загружать сведения доступна, если выбрано не более 200 тегов.

► *Чтобы просмотреть сведения об устройствах в таблице устройств, выполните следующие действия:*

1. Выберите раздел **Контроль процесса**.
2. На закладке **Теги** выберите теги (см. раздел "Выбор тегов в таблице" на стр. [165](#)), для которых вы хотите просмотреть сведения об устройствах.

В правой части окна веб-интерфейса появится область деталей.

3. Нажмите на кнопку **Показать устройство** (если выбран один тег) или **Показать устройства** (если выбрано несколько тегов).

Кнопка **Показать устройства** недоступна, если количество выбранных тегов превышает 200.

Откроется раздел **Активы**. На закладке **Устройства** будет применена фильтрация по идентификаторам устройств, с которыми связаны выбранные теги.

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 регистрирует соответствующее событие. Для регистрации событий обнаружения паролей по умолчанию используется системный тип события обнаружения системных команд (см. раздел "Выбор отслеживаемых системных команд" на стр. [160](#)).

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).

Таблица 5. Поддерживаемые устройства и протоколы с паролями по умолчанию

Устройства	Протоколы	Системные команды
ABB серии Relion: RED670, REL670, RET670	ABB SPA-Bus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD SET
BECKHOFF серий CX	BECKHOFF ADS/AMS	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
Emerson серии ControlWave	Emerson ControlWave Designer	DEFAULT PASSWORD ENTRY
General Electric серии Multilin: B30, C60	Modbus TCP	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD READ WITH TYPE DEFAULT PASSWORD SET
Mitsubishi System Q E71	Mitsubishi MELSEC System Q	DEFAULT PASSWORD SET
Schneider Electric серии Modicon: M580, M340	Modbus TCP	DEFAULT PASSWORD READ WITH TYPE
Siemens SIMATIC серий S7-200, S7- 300, S7-400	Siemens Industrial Ethernet Siemens S7comm	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ

Устройства	Протоколы	Системные команды
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 взаимодействий включен в режиме наблюдения (см. раздел "Выбор применяемых технологий контроля взаимодействий" на стр. [189](#)) с применением технологии Контроль системных команд.
- В таблице разрешающих правил отсутствуют правила для технологии Контроль системных команд, которые разрешают системные команды с паролями по умолчанию. Например, программа может автоматически создать такие правила в режиме обучения контроля взаимодействий. Если такие правила присутствуют в таблице разрешающих правил, рекомендуется их выключить (см. раздел "Включение и выключение правил контроля взаимодействий" на стр. [201](#)).
- Для нужных устройств включено отслеживание системных команд с паролями по умолчанию (см. раздел "Выбор отслеживаемых системных команд" на стр. [160](#)).

Обнаружение проблем безопасности в протоколах шифрования

Если в промышленной сети используются протоколы шифрования (например, SSL/TLS или SSH), Kaspersky Industrial CyberSecurity for Networks может обнаруживать различные проблемы безопасности в сетевых взаимодействиях по этим протоколам. При обнаружении проблемы безопасности программа регистрирует соответствующее событие. Для регистрации таких событий используется системный тип события обнаружения системных команд (см. раздел "Выбор отслеживаемых системных команд" на стр. [160](#)).

Программа регистрирует события при обнаружении следующих проблем безопасности в протоколе шифрования:

- Использование устаревшей версии протокола шифрования (DEPRECATED PROTOCOL VERSION).
- Использование слабого алгоритма шифрования (WEAK CIPHER TYPE).

- Использование просроченного сертификата (OUTDATED CERTIFICATE).
- Использование самоподписанного сертификата (SELF-SIGNED CERTIFICATE).

Перечень обнаруживаемых проблем безопасности зависит от протокола шифрования.

После установки программы используются исходные модули обработки протоколов, обеспечивающие поддержку ограниченного количества протоколов шифрования. Вы можете обновлять модули обработки протоколов, устанавливая обновления (см. раздел "Обновление баз и программных модулей" на стр. [110](#)).

Для обнаружения проблем безопасности в протоколах шифрования не требуется добавлять параметры контроля процесса для устройств. Программа анализирует протоколы шифрования во всех обнаруженных взаимодействиях.

Для регистрации событий обнаружения проблем безопасности должны выполняться следующие условия:

- Контроль взаимодействий включен в режиме наблюдения (см. раздел "Выбор применяемых технологий контроля взаимодействий" на стр. [189](#)) с применением технологии Контроль системных команд.
- В таблице разрешающих правил отсутствуют правила для технологии Контроль системных команд, которые блокируют регистрацию событий о проблемах безопасности в протоколах шифрования. Например, программа может автоматически создать такие правила в режиме обучения контроля взаимодействий. Если такие правила присутствуют в таблице разрешающих правил, рекомендуется их выключить (см. раздел "Включение и выключение правил контроля взаимодействий" на стр. [201](#)).

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 (см. раздел "Изменение параметров и централизованная переустановка компонентов программы" на стр. [43](#)).
- В Kaspersky Security Center установлен плагин управления (см. раздел "Установка плагина управления Kaspersky Industrial CyberSecurity for Networks для Kaspersky Security Center" на стр. [50](#) 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.

В этом разделе

Подключение к компьютеру Сервера из Kaspersky Security Center	354
Добавление лицензионного ключа в Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center	355
Использование Сервера администрирования Kaspersky Security Center в качестве источника обновлений	356
Мониторинг событий через Kaspersky Security Center	356
Контроль состояния безопасности АСУ ТП: Kaspersky Security Center и SCADA	360

Подключение к компьютеру Сервера из Kaspersky Security Center

Вы можете удаленно подключаться к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks из Консоли администрирования Kaspersky Security Center. Подключение выполняется с помощью системы удаленного доступа к рабочему столу Virtual Network Computing (далее VNC).

Для подключения вам необходимо установить и настроить следующие компоненты VNC:

- VNC-сервер. Устанавливается на компьютере, который выполняет функции Сервера Kaspersky Industrial CyberSecurity for Networks. При настройке VNC-сервера нужно задать пароль для VNC-подключения. Дополнительно, если на этом компьютере включен межсетевой экран, нужно открыть порты для протоколов VNC и SSH.
- VNC-клиент. Устанавливается на компьютере с Консолью администрирования Kaspersky Security Center.

► Чтобы получить доступ к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center, 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\tnvviewer.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.

Добавление лицензионного ключа в Kaspersky Industrial CyberSecurity for Networks из Kaspersky Security Center

Вы можете добавить лицензионный ключ (см. раздел "О лицензионном ключе для активации функциональности обновления" на стр. [75](#)) в Kaspersky Industrial CyberSecurity for Networks с использованием функциональности автоматического распространения лицензионных ключей в Kaspersky Security Center. Лицензионный ключ, полученный таким способом, обрабатывается в Kaspersky Industrial CyberSecurity for Networks так же, как и при добавлении ключа вручную в программе (см. раздел "Добавление лицензионного ключа при подключении к Серверу через веб-интерфейс" на стр. [76](#)).

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 (см. раздел "О файле лицензионного ключа для активации функциональности обновления" на стр. [75](#)).

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 (см. раздел "Обновление баз и программных модулей" на стр. [110](#)) 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. Выберите Сервер администрирования Kaspersky Security Center в качестве источника обновлений при запуске обновления вручную (см. раздел "Запуск обновления вручную" на стр. [111](#)) и / или при настройке автоматического обновления (см. раздел "Настройка автоматического обновления" на стр. [111](#)).

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 (см. раздел "Типы событий в Kaspersky Security Center для событий Kaspersky Industrial CyberSecurity for Networks" на стр. [358](#)).
- **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 (см. раздел "Соответствие уровней важности событий в Kaspersky Security Center" на стр. [360](#)).
- **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 (см. раздел "Взаимодействие программы с Kaspersky Security Center" на стр. [354](#)).
2. Убедитесь, что на компьютере Сервера Kaspersky Industrial CyberSecurity for Networks доступен порт (см. раздел "Используемые порты для установки и работы компонентов" на стр. [34](#)) для подключения к компьютеру с Kaspersky Security Center.
3. 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.
4. В Kaspersky Industrial CyberSecurity for Networks настройте передачу событий (см. раздел "Настройка передачи событий через коннекторы" на стр. [231](#)) через коннектор **Kaspersky Security Center Connector**.

При регистрации в Kaspersky Industrial CyberSecurity for Networks указанных типов событий эти события также будут отображаться в таблице событий Kaspersky Security Center.

В этом разделе

Типы событий в Kaspersky Security Center для событий Kaspersky Industrial CyberSecurity for Networks.....	358
Соответствие уровней важности событий в Kaspersky Security Center	360

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).

Таблица 6. Типы событий в Kaspersky Security Center для получения событий Kaspersky Industrial CyberSecurity for Networks

Отображаемое имя типа события	Код типа события в Kaspersky Security Center	Регистрация в качестве инцидента Kaspersky Security Center	Соответствующий код типа события в Kaspersky Industrial CyberSecurity for Networks
Достигнуто максимальное количество переданных событий	32769	да, с уровнем важности <i>Предупреждение</i>	–
Тестовое событие (DPI)	32770	нет	4000000001
Тестовое событие (NIC)	32771	нет	4000000002
Тестовое событие (IDS)	32772	нет	4000000003
Тестовое событие (AM)	32773	нет	4000000004
Обнаружено неразрешенное сетевое взаимодействие	32774	нет	4000002601
Обнаружена системная команда	32775	только события с уровнем важности <i>Критические</i>	4000002602
Отсутствует трафик на точке мониторинга	32776	нет	4000002700
Обнаружена аномалия в протоколе TCP: подмена содержимого в перекрывающихся TCP-сегментах	32777	да	4000002701
Нарушено правило контроля процесса	32778	только события с уровнем важности <i>Критические</i>	4000002900
Сработало правило обнаружения вторжений из системного набора правил	32779	нет	4000003000
Сработало правило обнаружения вторжений из пользовательского набора правил	32780	нет	4000003001

