kaspersky

Kaspersky Industrial CyberSecurity for Nodes 5.0

© 2026 АО "Лаборатория Касперского"

Содержание

- Kaspersky Industrial CyberSecurity for Nodes
  - Что нового
  - Исправленные ошибки
  - Комплект поставки
  - Аппаратные и программные требования
  - Поддерживаемые версии Kaspersky Security Center
  - Kaspersky Virus Removal Tool
  - Функциональные требования и ограничения
    - Установка и удаление приложения
    - Контроль целостности системы
    - Сетевой экран
    - Ограничения в устаревших версиях Windows
    - Интеграция с Kaspersky Security Center
    - Прочие ограничения
  - Типовые схемы развертывания
  - Совместимость с другими приложениями
- Установка и удаление приложения
  - Планирование установки
    - Выбор средств администрирования
    - Выбор способа установки
    - Используемые порты
  - Установка и удаление приложения с помощью мастера
    - Установка с помощью мастера установки
      - Установка Kaspersky Industrial CyberSecurity for Nodes
      - Установка Консоли Kaspersky Industrial CyberSecurity for Nodes
      - Дополнительная настройка после установки Консоли приложения на другое устройство
      - Действия после установки Kaspersky Industrial CyberSecurity for Nodes
        - Запуск и настройка задачи Обновление баз и модулей приложения
        - Проверка важных областей
    - Изменение состава компонентов и восстановление Kaspersky Industrial CyberSecurity for Nodes
    - Удаление с помощью мастера установки
      - Удаление Kaspersky Industrial CyberSecurity for Nodes
      - Удаление Консоли Kaspersky Industrial CyberSecurity for Nodes
  - Установка и удаление приложения из командной строки
    - Об установке и удалении Kaspersky Industrial CyberSecurity for Nodes из командной строки
    - Коды программных компонентов Kaspersky Industrial CyberSecurity for Nodes для службы установщика Windows
    - Настройки установки и восстановления приложения и ключи командной строки для службы установщика Windows
    - Примеры команд установки Kaspersky Industrial CyberSecurity for Nodes
    - Действия после установки Kaspersky Industrial CyberSecurity for Nodes
    - Добавление и удаление компонентов. Примеры команд
    - Удаление Kaspersky Industrial CyberSecurity for Nodes. Примеры команд
    - Коды возврата

Установка и удаление приложения с помощью Kaspersky Security Center
Общие сведения об установке через Kaspersky Security Center
Права для установки или удаления Kaspersky Industrial CyberSecurity for Nodes
Установка Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center
Действия после установки Kaspersky Industrial CyberSecurity for Nodes
Установка Консоли приложения через Kaspersky Security Center
Удаление Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center
Изменение состава компонентов приложения с помощью Kaspersky Security Center
Установка и удаление приложения через групповые политики Active Directory
Установка Kaspersky Industrial CyberSecurity for Nodes через групповые политики Active Directory
Действия после установки Kaspersky Industrial CyberSecurity for Nodes
Удаление Kaspersky Industrial CyberSecurity for Nodes через групповые политики Active Directory
Журналы установки и удаления Kaspersky Industrial CyberSecurity for Nodes
Изменения в системе после установки Kaspersky Industrial CyberSecurity for Nodes
Процессы Kaspersky Industrial CyberSecurity for Nodes
Проверка функций Kaspersky Industrial CyberSecurity for Nodes. Использование тестового вируса EICAR
О тестовом вирусе EICAR
Проверка функций постоянной защиты файлов и проверки по требованию
Обновление Kaspersky Industrial CyberSecurity for Nodes предыдущих версий до версии 5.0
Об обновлении Kaspersky Industrial CyberSecurity for Nodes
Об обновлении средств администрирования Kaspersky Industrial CyberSecurity for Nodes
Миграция политик и задач
Миграция настроек обновляемой версии приложения
Соответствие компонентов и задач Kaspersky Industrial CyberSecurity for Nodes версии 4.0 и 5.0
Установка и удаление Kaspersky Security Gateway
Об обновлении Kaspersky Security Gateway
Установка Kaspersky Security Gateway с помощью мастера установки
Шаг 1. Проверка требований к установке
Шаг 2. Страница приветствия в начале установки
Шаг 3. Ознакомление с текстом Лицензионного соглашения и Политики конфиденциальности
Шаг 4. Выбор папки назначения
Шаг 5. Выбор компонентов
Шаг 6. Настройка подключения к системе SCADA
Шаг 7. Установка Kaspersky Security Gateway
Установка Kaspersky Security Gateway из командной строки
Удаление Kaspersky Security Gateway
Шаг 1. Сохранение данных Kaspersky Security Gateway для дальнейшего использования
Шаг 2. Удаление Kaspersky Security Gateway
Установка OPC Core Components Redistributables
Интерфейс приложения
Работа с Плагином управления
Управление Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center
Управление параметрами приложения
Настройка общих параметров приложения в Kaspersky Security Center
Настройка параметров интерфейса и проверки в Kaspersky Security Center
Настройка параметров безопасности в Kaspersky Security Center