Отображаемое имя типа события	Код типа события в Kaspersky Security Center	Регистрация в качестве инцидента Kaspersky Security Center	Соответствующий код типа события в Kaspersky Industrial CyberSecurity for Networks
Обнаружены признаки ARP-спуфинга в ARP-ответах	32781	да	4000004001
Обнаружены признаки ARP-спуфинга в ARP-запросах	32782	да	4000004002
Обнаружено новое устройство в сети	32783	да	4000005003
Обнаружены новые параметры устройства	32784	нет	4000005004
Обнаружен конфликт IP-адреса	32785	да	4000005005
Обнаружена активность устройства со статусом Неиспользуемое	32786	нет	4000005006
Обнаружен новый IP-адрес устройства	32787	да	4000005007
Обнаружен новый MAC-адрес устройства	32788	да	4000005010
Добавлен MAC-адрес устройству	32789	нет	4000005008
Добавлен IP-адрес устройству	32790	нет	4000005009
Контроль проектов ПЛК: обнаружено чтение неизвестного блока из ПЛК	32791	нет	4000005200
Контроль проектов ПЛК: обнаружено чтение известного блока из ПЛК	32792	нет	4000005201
Контроль проектов ПЛК: обнаружена запись нового блока в ПЛК	32793	нет	4000005202
Контроль проектов ПЛК: обнаружена запись известного блока в ПЛК	32794	нет	4000005203
Контроль проектов ПЛК: обнаружено чтение неизвестного проекта из ПЛК	32795	нет	4000005204
Контроль проектов ПЛК: обнаружено чтение известного проекта из ПЛК	32796	нет	4000005205
Контроль проектов ПЛК: обнаружена запись нового проекта в ПЛК	32797	нет	4000005206
Контроль проектов ПЛК: обнаружена запись известного проекта в ПЛК	32798	нет	4000005207
Обнаружена аномалия в протоколе IP: конфликт данных при сборке IP-пакета	32799	да	4000005100
Обнаружена аномалия в протоколе IP: превышение размера фрагментированного IP-пакета	32800	да	4000005101

Отображаемое имя типа события	Код типа события в Kaspersky Security Center	Регистрация в качестве инцидента Kaspersky Security Center	Соответствующий код типа события в Kaspersky Industrial CyberSecurity for Networks
Обнаружена аномалия в протоколе IP: размер начального фрагмента IP-пакета меньше ожидаемого	32801	да	4000005102
Обнаружена аномалия в протоколе IP: несоответствие фрагментов IP-пакета (mis-associated fragments)	32802	да	4000005103
Обнаружена уязвимость	32803	да	4000005300
Изменены сведения об уязвимости	32804	нет	4000005303
Зарегистрировано событие по правилу корреляции	32805	только события с уровнем важности <i>Критические</i>	8000000001
Событие от внешней системы	32807	да	4000005400

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).

Таблица 7. 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 (см. раздел "Взаимодействие программы с Kaspersky Security Center" на стр. [354](#)).

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 (см. раздел "Мониторинг событий через Kaspersky Security Center" на стр. [356](#)).

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.

В этом разделе

Не выполняется установка компонента программы на выбранном узле	362
Обнаружены проблемы в работе программы	363
Новое сообщение программы.....	363
Закончилось свободное пространство на жестком диске	364
При включении точки мониторинга возникает ошибка	364
Отсутствует трафик на точке мониторинга	365
Не загружается трафик для событий или инцидентов	366
Профилактические и пусконаладочные работы на АСУ ТП	366
Непредвиденная перезагрузка системы.....	367
После переустановки Сервера администрирования Kaspersky Security Center не выполняется синхронизация Агента администрирования	368
Не выполняется подключение к Серверу через веб-интерфейс	369
При подключении к Серверу браузер выводит предупреждение о сертификате.....	369

Не выполняется установка компонента программы на выбранном узле

Проблема

При централизованной установке компонентов программы выводится сообщение о недоступности узла для установки компонента из-за невозможности подключения по протоколу SSH. Установка компонента на этом узле не выполняется.

Решение

Централизованная установка компонента программы невозможна, если после настройки доступа по протоколу SSH на узле для установки компонента изменилась адресная информация или сетевое имя компьютера. Для централизованной установки компонента программы требуется восстановить доступ по протоколу SSH к удаленному компьютеру.

► *Чтобы восстановить доступ по протоколу SSH и установить компонент программы, выполните следующие действия:*


1. На компьютере, с которого выполняется централизованная установка компонентов программы, обновите ключ для подключения к узлу по протоколу SSH. Для этого войдите в систему с учетными данными пользователя, от имени которого выполняется установка программы, и в консоли операционной системы введите команду:

```
sudo ssh-keygen -R <IP-адрес узла>
```

2. Выполните переустановку программы с теми же параметрами установки (см. раздел "Изменение параметров и централизованная переустановка компонентов программы" на стр. [43](#)). При переустановке убедитесь в отсутствии сообщения о недоступности узла для установки компонента.

Обнаружены проблемы в работе программы

Проблема

При подключении к Серверу через веб-интерфейс в верхней части меню веб-интерфейса программы отображается значок красного цвета рядом с кнопкой .

Решение

Такое состояние Kaspersky Industrial CyberSecurity for Networks означает, что работа одного из процессов программы нарушена.

► *Чтобы восстановить работу программы, 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" (см. раздел "Обращение в Службу технической поддержки" на стр. [370](#)). 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 (на стр. [80](#)). Для доступа к журналам нужно иметь root-права в операционной системе.

Новое сообщение программы

Проблема

Появилось новое сообщение программы в разделе **Параметры** → **Сообщения программы**.

О сообщениях, на которые вам нужно обратить внимание, оповещает значок красного или желтого цвета рядом с кнопкой  в меню веб-интерфейса. Если значок отображается, это может означать, что появилось сообщение о нарушении работы программы или о некритическом сбое и эта проблема не устранена. Для просмотра сведений вы можете перейти в раздел **Параметры** → **Сообщения программы** с помощью кнопки , пока рядом с этой кнопкой отображается значок красного или желтого цвета.

Решение

Сообщение программы означает, что в работе программы произошло какое-либо событие.

Просмотрите краткую информацию в сообщении в разделе **Параметры** → **Сообщения программы**. По этой информации вы можете принять решение о необходимых действиях.

Дальнейшие действия зависят от статуса сообщения. Для сообщений предусмотрены следующие статусы:

- *Нормальная работа* – в большинстве случаев сообщение не требует реакции. Однако возможны ситуации, требующие дополнительного выяснения обстоятельств. Например, по сообщению об успешном применении политики безопасности, если вам неизвестны причины, по которым было выполнено это действие.
- *Состояние неизвестно, Сбой* – если сообщение появилось только что, подождите 20–30 секунд и проверьте текущее состояние программы.
- *Серьезный сбой, Критический сбой или Неустранимый сбой* – работа программы нарушена. Если проблему решить не удалось, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. [370](#)). 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 (на стр. [80](#)). 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 (см. раздел "Аппаратные и программные требования" на стр. [13](#)).
2. Перезапустите сервисы, обеспечивающие работу компонентов программы (см. раздел "Перезагрузка компьютера с установленными компонентами программы" на стр. [108](#)).

При включении точки мониторинга возникает ошибка

Проблема

После переключения точки мониторинга в режим *Включена* она находится в состоянии *Ошибка*. Вследствие этого узел, к которому относится точка мониторинга, переводится в состояние *Нарушена работа*. Также в списке уведомлений о проблемах в работе программы (см. раздел "Контроль состояния программы при подключении через веб-интерфейс" на стр. [95](#)) появляется сообщение о нарушении работы из-за обнаруженных проблем на точке мониторинга.

Решение

Состояние *Ошибка* на точке мониторинга может быть связано с неподдерживаемым операционным состоянием (operational state), в котором находится сетевой интерфейс. Для успешного завершения проверки при включении точки мониторинга сетевой интерфейс должен находиться в операционном состоянии *UP*. Другие состояния сетевого интерфейса (например, *UNKNOWN*) переводят точку мониторинга в состояние *Ошибка* из-за возможных проблем при получении или обработке сетевых пакетов.

Вы можете проверить текущее операционное состояние сетевого интерфейса на компьютере узла с помощью команды `ip link`. Сведения о текущем операционном состоянии выводятся в строке с именем интерфейса в виде: `state <состояние>`. На проблемном сетевом интерфейсе наиболее вероятны следующие операционные состояния:

- *DOWN*. В этом случае вы можете перевести интерфейс в операционное состояние *UP* с помощью команды:

```
sudo ip link set <имя интерфейса> up
```
- *UNKNOWN*. Такое операционное состояние может быть связано с неправильным добавлением интерфейса. Например, в состоянии *UNKNOWN* могут работать сетевые интерфейсы, добавляемые по умолчанию на виртуальной машине VMware™. В этом случае рекомендуется заново добавить (создать) сетевой интерфейс с правильными параметрами, используя соответствующие средства для работы с сетевыми интерфейсами.

После перевода сетевого интерфейса в операционное состояние *UP* проверьте состояние точки мониторинга, которая добавлена на этот сетевой интерфейс. Если точка мониторинга остается в состоянии *Ошибка*, выключите и снова включите эту точку мониторинга.

Отсутствует трафик на точке мониторинга

Проблема

Программа зарегистрировала событие, описание которого содержит следующий текст: [Отсутствует трафик на точке мониторинга](#). В описании события указана длительность отсутствия трафика, имя точки мониторинга и сетевой интерфейс, на который не поступает трафик.

Решение

Для того чтобы трафик поступал на точку мониторинга, должны выполняться следующие условия:

- точка мониторинга включена и ее 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** → **Развертывание**.

Если на сетевом интерфейсе точки мониторинга отображается скорость поступления входящего трафика 0 бит/с, проверьте выполнение следующих условий:

- сетевой интерфейс точки мониторинга правильно настроен в операционной системе;
- при подключении сетевого интерфейса к сетевому коммутатору промышленной сети – на сетевом коммутаторе правильно настроена передача зеркалированного трафика через порт подключения (SPAN).

Не загружается трафик для событий или инцидентов

Проблема

Невозможно загрузить трафик для выбранных событий и / или инцидентов. В таблице событий либо не отображаются инструменты для загрузки трафика (например, отсутствует кнопка **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 (см. раздел "Настройка типов событий" на стр. [225](#)) этого события. По умолчанию сохранение трафика выключено для всех типов событий. Вы можете включить и настроить (см. раздел "Настройка автоматического сохранения трафика для системных типов событий" на стр. [230](#)) сохранение трафика для нужных типов событий.

Программа удаляет сохраненный трафик для зарегистрированных событий при достижении одного из ограничений хранения трафика (например, если превышен максимальный объем сохраненного трафика в базе данных). Из базы данных удаляются пакеты трафика, которые были сохранены раньше других пакетов. Если сохраненный трафик удаляется слишком быстро и вы не успеваете его загрузить для нужных событий, вы можете увеличить максимальные значения параметров сохранения трафика (см. раздел "Управление параметрами сохранения трафика в базе данных Сервера" на стр. [212](#)).

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 (см. раздел "Настройка контроля процесса" на стр. [152](#)), контроля взаимодействий (см. раздел "Настройка контроля взаимодействий" на стр. [185](#)) и контроля активов (см. раздел "Настройка контроля активов" на стр. [120](#)).

См. также

Управление точками мониторинга на узлах[90](#)

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 (см. раздел "Обнаружены проблемы в работе программы" на стр. [363](#)).

Если неисправность сохраняется, перезапустите сервисы, обеспечивающие работу компонентов программы (см. раздел "Перезагрузка компьютера с установленными компонентами программы" на стр. [108](#)). Если после перезапуска проблема не устранена, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. [370](#)). 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 (на стр. [80](#)). 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 kbackup. Утилита kbackup 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 kbackup, 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/klagent64/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 ./klmagchk
```

На экране отобразится информация о подключении к Серверу администрирования.

После успешного восстановления синхронизации Агента администрирования в Консоли администрирования Kaspersky Security Center отобразится компьютер, на котором установлен Kaspersky Industrial CyberSecurity for Networks.

Не выполняется подключение к Серверу через веб-интерфейс

Проблема

При попытке подключения к Серверу не загружается страница веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Решение

Возможны следующие ситуации:

- Отсутствует доступ по сети к компьютеру Сервера Kaspersky Industrial CyberSecurity for Networks с установленным веб-сервером. Проверьте соединение с компьютером по указанному имени Сервера (например, с помощью команды `ping`).
- В адресной строке браузера введены неправильные данные. Введите IP-адрес или имя компьютера Сервера, которое было указано для веб-сервера в разделе **Параметры** → **Серверы подключений**. Номер порта можно не указывать, если задан порт по умолчанию 443. Если задан другой номер порта, введите в адресной строке полный адрес `https://<имя Сервера>:<порт>`
- В браузере выключено выполнение сценариев JavaScript. Сообщение об этом выводится на странице предупреждения о невозможности подключения. В параметрах браузера включите выполнение JavaScript и обновите страницу.
- Доступ к компьютеру Сервера заблокирован межсетевым экраном. Выполните настройку используемого межсетевого экрана.

При подключении к Серверу браузер выводит предупреждение о сертификате

Проблема

При попытке подключения к компьютеру с установленным компонентом Kaspersky Industrial CyberSecurity for Networks браузер выводит предупреждение о том, что сертификат безопасности или устанавливаемое соединение не является доверенным. Содержание предупреждения зависит от используемого браузера.

Решение

Предупреждение означает, что на веб-сервере используется самоподписанный сертификат. Для получения и использования доверенного сертификата вам нужно обратиться к администратору.

Вы можете временно использовать самоподписанный сертификат для подключения к Серверу (например, при тестовой эксплуатации Kaspersky Industrial CyberSecurity for Networks). Для использования самоподписанного сертификата в окне предупреждения браузера выберите вариант, позволяющий продолжить подключение. После подключения к Серверу в окне браузера будет отображаться предупреждающее сообщение о сертификате. Текст сообщения зависит от используемого браузера.

Для постоянного использования вы можете добавить для веб-сервера доверенный сертификат в разделе **Параметры** → **Серверы подключений**.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки	370
Техническая поддержка по телефону	370
Техническая поддержка через Kaspersky CompanyAccount	371
Получение информации для технической поддержки	371

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Industrial CyberSecurity for Networks, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Industrial CyberSecurity for Networks.

Kaspersky предоставляет поддержку Kaspersky Industrial CyberSecurity for Networks в течение жизненного цикла (см. страницу жизненного цикла программ (<https://support.kaspersky.com/corporate/lifecycle>)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (<https://support.kaspersky.ru/b2b>);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<https://support.kaspersky.ru/b2b>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

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 (на стр. [80](#)).

Для доступа к журналам нужно иметь root-права в операционной системе.

Также специалисты Службы технической поддержки "Лаборатории Касперского" могут запросить дополнительные данные о компонентах программы. Эти данные можно получить с помощью скрипта централизованной установки компонентов программы `kics4net-deploy-<номер версии программы>.bundle.sh` или с помощью скрипта для локального запуска `kics4net-gather-artefacts.sh`, который находится на компьютере с установленным компонентом программы в директории `/opt/kaspersky/kics4net/sbin/`.

► Чтобы получить данные о компонентах программы с помощью скрипта `kics4net-deploy-
<номер версии программы>.bundle.sh`, выполните следующие действия:

1. На компьютере, с которого выполнялась централизованная установка компонентов программы, перейдите в директорию с сохраненными файлами из комплекта поставки Kaspersky Industrial CyberSecurity for Networks.
2. Введите команду запуска скрипта централизованной установки 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 `BECOME password` введите пароль учетной записи пользователя, от имени которого выполнялась установка компонентов программы.

Дождитесь завершения работы скрипта `kics4net-deploy-
<номер версии программы>.bundle.sh`. При успешном завершении файлы будут созданы в указанной директории.

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.

BACnet – товарный знак компании American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

General Electric и Multilin – зарегистрированные товарные знаки компании General Electric.

Chromium и Google Chrome – товарные знаки Google, Inc.

Intel и Core – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft и Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CVE – зарегистрированный товарный знак MITRE Corporation.

MOXA – зарегистрированный товарный знак Moxa Inc.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Java и JavaScript – зарегистрированные товарные знаки компании Oracle и/или ее аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Schneider Electric – товарный знак компании Schneider Electric.

VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 8. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
администратор – пользователь, которому доступны привилегированные функции	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь
правила обнаружения вторжений – описывают аномалии трафика, которые могут быть признаками атак в промышленной сети	база решающих правил – составная часть СОВ, содержащая информацию о вторжениях (сигнатуры), на основе которой СОВ принимает решение о наличии вторжения (атаки)
вторжение – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам, критическое изменение параметров технологического процесса	вторжение – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам
программа	продукт, объект оценки, программное изделие, средство защиты информации
политика безопасности – набор параметров и правил, определяющих работу программы, в том числе для определения запрещенных действий в АСУ ТП	политика безопасности – совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых объектом оценки
сенсор – компонент программы, установленный на отдельном компьютере (не на компьютере Сервера программы) и выполняющий функции анализа трафика в соответствующем сегменте промышленной сети и последующей передачи данных о трафике и событиях на Сервер	сенсор – программный или программно-технический компонент СОВ, предназначенный для сбора и первичного анализа информации (данных) о событиях в контролируемой ИС, а также – передачи этой информации (данных) анализатору СОВ
события – записи, содержащие информацию об обнаружении в трафике промышленной сети данных, которые требуют внимания специалиста по безопасности АСУ ТП	события – данные аудита
оператор, пользователь	пользователь

Глоссарий

A

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).

C

CVE

Аббревиатура от Common Vulnerabilities and Exposures. База данных общеизвестных уязвимостей и рисков информационной безопасности. Уязвимостям присваиваются идентификационные номера в формате CVE-<год>-<номер>.

S

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.

A

АСУ ТП

Аббревиатура от "автоматизированная система управления технологическим процессом". Группа технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

B

Внешние системы

Технология регистрации инцидентов, а также событий, которые поступают в Kaspersky Industrial CyberSecurity for Networks от сторонних систем с использованием методов Kaspersky Industrial CyberSecurity for Networks API.

Выделенная сеть Kaspersky Industrial CyberSecurity

Вычислительная сеть, которая состоит из компьютеров, предназначенных для работы программ из состава решения Kaspersky Industrial CyberSecurity, и сетевого оборудования для обеспечения взаимодействия компьютеров. Выделенная сеть должна быть недоступна из других сетей.

И

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.

К

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.

Контроль активов

Технология регистрации событий, связанных с обнаружением в трафике активности устройств (например, событие при обнаружении активности ранее неизвестного устройства).

Контроль системных команд

Технология регистрации событий, связанных с обнаружением в трафике системных команд для устройств (например, обнаружение неразрешенной системной команды).

Контроль технологического процесса

Технология регистрации событий, связанных с нарушениями технологического процесса (например, обнаружено превышение заданного значения температуры).

Контроль целостности сети

Технология регистрации событий, связанных с целостностью промышленной сети или с безопасностью взаимодействий (например, обнаружено взаимодействие устройств по неразрешенному протоколу).

О

Обнаружение вторжений

Технология регистрации событий, связанных с обнаружением в трафике аномалий, которые являются признаками атак (например, обнаружены признаки ARP-спуфинга).

П

Политика безопасности

Набор данных, которые определяют параметры работы Kaspersky Industrial CyberSecurity for Networks.

Правило контроля взаимодействий

Описание разрешенного взаимодействия для устройств промышленной сети. При обнаружении сетевого взаимодействия, которое удовлетворяет включенному правилу контроля взаимодействий, Kaspersky Industrial CyberSecurity for Networks не регистрирует событие.

Правило контроля процесса

Набор условий для значений тегов. При выполнении условий правила контроля процесса Kaspersky Industrial CyberSecurity for Networks регистрирует событие.

Правило корреляции событий

Набор условий для проверки последовательностей событий в Kaspersky Industrial CyberSecurity for Networks. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции событий, Kaspersky Industrial CyberSecurity for Networks регистрирует инцидент.

Правило обнаружения вторжений

Набор условий, по которым система обнаружения вторжений анализирует трафик. Правило описывает аномалию трафика, которая может быть признаком атаки в промышленной сети.

Программируемый логический контроллер (ПЛК)

Промышленный контроллер, используемый для автоматизации технологических процессов на предприятии.

Проект ПЛК

Микропрограмма, написанная для ПЛК. Хранится в памяти ПЛК и выполняется в рамках технологического процесса, использующего ПЛК. Проект ПЛК может состоять из блоков, которые по отдельности передаются и принимаются по сети при чтении или записи проекта.

Промышленная сеть

Вычислительная сеть, соединяющая узлы автоматизированной системы управления технологическим процессом промышленного предприятия.

Р

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.

С

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).

Соединение на карте сети

Отображаемый объект на карте сети, который обозначает взаимодействие узлов в виде линии связи между узлами.

Т

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).

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).

у

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).

Уязвимость устройства

Недостаток в программном или аппаратном обеспечении устройства, используя который злоумышленник может повлиять на работу информационной системы или получить несанкционированный доступ к информации.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа примерами, а также справочными и дополнительными сведениями.

В этом разделе

Настройка синхронизации времени по протоколу NTP	381
Поддерживаемые типы кадров ASDU в протоколах стандартов IEC 60870-5-104 и IEC 60870-5-101	382
Отправка событий Kaspersky Industrial CyberSecurity for Networks в SIEM-системы.....	387
Изменение времени действия для сеансов подключения и токенов аутентификации с помощью скрипта	395
Файлы для импорта проекта универсального формата.....	396
Системные типы событий в Kaspersky Industrial CyberSecurity for Networks.....	414

Настройка синхронизации времени по протоколу NTP

Синхронизация времени узлов с установленными компонентами Kaspersky Industrial CyberSecurity for Networks должна выполняться с общим источником времени, который используют устройства промышленной сети. Для синхронизации вы можете использовать стандартный протокол Network Time Protocol (NTP).

В Kaspersky Industrial CyberSecurity for Networks текущей версии не применяется команда автоматического включения синхронизации времени Сервера с узлами, на которых установлены сенсоры. Для синхронизации времени требуется выполнить действия по настройке программных средств из состава операционной системы на всех узлах с установленными компонентами программы.

Настройка синхронизации времени по протоколу NTP в Astra Linux

► Чтобы настроить синхронизацию времени по протоколу NTP, выполните следующие действия:

1. Откройте системное окно настройки **Дата и время** с помощью пиктограммы часов в нижнем правом углу экрана.
2. Перейдите на закладку **Синхронизация**.
3. Укажите NTP-сервер, который будет использоваться для синхронизации времени.
4. Нажмите на кнопку **Применить**.
5. При запросе пароля введите пароль пользователя, который может исполнять команды с root-правами.

Поддерживаемые типы кадров ASDU в протоколах стандартов IEC 60870-5-104 и IEC 60870-5-101

В этом разделе приведено описание типов кадров ASDU, поддерживаемых в Kaspersky Industrial CyberSecurity for Networks (см. таблицу ниже). Перечисленные типы кадров обрабатываются при контроле технологического процесса на устройствах, которые взаимодействуют по протоколам стандартов IEC 60870-5-104 и IEC 60870-5-101.

Таблица 9. Типы кадров в протоколах стандартов IEC 60870-5-104 и IEC 60870-5-101

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
1. Информация о процессе в направлении контроля			
<1>	M_SP_NA	Одноэлементная информация	0 – ВЫКЛ, 1 – ВКЛ
<2>	M_SP_TA	Одноэлементная информация (с меткой времени)	0 – ВЫКЛ, 1 – ВКЛ
<3>	M_DP_NA	Двухэлементная информация	0 – Неопределенное или промежуточное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное
<4>	M_DP_TA	Двухэлементная информация (с меткой времени)	0 – Неопределенное или промежуточное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное
<5>	M_ST_NA	Информация о положении отпаяк	-64 ... +64
<6>	M_ST_TA	Информация о положении отпаяк (с меткой времени)	-64 ... +64
<7>	M_BO_NA	Строка из 32 бит	unsigned int32
<8>	M_BO_TA	Строка из 32 бит (с меткой времени)	unsigned int32
<9>	M_ME_NA	Значение измеряемой величины, нормализованное значение	float
<10>	M_ME_TA	Значение измеряемой величины, нормализованное значение (с меткой времени)	float
<11>	M_ME_NB	Значение измеряемой величины, масштабированное значение	float
<12>	M_ME_TB	Значение измеряемой величины, масштабированное значение (с меткой времени)	float
<13>	M_ME_NC	Значение измеряемой величины, короткий формат с плавающей запятой	float
<14>	M_ME_TC	Значение измеряемой величины, короткий формат с плавающей запятой (с меткой времени)	float

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
<15>	M_IT_NA	Интегральная сумма	int32
<16>	M_IT_TA	Интегральная сумма (с меткой времени)	int32
<17>	M_EP_TA	Информация о работе релейной защиты (с меткой времени)	0 – Неопределенное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное
<18>	M_EP_TB	Упакованная информация о срабатывании пусковых органов защиты (с меткой времени)	Набор битов в соответствии со стандартом
<19>	M_EP_TC	Упакованная информация о срабатывании выходных цепей защиты (с меткой времени)	Набор битов в соответствии со стандартом
<20>	M_PS_NA	Упакованная одноэлементная информация с определением изменения состояния	unsigned int16
<21>	M_ME_ND	Значение измеряемой величины, нормализованное значение без описателя качества	float
<30>	M_SP_TB	Одноэлементная информация (с меткой времени CP56Время2а)	0 – ВЫКЛ, 1 – ВКЛ
<31>	M_DP_TB	Двухэлементная информация (с меткой времени CP56Время2а)	0 – Неопределенное или промежуточное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное
<32>	M_ST_TB	Информация о положении отпаяк (с меткой времени CP56Время2а)	-64 ... +64
<33>	M_BO_TB	Строка из 32 бит (с меткой времени CP56Время2а)	unsigned int32
<34>	M_ME_TD	Значение измеряемой величины, нормализованное значение (с меткой времени CP56Время2а)	float
<35>	M_ME_TE	Значение измеряемой величины, масштабированное значение (с меткой времени CP56Время2а)	float
<36>	M_ME_TF	Значение измеряемой величины, короткий формат с плавающей запятой (с меткой времени CP56Время2а)	float
<37>	M_IT_TB	Интегральные суммы (с меткой времени CP56Время2а)	int32
<38>	M_EP_TD	Информация о работе релейной защиты (с меткой времени CP56Время2а)	0 – Неопределенное, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Неопределенное

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
<39>	M_EP_TE	Упакованная информация о срабатывании пусковых органов защиты (с меткой времени CP56Время2а)	Набор битов в соответствии со стандартом
<40>	M_EP_TF	Упакованная информация о срабатывании выходных цепей защиты (с меткой времени CP56Время2а)	Набор битов в соответствии со стандартом
2. Информация о процессе в направлении управления			
<45>	C_SC_NA	Одноэлементная команда	0 – ВЫКЛ, 1 – ВКЛ
<46>	C_DC_NA	Двухэлементная команда	0 – Не разрешено, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Не разрешено
<47>	C_RC_NA	Команда пошагового регулирования	0 – Не разрешено, 1 – Следующий шаг ВВЕРХ, 2 – Следующий шаг ВНИЗ, 3 – Не разрешено
<48>	C_SE_NA	Команда уставки, нормализованное значение	float
<49>	C_SE_NB	Команда уставки, масштабированное значение	float
<50>	C_SE_NC	Команда уставки, короткое число с плавающей запятой	float
<51>	C_BO_NA	Строка из 32 битов	int32
<58>	C_SC_TA	Одноэлементная команда (с меткой времени CP56Время2а)	0 – ВЫКЛ, 1 – ВКЛ
<59>	C_DC_TA	Двухэлементная команда (с меткой времени CP56Время2а)	0 – Не разрешено, 1 – ВЫКЛ, 2 – ВКЛ, 3 – Не разрешено
<60>	C_RC_TA	Команда пошагового регулирования (с меткой времени CP56Время2а)	0 – Не разрешено, 1 – Следующий шаг ВВЕРХ, 2 – Следующий шаг ВНИЗ, 3 – Не разрешено
<61>	C_SE_TA	Команда уставки, нормализованное значение (с меткой времени CP56Время2а)	float
<62>	C_SE_TB	Команда уставки, масштабированное значение (с меткой времени CP56Время2а)	float
<63>	C_SE_TC	Команда уставки, короткое число с плавающей запятой (с меткой времени CP56Время2а)	float
<64>	C_BO_TA	Строка из 32 битов (с меткой времени CP56Время2а)	int32

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
3. Информация о системе в направлении контроля			
<70>	M_EI_NA	Конец инициализации	Системная команда END OF INITIALIZATION
4. Информация о системе в направлении управления			
<100>	C_IC_NA	Команда опроса	Системная команда INTERROGATION
<101>	C_CI_NA	Команда опроса счетчика	Системная команда COUNTER INTERROGATION
<102>	C_RD_NA	Команда чтения	Системная команда READ
<103>	C_CS_NA	Команда синхронизации времени	Системная команда CLOCK SYNCHRONIZATION
<104>	C_TS_NA	Команда тестирования	Системная команда TEST
<105>	C_RP_NA	Команда установки процесса в исходное состояние	Системные команды RESET PROCESS ACTIVATION / RESET PROCESS CONFIRMATION
<106>	C_CD_NA	Команда задержки сбора данных	Системная команда DELAY ACQUISITION
<107>	C_TS_TA	Команда тестирования (с меткой времени CP56Время2а)	Системная команда TEST WITH TIME TAG
5. Параметры в направлении управления			
<110>	P_ME_NA	Параметр измеряемой величины, нормализованное значение	float
<111>	P_ME_NB	Параметр измеряемой величины, масштабированное значение	float
<112>	P_ME_NC	Параметр измеряемой величины, короткий формат с плавающей запятой	float
<113>	P_AC_NA	Активация параметра	Системная команда PARAMETER ACTIVATION
6. Пересылка файлов			
<120>	F_FR_NA	Файл готов	Не обрабатывается
<121>	F_SR_NA	Секция готова	Не обрабатывается
<122>	F_SC_NA	Вызов директории, выбор файла, вызов файла, вызов секции	Системная команда CALL DIRECTORY, SELECT FILE, CALL FILE, CALL SELECTION

ID типа кадра	Операция	Описание	Тип основного значения / системные команды
<123>	F_LS_NA	Последняя секция, последний сегмент	Не обрабатывается
<124>	F_AF_NA	Подтверждение файла, подтверждение секции	Не обрабатывается
<125>	F_SG_NA	Сегмент	Не обрабатывается
<126>	F_DR_TA	Директория	Не обрабатывается

Отправка событий Kaspersky Industrial CyberSecurity for Networks в SIEM-системы

В Kaspersky Industrial CyberSecurity for Networks вы можете использовать коннектор (см. раздел "Управление коннекторами" на стр. 216) для отправки данных на сервер SIEM-системы. После добавления коннектора (см. раздел "Добавление коннектора" на стр. 218) вам нужно настроить передачу событий (см. раздел "Настройка передачи событий через коннекторы" на стр. 231) через этот коннектор.

Содержание и порядок отображения сведений о событиях, передаваемых в SIEM-систему, могут отличаться от отображаемых данных в разделе **События** веб-интерфейса Сервера Kaspersky Industrial CyberSecurity for Networks.

- Проверка передачи событий на примере системы HP ArcSight

► Чтобы проверить передачу событий, выполните следующие действия:

1. Убедитесь, что настроен канал приема сообщений от Kaspersky Industrial CyberSecurity for Networks штатными средствами системы HP ArcSight.
2. Откройте браузер и перейдите по адресу вашей системы HP ArcSight.
3. Войдите под своей учетной записью и перейдите к разделу **Analyze** → **Live Event Viewer** (см. рис. ниже).
4. Нажмите на кнопку **Start** (см. рис. ниже).
5. Откройте интерфейс командной строки и введите команду, чтобы соединиться с сервером по протоколу Telnet:

```
telnet <адрес сервера ArcSight> <порт>
```

6. Отправьте тестовое сообщение в формате CEF:

```
CEF:0|KasperskyLab|TMS|1.0|KLAUD_EV_TESTEVENT|Critical Test event|1|src=10.0.0.1 dst=10.0.0.2 code=1234
```

Если есть соединение с системой HP ArcSight, в разделе **Live Event Viewer** появится событие, содержимое которого совпадает с отправленным сообщением (см. рис. ниже).

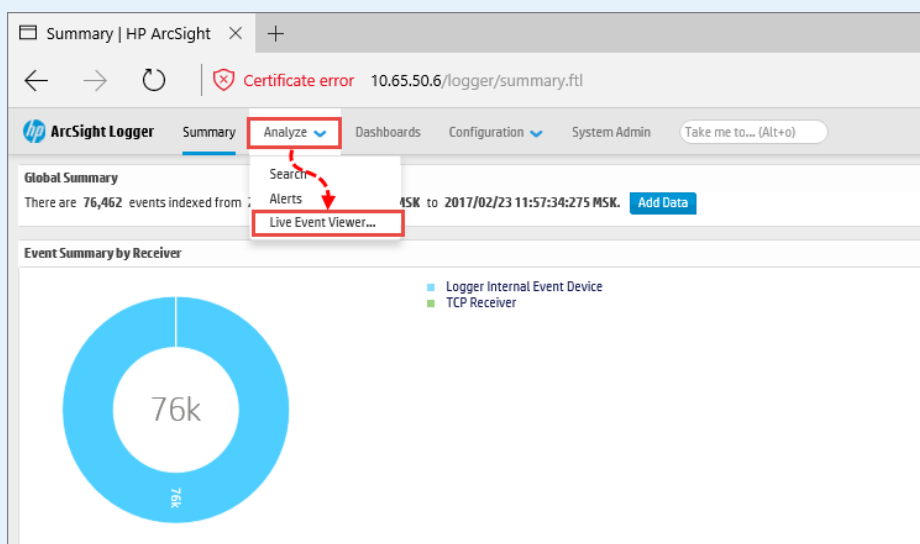


Рисунок 18. Открытие раздела **Live Event Viewer** в системе ArcSight

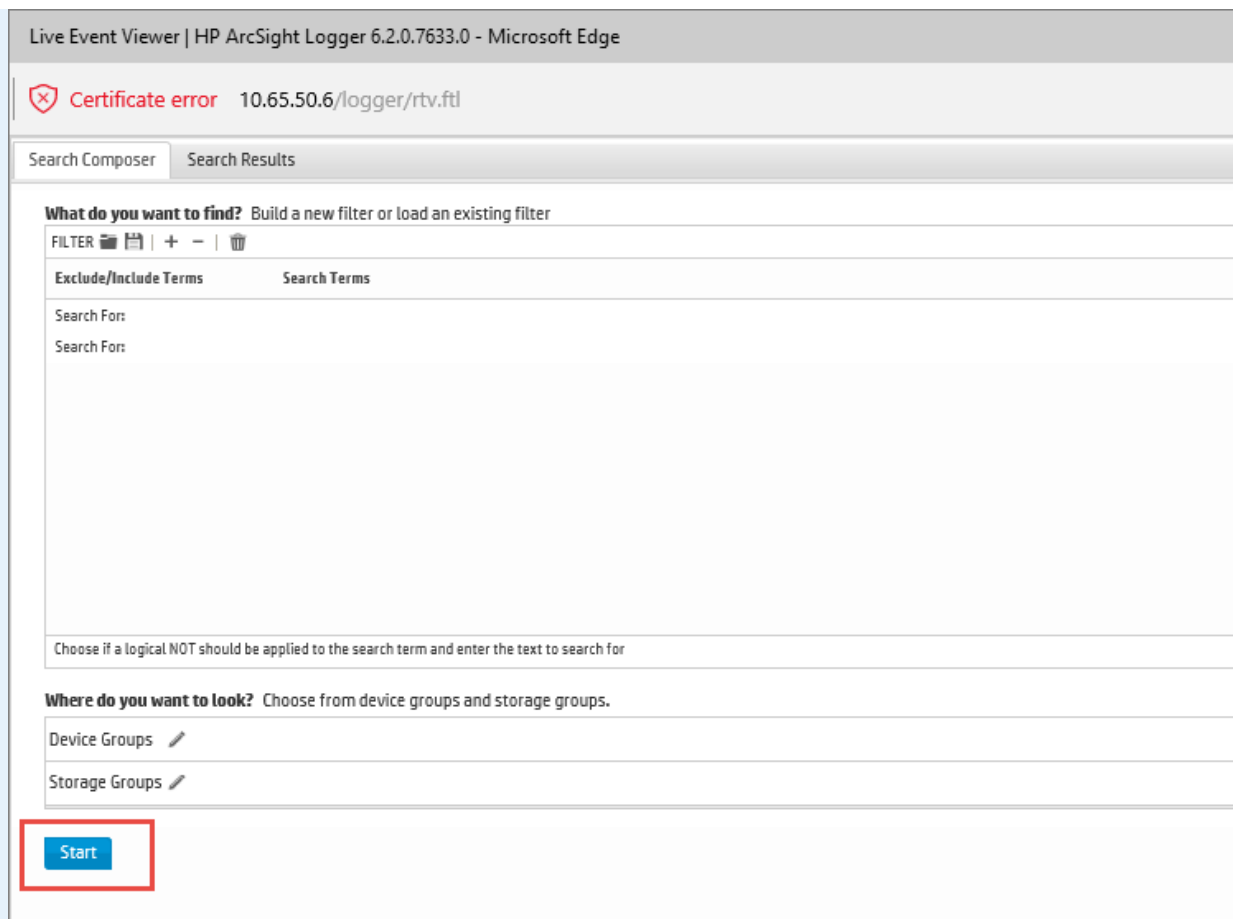


Рисунок 19. Запуск Live Event Viewer в системе ArcSight

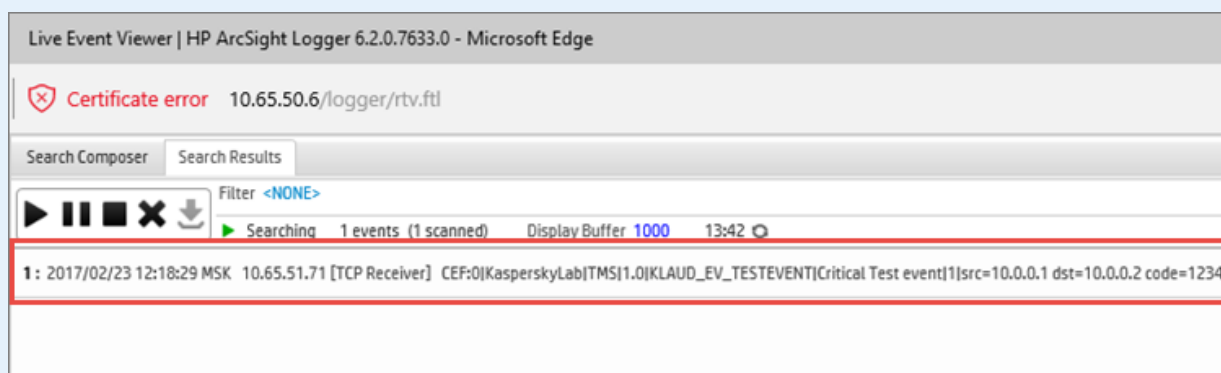


Рисунок 20. Проверка результатов работы

- Формат сообщений, посылаемых в SIEM-систему

Программа передает данные в SIEM-систему в формате CEF 20. При передаче данных используется внутренняя структура `EventMessage`.

Получаемые сообщения не преобразуются в формат протокола системного журнала.

Формат структуры `EventMessage`

В таблице ниже данные представлены в следующих графах:

- `EventMessage` — имя поля в сообщении.
- `Event` — соответствующее поле события в Kaspersky Industrial CyberSecurity for Networks или конкретное значение.
- Описание — описание поля.

<code>EventMessage</code>	<code>Event</code>	Описание
<code>dateTime</code>	Начало	Дата и время (с точностью до миллисекунды) перехвата сетевого пакета, который привел к возникновению события.
<code>hostname</code>	Адрес Сервера Kaspersky Industrial CyberSecurity for Networks	Адрес Сервера Kaspersky Industrial CyberSecurity for Networks.
<code>cefVersion</code>	0	Номер версии CEF.
<code>deviceVendor</code>	Kaspersky Lab	Производитель.
<code>deviceProduct</code>	Kaspersky Industrial CyberSecurity for Networks	Название продукта.
<code>deviceVersion</code>	Пример: 3.0.0.472.	Версия Kaspersky Industrial CyberSecurity for Networks.
<code>signatureId</code>	Тип события	Идентификатор типа события.

name	Заголовок	Описание события.
severity	Уровень важности события: <ul style="list-style-type: none"> • 10 – Критические; • 5 – Важные; • 0 – Информационные. 	Уровень важности события. Значения от 0 до 10, где 10 – наиболее важное событие.
extension	Указано в таблице Extension Fields	Определяется отдельно для каждого типа сообщения.

Дата и время отправляются в формате: `ГГГГ-ММ-ДДТч:мм:сс.мсZ`. Пример: `2021-04-01T22:14:15.030Z` — время события, которое возникло 01 апреля 2021 года в 22 часа, 14 минут, 15 секунд, 030 миллисекунд.

Содержимое Extension Fields

В таблице ниже данные представлены в следующих графах:

- Extension — имя поля в сообщении.
- Связанные события — события, в которых отправляется конкретное поле.
- Описание — описание поля.

Extension	Связанные события	Описание
cnt	Общие поля событий	Счетчик количества повторов после регистрации события.
dmac	Общие поля событий	MAC-адрес получателя.
dpt	Общие поля событий	Порт получателя.
dst	Общие поля событий	IP-адрес получателя.
end	Общие поля событий	Время завершения события.
smac	Общие поля событий	MAC-адрес отправителя.

spt	Общие поля событий	Порт отправителя.
src	Общие поля событий	IP-адрес отправителя.
start	Общие поля событий	Время регистрации события.
technology	Общие поля событий	Технология, которая использовалась для регистрации события.
triggeredRule	Общие поля событий	Сработавшее правило.
protocol	Общие поля событий	Протокол.
vlanId	Общие поля событий	VLAN ID.
monitoringPoint	Общие поля событий	Точка мониторинга, трафик с которой вызвал регистрацию события.
sourceIndustrialAddress	Общие поля событий	Адрес прикладного уровня для отправителя.
destinationIndustrialAddress	Общие поля событий	Адрес прикладного уровня для получателя.
eventIdIdentifier	Общие поля событий	Идентификатор события.
noTrafficDuration	Отсутствует трафик на точке мониторинга	Длительность отсутствия трафика.
tagId	Неверный тип тега	ID тега.

expectedTagType	Неверный тип тега	Ожидаемый тип данных тега.
actualTagType	Неверный тип тега	Фактический тип данных тега.
ruleName	<ul style="list-style-type: none"> Нарушение правила контроля процесса Сработало правило обнаружения вторжений из системного набора правил 	Имя правила.
tags	Нарушение правила контроля процесса	Теги.
msg	Сработало правило обнаружения вторжений из системного набора правил	Сообщение.
substitutedIpAddress	<ul style="list-style-type: none"> Обнаружены признаки ARP-подмены в ARP-ответах Обнаружены признаки ARP-подмены в ARP-запросах 	IP-адрес отправителя сетевых пакетов.
targetIpAddress	<ul style="list-style-type: none"> Обнаружены признаки ARP-подмены в ARP-ответах Обнаружены признаки ARP-подмены в ARP-запросах 	IP-адрес получателя сетевых пакетов.
attackStartTime	<ul style="list-style-type: none"> Обнаружены признаки ARP-подмены в ARP-ответах Обнаружены признаки ARP-подмены в ARP-запросах 	Время начала действий, имеющих признаки атаки.
ownerMac	<ul style="list-style-type: none"> Обнаружен конфликт IP-адреса Обнаружен новый IP-адрес Обнаружено новое устройство Получена новая информация Обнаружен трафик с MAC-адреса Добавлен MAC-адрес к устройству Добавлен IP-адрес к устройству 	MAC-адрес владельца.
ownerIp	<ul style="list-style-type: none"> Обнаружено новое устройство Добавлен MAC-адрес к устройству Добавлен IP-адрес к устройству Обнаружен конфликт IP-адреса Обнаружен новый MAC-адрес 	IP-адрес владельца.
challengerMac	Обнаружен конфликт IP-адреса	MAC-адрес претендента.

newIpAddress	Обнаружен новый IP-адрес	Новый IP-адрес.
newMacAddress	Обнаружен новый MAC-адрес	Новый MAC-адрес.
oldIpAddress	Обнаружен старый IP-адрес	Старый IP-адрес.
assetName	Обнаружено новое устройство	Имя устройства.

Параметры устройств

В таблице ниже представлены данные о параметрах устройств.

Если для обнаруженного взаимодействия определены одно или два устройства, Kaspersky Industrial CyberSecurity for Networks дополнительно отправляет в SIEM-систему известную информацию об одном или двух устройствах.

Если для обнаруженного взаимодействия определены несколько устройств, сообщение дублируется с другой адресной информацией и другими параметрами устройств (если устройства различны).

Extension	Параметр устройства
srcAssetName	Имя устройства-отправителя.
srcVendor	Производитель устройства-отправителя.
srcOS	Операционная система устройства-отправителя.
srcNetworkName	Сетевое имя устройства-отправителя.
srcModel	Модель устройства-отправителя.

dstAssetName	Имя устройства-получателя.
dstVendor	Производитель устройства-получателя.
dstOS	Операционная система устройства-получателя.
dstNetworkName	Сетевое имя устройства-получателя.
dstModel	Модель устройства-получателя.

Изменение времени действия для сеансов подключения и токенов аутентификации с помощью скрипта

В Kaspersky Industrial CyberSecurity for Networks вы можете изменять заданное время действия для сеансов подключения к Серверу через веб-интерфейс (см. раздел "Подключение к Серверу через веб-интерфейс" на стр. [54](#)) и для токенов аутентификации в Kaspersky Industrial CyberSecurity for Networks API (см. раздел "Использование Kaspersky Industrial CyberSecurity for Networks API" на стр. [240](#)). Для изменения параметра, определяющего ограничение по времени, используется скрипт `kics4net-params.py`, который находится на компьютере с установленным Сервером в директории `/opt/kaspersky/kics4net/sbin/`.

С помощью скрипта `kics4net-params.py` вы можете просмотреть текущее значение для времени действия и задать другое значение. Значение представлено в минутах. Вы можете задать ограничение по времени в диапазоне от 1 до 43200 минут (по умолчанию 600 минут, что соответствует 10 часам).

► *Чтобы просмотреть текущее значение для ограничения по времени, выполните следующие действия:*

1. На компьютере Сервера выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить скрипт `kics4net-params.py`.
2. Перейдите в директорию `/opt/kaspersky/kics4net/sbin/` и введите команду запуска скрипта в режиме просмотра текущего заданного значения:

```
python kics4net-params.py get -t -n
```

где:

- `-t` – параметр, обозначающий запрос текущего заданного значения для времени действия (обязательный параметр).
- `-n` – включает вывод внутреннего имени, под которым значение представлено в конфигурации программы. Если параметр не задан, значение выводится вместе с именем:
`login_session_timeout=<значение>`.

► *Чтобы изменить значение для ограничения по времени, выполните следующие действия:*

1. На компьютере Сервера выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить скрипт `kics4net-params.py`.
2. Перейдите в директорию `/opt/kaspersky/kics4net/sbin/` и введите команду запуска скрипта в режиме изменения значения:

```
python kics4net-params.py set -t=<значение> -r
```

где:

- `-t=<значение>` – новое значение для времени действия (обязательный параметр).
- `-r` – включает автоматический перезапуск сервисов программы на компьютере Сервера после применения нового значения для времени действия. Если параметр не задан, после завершения работы скрипта требуется вручную перезагрузить компьютер Сервера или перезапустить сервисы (см. раздел "Перезагрузка компьютера с установленными компонентами программы" на стр. [108](#)).

Файлы для импорта проекта универсального формата

Вы можете использовать проект универсального формата для импорта в Kaspersky Industrial CyberSecurity for Networks (см. раздел "Импорт конфигураций устройств и тегов из внешних проектов" на стр. [162](#)) конфигураций параметров контроля процесса для устройств и тегов. Импорт из проекта универсального формата выполняется с помощью текстовых файлов с разделителями (csv-файлов). Формат CSV – это текстовый формат для представления табличных данных.

Вы можете создавать файлы данных любым удобным для вас способом (например, из систем SCADA). Для импорта в программу созданные файлы нужно упаковать в ZIP-архив.

Набор файлов для импорта проекта универсального формата может состоять из следующих CSV-файлов:

- `devices.csv`. Содержит описания устройств 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.

При использовании файлов данных учитывайте следующие особенности:

- Файлы данных должны быть в кодировке UTF-8.
- Список тегов в файле `variables.csv` имеет группирующий признак "соединение".
- Для одного соединения в файле `connections.csv` можно указать несколько разных протоколов и адресов.
- Протокол может иметь один или несколько адресов.
- Одно устройство может иметь несколько соединений с разными наборами тегов.

Строки, содержащие значения параметров, в файлах `enums.csv` и `datasets.csv` заполняются только при описании перечислений и наборов данных для протоколов MMS и GOOSE стандарта IEC 61850. Для других протоколов файлы `enums.csv` и `datasets.csv` могут содержать только заголовочные строки. При этом файлы `enums.csv` и `datasets.csv` должны присутствовать в наборе файлов для импорта.

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.

В этом разделе

Файл описания устройств: <code>devices.csv</code>	397
Файл описания соединений и протоколов: <code>connections.csv</code>	400
Файл описания переменных и тегов: <code>variables.csv</code>	405
Файл описания перечислений: <code>enums.csv</code>	410
Файл описания наборов данных (группы тегов): <code>datasets.csv</code>	411
Файл описания отчетов протокола MMS: <code>iec61850_mms_reports.csv</code>	412

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 (см. раздел "Файлы для импорта проекта универсального формата" на стр. [396](#)).

- `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 CONTROLLEDGE 900 series;
 - 48 – HONEYWELL EXPERION C300;
 - 49 – SCHNEIDER ELECTRIC MICOM C264;
 - 50 – UMAS device;
 - 51 – TASE.2 server;
 - 52 – PROFINET device;
 - 53 – DIRECTLOGIC;
 - 54 – Server with encryption support;
 - 55 – BACNET device;
 - 56 – SCHNEIDER ELECTRIC P545.
- `Connection` – идентификатор соединения из файла описания соединений и протоколов `connections.csv` (см. раздел "Файл описания соединений и протоколов: `connections.csv`" на стр. [400](#)).

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 (см. раздел “Файл описания устройств: devices.csv” на стр. [397](#)).

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;
 - 28 – WMI INTERACTION;
 - 29 – HONEYWELL EXPERION INTERACTION;
 - 30 – MiCOM C264 INTERACTION;
 - 31 – SCHNEIDER ELECTRIC UMAS;
 - 32 – TASE.2;
 - 33 – PROFINET IO;
 - 34 – DIRECTLOGIC INTERACTION;
 - 35 – BACNET.
- **Address** – строка, содержащая полный сетевой адрес устройства, специфичный для указанного протокола.

Пример:

Соединение с контроллером Schneider Momentum (один IP-адрес):

```
"Barline1";0;"IP-Address=192.168.0.7;Port=502"
```

Соединение с контроллером Mitsubishi System Q (один IP-адрес, два порта):

```
"Station1";3;"IP-Address=192.168.0.8;Port=5001  
Network=0;Station=0;PC=255"
```

```
"Station1";3;"IP-Address=192.168.0.8;Port=5002  
Network=0;Station=0;PC=255"
```

Соединение с резервируемым контроллером Siemens S7-400, два контроллера (два IP-адреса, один набор тегов):

```
"S7$Program";1;"IP-Address=192.168.0.21;Port=102;Rack=0;Slot=2"
```

```
"S7$Program";1;"IP-Address=192.168.0.22;Port=102;Rack=0;Slot=2"
```

Соединение с контроллером Siemens S7-400, используется два протокола: S7Comm поверх стека TCP / IP и S7Comm поверх сети Industrial Ethernet (один набор тегов):

```
"S7$Program";1;"IP-Address=192.168.0.21;Port=102;Rack=0;Slot=2"
```

```
"S7$Program";2;"MAC=00:01:02:03:04:05;Rack=0;Slot=2"
```

После заголовочных строк следует тело файла, содержащее значения параметров (идентификатор соединения, код протокола прикладного уровня, полный сетевой адрес устройства). Пример файла connections.csv приведен ниже.

Пример:

```
'Connections  
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0  
'Field separator: ; Decimal separator: . Text quotes: " Var name  
separator: .  
'Connection;Protocol;Address  
"ms_plc";3;"IP-Address=192.168.0.77;Port=1025"  
"mc_SysQ";7;"IP-Address=192.168.0.77;Port=2404;Asdu=555"
```

Формат сетевого адреса устройства в файле connections.csv зависит от типа используемого протокола.

Пример:

Для поддерживаемых в Kaspersky Industrial CyberSecurity for Networks протоколов могут использоваться следующие форматы адреса:

- MODBUS TCP:

```
"IP-Address=192.168.0.7;Port=502"
```

- SIEMENS S7COMM over TCP:

```
"IP-Address=192.168.0.7;Port=502;Rack=0;Slot=2"
```

- **SIEMENS S7COMM over INDUSTRIAL ETHERNET:**
"MAC=00:01:02:03:04:05;Rack=0;Slot=2"
- **MITSUBISHI MELSEC SYSTEM Q:**
"IP-Address=192.168.0.7;Port=502;Network=0;Station=0;PC=255"
- **ALLEN-BRADLEY ETHERNET/IP:**
"IP-Address=192.168.0.7;Port=44818"
- **IEC 61850 MMS:**
"IP-Address=192.168.0.7;Port=502;Domains=IED_0009CTRL, IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"
- **IEC 61850 GOOSE:**
"Domains=IED_0009CTRL, IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"
- **IEC 60870-5-104:**
"IP-Address=192.168.0.7;Port=104;Asdu=2"
- **GENERAL ELECTRIC SRTP:**
"IP-Address=192.168.0.50;Port=18245"
- **IEC 61850 SAMPLED VALUES:**
"MAC=00:01:02:03:04:05;Domains=IED_TRANSFORMER1;Vendor=TMW;Model=IED"
- **SIEMENS S7COMMPLUS over TCP:**
"IP-Address=192.168.0.22;Port=102"
- **EMERSON DELTAV:**
"IP-Address=192.168.0.38;Port=18507"
- **OMRON FINS over UDP:**
"IP-Address=192.168.0.1;Port=9600"
- **MMS for ABB AC 800M:**
"IP-Address=192.168.0.60;Port=102"
- **YOKOGAWA VNET/IP:**
"IP-Address=192.168.0.4;Port=5313"

- **CODESYS V3 GATEWAY over TCP:**
"IP-Address=192.168.0.4;Port=11740"
- **DNP3:**
"IP-Address=192.168.1.10;Port=20000"
- **OMRON FINS over TCP:**
"IP-Address=192.168.0.1;Port=9600"
- **OPC UA BINARY:**
"IP-Address=192.168.0.213;Port=49320"
- **DMS for ABB AC 700F:**
"IP-Address=192.168.0.7;Port=9991"
- **OMRON FINS over ETHERNET/IP:**
"IP-Address=192.168.0.1;Port=44818"
- **OPC DA:**
"IP-Address=192.168.0.7;Port=135"
- **CODESYS V3 GATEWAY over UDP:**
"IP-Address=192.168.0.7;Port=1740"
- **BECKHOFF ADS/AMS:**
"IP-Address=192.168.0.7;Port=48898"
- **IEC 60870-5-101:**
"IP-Address=192.168.0.7;Port=950"
- **FOXBORO FCP270, FCP280 INTERACTION:**
"MAC=00:00:6C:C0:00:0A"
- **EMERSON CONTROLWAVE DATA EXCHANGE:**
"IP-Address=192.168.0.7;Port=1234"
- **HONEYWELL CONTROLEDGE 900 INTERACTION:**
"IP-Address=192.168.1.99;Port=41103"

- HONEYWELL EXPERION INTERACTION:
"IP-Address=192.168.1.10;Port=55553"
- SCHNEIDER ELECTRIC UMAS:
"IP-Address=192.168.0.7;Port=502"
- TASE.2:
"IP-Address=192.168.0.20;Port=102"
- PROFINET IO:
"MAC=00:01:02:03:04:05;\IP-Address=192.168.0.20;\Frame=IDS_TEL352"
- DIRECTLOGIC INTERACTION:
"IP-Address=192.168.0.70;Port=28784"
- BACNET:
"IP-Address=192.168.5.200;Port=47808"

Файл описания переменных и тегов: variables.csv

Файл описания переменных и тегов содержит перечисления тегов, их параметров и соединений, с которыми связаны теги.

В начале файла должны быть указаны заголовочные строки, которые содержат данные для обработки файла. Пример заголовочных строк файла variables.csv приведен ниже.

Пример

```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
```

Первые три заголовочные строки аналогичны заголовочным строкам в файле devices.csv (см. раздел "Файл описания устройств: devices.csv" на стр. [397](#)).

Строка

ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName содержит наименования столбцов с данными:

- ID – уникальный числовой идентификатор тега.
Идентификатор тега нужен для создания ссылок на тег в файле datasets.csv (см. раздел "Файл описания наборов данных (группы тегов): datasets.csv" на стр. [411](#)).
- 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` (см. раздел "Файл описания перечислений: `enums.csv`" на стр. [410](#)).

Пример:

Поле EnumName в файле variables.csv:

```
EnumName = "OnOffSwitch"
```

Описание перечисления в файле enums.csv:

```
"OnOffSwitch"; 0; "Включено"
```

```
"OnOffSwitch"; 1; "Отключено"
```

После заголовочных строк следует тело файла, содержащее значения параметров (например, идентификатор тега, имя тега, идентификатор соединения). Пример файла variables.csv приведен ниже.

Пример:

```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
5;"System.mitsub_n.ms_plc.Bit01";"ms_plc";"W0";4;0;0;0;0;0;0;"System.mitsub_n.ms_plc.Bit01";"";""
6;"System.mitsub_n.ms_plc.Register01";"ms_plc";"W20";9;0;0;0;0;0;0;"System.mitsub_n.ms_plc.Register01";"";""
1;"systemQ.Bit01";"mc_SysQ";"10";0;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=LNCClassName`, 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.
- FOXBORO FCP280 / FCP270 INTERACTION: строка с именем тега.
- HONEYWELL EXPERION INTERACTION: строка вида `[BLOCK_ID] : [SUBBLOCK_ID] : [PROPERTY_ID]`, где:
 - `BLOCK_ID` – порядковый номер блока в программе ПЛК, представленный целым числом в диапазоне 0–65535.
 - `SUBBLOCK_ID` – порядковый номер вложенного блока в программе ПЛК, представленный целым числом в диапазоне 0–65535.
 - `PROPERTY_ID` – порядковый номер параметра блока в программе ПЛК, представленный целым числом в диапазоне 0–65535.
- DIRECTLOGIC INTERACTION: строка вида `[Area] [ByteAddress] . [BitAddress]`, где:
 - `Area` – перечисление кодов области памяти в соответствии со спецификацией протокола: X, Y, C, S, T, CT, GX, GY, V, P, SP, B, PB.
 - `ByteAddress` – адрес регистра, представленный целым числом.
 - `BitAddress` – адрес бита внутри регистра, представленный целым числом.
- BACNET: строка вида `[OBJECT_TYPE] : [OBJECT_ID]`, где:
 - `OBJECT_TYPE` – тип объекта в соответствии со спецификацией протокола.
 - `OBJECT_ID` – порядковый номер объекта, представленный целым числом в диапазоне 0–4194303.
- PROFINET IO: строка вида `[IO] : [SubSlot] : [Index] : [Offset] . [BitAddress]`, где:
 - `IO` – направление переменной (input, output).
 - `SubSlot` – номер подслота, представленный целым числом.
 - `Index` – индекс тега, представленный целым числом.
 - `Offset` – адрес байта тега, представленный целым числом.
 - `BitAddress` – адрес бита внутри регистра, представленный целым числом (используется только для тегов с типом данных bool).

Кроме того, для правильной загрузки параметров протокола требуется указать файл GSDML, специфичный для устройства.

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 (см. раздел “Файл описания устройств: devices.csv” на стр. [397](#)).

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 (см. раздел "Файл описания устройств: devices.csv" на стр. [397](#)).

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 (см. раздел "Файл описания устройств: devices.csv" на стр. [397](#)).

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$DS
List";"Buffered"
"IED24151LD";"IED24151LD/LLN0$RP$urcbMX01";"urcbMX01";"IED24151LD/LLN0$MX
List";"Unbuffered"
```

Системные типы событий в Kaspersky Industrial CyberSecurity for Networks

Для регистрации событий в Kaspersky Industrial CyberSecurity for Networks используются системные типы событий (см. раздел "Настройка типов событий" на стр. [225](#)), автоматически созданные при установке программы.

Каждый тип события относится к определенной технологии регистрации событий (на стр. [307](#)).

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).

Таблица 10. Системные типы событий по технологии Контроль технологического процесса (DPI)

Код	Заголовок типа события	Важность	Условия для регистрации
4000002900	\$technology_rule	<i>Критические</i>	<p>Сработало правило контроля процесса (см. раздел "Настройка контроля процесса" на стр. 152).</p> <p>В заголовке и в описании системного типа события используются следующие переменные:</p> <ul style="list-style-type: none"> \$technology_rule – название правила; \$tags – полученные значения тегов, для которых заданы условия в правиле. <p>В зарегистрированном событии для заголовка, описания и уровня важности события используются пользовательские параметры, заданные в сработавшем правиле контроля процесса.</p>
4000000001	Тестовое событие (DPI)	<i>Информационные</i>	<p>Обнаружен тестовый сетевой пакет (см. раздел "Проверка регистрации событий с помощью тестового сетевого пакета" на стр. 58).</p>

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).

Таблица 11. Системный тип события по технологии Контроль системных команд (CC)

Код	Заголовок типа события	Важность	Условия для регистрации
4000002602	\$systemCommandShort	Определяется по уровню важности системной команды	<p>Обнаружена системная команда, выбранная для отслеживания (см. раздел "Выбор отслеживаемых системных команд" на стр. 160) (при этом для системной команды нет включенного правила контроля взаимодействий (см. раздел "Настройка контроля взаимодействий" на стр. 185)).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> \$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).

Таблица 12. Системные типы событий по технологии Контроль целостности сети (NIC)

Код	Заголовок типа события	Важность	Условия для регистрации
4000002601	Обнаружено неразрешенное сетевое взаимодействие (\$stop_level_protocol)	<i>Важные</i>	<p>Обнаружено сетевое взаимодействие, не указанное во включенном правиле контроля взаимодействий (см. раздел "Настройка контроля взаимодействий" на стр. 185).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> \$stop_level_protocol – название протокола верхнего уровня; \$protocol – название протокола прикладного уровня.

Код	Заголовок типа события	Важность	Условия для регистрации
4000002700	Отсутствует трафик на точке мониторинга \$monitoringPoint	<i>Важные</i>	На сетевой интерфейс, связанный с точкой мониторинга, не поступает трафик более 15 секунд. В заголовке и в описании типа события используются следующие переменные: <ul style="list-style-type: none"> • \$monitoringPoint – название точки мониторинга; • \$interface – имя сетевого интерфейса, который связан с точкой мониторинга; • \$duration – длительность отсутствия трафика (в секундах).
4000000002	Тестовое событие (NIC)	<i>Информационные</i>	Обнаружен тестовый сетевой пакет (см. раздел "Проверка регистрации событий с помощью тестового сетевого пакета" на стр. 58) (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).

Таблица 13. Системные типы событий по технологии Обнаружение вторжений (IDS)

Код	Заголовок типа события	Важность	Условия для регистрации
4000003000	Сработало правило из набора \$fileName (системный набор правил)	Определяется по приоритету правила	Сработало правило обнаружения вторжений (см. раздел "Правила обнаружения вторжений" на стр. 203), входящее в системный набор правил (набор правил находится в активном состоянии). В заголовке и в описании типа события используются следующие переменные: <ul style="list-style-type: none"> • \$fileName – название набора правил; • \$category – класс правила; • \$ruleName – название правила; • \$severity – приоритет правила; • \$signature_id – идентификатор правила (sid); • \$action – тип действия с сетевыми пакетами, заданный в правиле (действия типов <code>drop</code> или <code>reject</code> не выполняются в Kaspersky Industrial CyberSecurity for Networks).

Код	Заголовок типа события	Важность	Условия для регистрации
4000003001	Сработало правило из набора \$fileName (пользовательский набор правил)	Определяется по приоритету правила	<p>Сработало правило обнаружения вторжений (см. раздел "Правила обнаружения вторжений" на стр. 203), входящее в пользовательский набор правил (набор правил находится в активном состоянии).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$fileName – название набора правил; • \$category – класс правила; • \$ruleName – название правила; • \$severity – приоритет правила; • \$signature_id – идентификатор правила (sid); • \$action – тип действия с сетевыми пакетами, заданный в правиле (действия типов <code>drop</code> или <code>reject</code> не выполняются в Kaspersky Industrial CyberSecurity for Networks).
4000004001	Обнаружены признаки ARP-спуфинга в ARP-ответах	<i>Критические</i>	<p>Обнаружены признаки подмены адресов в ARP-пакетах (см. раздел "Дополнительные методы обнаружения вторжений" на стр. 204): несколько ARP-ответов, которые не связаны с ARP-запросами.</p> <p>В описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$senderIp – подменяемый IP-адрес; • \$targetIp – IP-адрес целевого узла; • \$attackStartTimestamp – время обнаружения первого ARP-ответа.
4000004002	Обнаружены признаки ARP-спуфинга в ARP-запросах	<i>Критические</i>	<p>Обнаружены признаки подмены адресов в ARP-пакетах (см. раздел "Дополнительные методы обнаружения вторжений" на стр. 204): несколько ARP-запросов с одного MAC-адреса разным получателям.</p> <p>В описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$senderIp – подменяемый IP-адрес; • \$targetIp – IP-адрес целевого узла; • \$attackStartTimestamp – время обнаружения первого ARP-ответа.

Код	Заголовок типа события	Важность	Условия для регистрации
4000005100	Обнаружена аномалия в протоколе IP: конфликт данных при сборке IP-пакета	<i>Критические</i>	Обнаружена аномалия в протоколе IP (см. раздел "Дополнительные методы обнаружения вторжений" на стр. 204): при наложении фрагментов IP-пакета данные не совпадают.
4000005101	Обнаружена аномалия в протоколе IP: превышение размера фрагментированного IP-пакета	<i>Критические</i>	Обнаружена аномалия в протоколе IP (см. раздел "Дополнительные методы обнаружения вторжений" на стр. 204): фактический суммарный размер фрагментированного IP-пакета после сборки превышает допустимый предел.
4000005102	Обнаружена аномалия в протоколе IP: размер начального фрагмента IP-пакета меньше ожидаемого	<i>Критические</i>	Обнаружена аномалия в протоколе IP (см. раздел "Дополнительные методы обнаружения вторжений" на стр. 204): размер начального фрагмента IP-пакета меньше минимально допустимого значения.
4000005103	Обнаружена аномалия в протоколе IP: несоответствие фрагментов IP-пакета (mis-associated fragments)	<i>Важные</i>	Обнаружена аномалия в протоколе IP (см. раздел "Дополнительные методы обнаружения вторжений" на стр. 204): фрагменты собираемого IP-пакета содержат различные данные о длине фрагментированного пакета.
4000002701	Обнаружена аномалия в протоколе TCP: подмена содержимого в перекрывающихся TCP-сегментах	<i>Критические</i>	Обнаружена аномалия в протоколе TCP (см. раздел "Дополнительные методы обнаружения вторжений" на стр. 204): пакеты содержат перекрывающиеся TCP-сегменты с различающимся содержимым.
4000000003	Тестовое событие (IDS)	<i>Информационные</i>	Обнаружен тестовый сетевой пакет (см. раздел "Проверка регистрации событий с помощью тестового сетевого пакета" на стр. 58) (при включенном методе обнаружения вторжений по правилам).

Системные типы событий по технологии Контроль активов

В этом разделе приведено описание системных типов событий, относящихся к технологии Контроль активов (см. таблицу ниже).

Таблица 14. Системные типы событий по технологии Контроль активов (AM)

Код	Заголовок типа события	Важность	Условия для регистрации
4000005003	Обнаружено новое устройство с адресом \$owner_ip_or_mac	<i>Критические</i>	<p>В режиме наблюдения контроля активов (см. раздел "Настройка контроля активов" на стр. 120) автоматически добавлено новое устройство по обнаруженному IP- или MAC-адресу, который не указан для других устройств в таблице.</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$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	<i>Информационные</i>	<p>В режиме наблюдения контроля активов (см. раздел "Настройка контроля активов" на стр. 120) автоматически обновлены сведения об устройстве на основе полученных данных из трафика.</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$owner_ip_or_mac – IP- или MAC-адрес устройства; • \$asset_name – имя устройства; • \$updated_params – список обновленных сведений; • \$asset_id – идентификатор устройства.

Код	Заголовок типа события	Важность	Условия для регистрации
4000005005	Обнаружен конфликт IP-адреса \$owner_ip	<i>Критические</i>	<p>В режиме наблюдения контроля активов (см. раздел "Настройка контроля активов" на стр. 120) обнаружено использование IP-адреса не тем устройством, для которого был указан этот IP-адрес.</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$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	<i>Критические</i>	<p>В режиме наблюдения контроля активов (см. раздел "Настройка контроля активов" на стр. 120) обнаружена активность устройства, которому был присвоен статус <i>Неиспользуемое</i>.</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$owner_ip_or_mac – IP- или MAC-адрес устройства; • \$asset_name – имя устройства; • \$last_seen_timestamp – дата и время последнего появления устройства в сети; • \$asset_id – идентификатор устройства.

Код	Заголовок типа события	Важность	Условия для регистрации
4000005007	Обнаружен новый IP-адрес \$new_ip_addr у устройства с MAC-адресом \$owner_mac	<i>Критические</i>	<p>В режиме наблюдения контроля активов (см. раздел "Настройка контроля активов" на стр. 120) обнаружен новый IP-адрес, использованный устройством.</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$new_ip_addr – обнаруженный IP-адрес; • \$owner_mac – MAC-адрес устройства; • \$asset_name – имя устройства; • \$owner_ips_list – список других IP-адресов устройства; • \$asset_id – идентификатор устройства.
4000005008	Добавлен MAC-адрес \$owner_mac устройству с IP-адресом \$owner_ip	<i>Информационные</i>	<p>В режиме наблюдения контроля активов (см. раздел "Настройка контроля активов" на стр. 120) автоматически добавлен MAC-адрес для сетевого интерфейса, у которого был указан только IP-адрес (при этом устройство было со статусом <i>Неразрешенное</i> или <i>Неиспользуемое</i>).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$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	<i>Информационные</i>	<p>В режиме наблюдения контроля активов (см. раздел "Настройка контроля активов" на стр. 120) автоматически добавлен IP-адрес для сетевого интерфейса, у которого был указан только MAC-адрес (при этом устройство было со статусом <i>Неразрешенное</i> или <i>Неиспользуемое</i>).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$owner_ip – обнаруженный IP-адрес устройства; • \$owner_mac – MAC-адрес устройства; • \$asset_name – имя устройства; • \$asset_id – идентификатор устройства.

Код	Заголовок типа события	Важность	Условия для регистрации
4000005010	Обнаружен новый MAC-адрес \$new_mac_addr у устройства с IP-адресом \$owner_ip	<i>Критические</i>	<p>В режиме наблюдения контроля активов (см. раздел "Настройка контроля активов" на стр. 120) обнаружен новый MAC-адрес, использованный устройством (при этом для устройства выключено автоматическое обновление адресной информации).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$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	<i>Критические</i>	<p>При контроле чтения и записи проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. 277) обнаружена операция чтения неизвестного блока проекта из ПЛК (если отсутствует сохраненная информация об этом блоке).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$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	<i>Критические</i>	<p>При контроле чтения и записи проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. 277) 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).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$asset_name – имя устройства; • \$block_name – имя блока; • \$saved_date_time – дата и время сохранения блока в программе.

Код	Заголовок типа события	Важность	Условия для регистрации
4000005202	Контроль проектов ПЛК: обнаружена запись нового блока в ПЛК \$asset_name	<i>Критические</i>	<p>При контроле чтения и записи проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. 277) обнаружена операция записи неизвестного блока проекта из ПЛК (если отсутствует сохраненная информация об этом блоке).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$asset_name – имя устройства; • \$block_name – имя блока; • \$saved_date_time – дата и время обнаружения операции.
4000005203	Контроль проектов ПЛК: обнаружена запись известного блока в ПЛК \$asset_name	<i>Критические</i>	<p>При контроле чтения и записи проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. 277) обнаружена операция записи известного блока проекта из ПЛК (если есть сохраненная информация об этом блоке, но полученная информация не совпадает с последней сохраненной информацией об этом блоке).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$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	<i>Критические</i>	<p>При контроле чтения и записи проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. 277) обнаружена операция чтения неизвестного проекта из ПЛК (если отсутствует сохраненная информация об этом проекте).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$asset_name – имя устройства; • \$saved_date_time – дата и время обнаружения операции.

Код	Заголовок типа события	Важность	Условия для регистрации
4000005205	Контроль проектов ПЛК: обнаружено чтение известного проекта из ПЛК \$asset_name	<i>Критические</i>	<p>При контроле чтения и записи проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. 277) 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).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$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	<i>Критические</i>	<p>При контроле чтения и записи проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. 277) обнаружена операция записи нового проекта в ПЛК (если отсутствует сохраненная информация об этом проекте).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$asset_name – имя устройства; • \$saved_date_time – дата и время обнаружения операции.
4000005207	Контроль проектов ПЛК: обнаружена запись известного проекта в ПЛК \$asset_name	<i>Критические</i>	<p>При контроле чтения и записи проектов ПЛК (см. раздел "Контроль чтения и записи проектов ПЛК" на стр. 277) 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).</p> <p>В заголовке и в описании типа события используются следующие переменные:</p> <ul style="list-style-type: none"> • \$asset_name – имя устройства; • \$saved_date_time – дата и время сохранения проекта в программе.

Код	Заголовок типа события	Важность	Условия для регистрации
4000000004	Тестовое событие (AM)	<i>Информационные</i>	Обнаружен тестовый сетевой пакет (см. раздел "Проверка регистрации событий с помощью тестового сетевого пакета" на стр. 58) (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).

Таблица 15. Системные типы событий по технологии Внешние системы (EXT)

Код	Заголовок типа события	Важность	Условия для регистрации
8000000001	Инцидент	Определяется по уровню важности правила корреляции	Обнаружена последовательность событий, удовлетворяющих условиям правила корреляции (см. раздел "Мониторинг событий и инцидентов" на стр. 305). При регистрации события в качестве заголовка и описания инцидента указываются заголовок и описание из правила корреляции.
4000005400	Событие от внешней системы	Определяется внешней системой	Поступило событие от внешней системы с использованием Kaspersky Industrial CyberSecurity for Networks API (см. раздел "Использование Kaspersky Industrial CyberSecurity for Networks API" на стр. 240). При регистрации события содержимое заголовка и описания определяются внешней системой.