Настройка параметров соединения в Kaspersky Security Center
Настройка режима запуска локальных задач
Настройка параметров карантина и резервного хранилища в Kaspersky Security Center
Создание и настройка политик
Создание политики
Настройка политики
Создание и настройка задач в Kaspersky Security Center
О создании задач в Kaspersky Security Center
Создание задачи в Kaspersky Security Center
Переход к параметрам локальной задачи и общим параметрам приложения для отдельного компьютера
Настройка групповых задач в Kaspersky Security Center
Задача Активация приложения
Задача обновления
Проверка целостности приложения
Настройка расписания задач
Отчеты в Kaspersky Security Center
Статус постоянной защиты
Работа с Консолью Kaspersky Industrial CyberSecurity for Nodes
Запуск Консоли приложения
Интерфейс Консоли Kaspersky Industrial CyberSecurity for Nodes
Окно Консоли Kaspersky Industrial CyberSecurity for Nodes
Значок области уведомлений в панели задач
Настройка общих параметров в Консоли приложения
Управление задачами Kaspersky Industrial CyberSecurity for Nodes
Категории задач Kaspersky Industrial CyberSecurity for Nodes
Запуск, приостановка, возобновление, остановка задач вручную
Настройка расписания задач
Использование учетных записей для запуска задач
Об использовании учетных записей для запуска задач
Указание учетной записи для запуска задачи
Импорт и экспорт настроек
Об импорте и экспорте настроек
Экспорт настроек
Импорт настроек
Просмотр состояния защиты и информации о Kaspersky Industrial CyberSecurity for Nodes
Настройка параметров резервного хранилища в Консоли приложения
Работа с Веб-плагином из Web Console
Управление Kaspersky Industrial CyberSecurity for Nodes из Web Console
Ограничения Веб-плагина
Управление параметрами приложения
Настройка общих параметров приложения с помощью Веб-плагина
Настройка параметров интерфейса и проверки с помощью Веб-плагина
Настройка параметров безопасности и надежности с помощью Веб-плагина
Настройка параметров соединения с помощью Веб-плагина
Настройка запуска по расписанию локальных задач с помощью Веб-плагина
Настройка параметров карантина и резервного хранилища с помощью Веб-плагина
Создание и настройка политик

- Создание и настройка задач в Kaspersky Security Center
  - О создании задач с помощью Веб-плагина
  - Создание задачи с помощью Веб-плагина
  - Настройка групповых задач с помощью Веб-плагина
    - Настройка задачи Активация приложения с помощью Веб-плагина
    - Настройка задачи обновления с помощью Веб-плагина
  - Настройка расписания задач
- Отчеты в Kaspersky Security Center

Лицензирование приложения
- О Лицензионном соглашении
- О лицензии
- О Лицензионном сертификате
- О ключе
- О файле ключа
- О коде активации
- Активация приложения с помощью файла ключа
- Активация приложения с помощью кода активации
- Просмотр информации о действующей лицензии
- Продление срока действия лицензии
- Удаление ключа

Запуск и остановка Kaspersky Industrial CyberSecurity for Nodes
- Запуск и остановка приложения
- Приостановка и восстановление защиты и контроля компьютера

Диагностическое окно
- О диагностическом окне
- Просмотр состояния Kaspersky Industrial CyberSecurity for Nodes с помощью диагностического окна
- Просмотр статистики событий безопасности
- Просмотр текущей активности приложения
- Настройка трассировки работы приложения и записи дампов памяти

Механизмы самозащиты Kaspersky Industrial CyberSecurity for Nodes
- Включение и выключение механизмов самозащиты
- Поддержка технологии AM-PPL
- Защита сервисов операционной системы
- Настройка прав пользователей на управление Kaspersky Industrial CyberSecurity for Nodes
- Настройка прав пользователей на управление службой Kaspersky Industrial CyberSecurity for Nodes Service
- Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля
- Уведомления Безопасного рабочего стола

Доверенная зона
- Создание исключения из проверки
- Выбор типов обнаруживаемых объектов
- Формирование списка доверенных приложений
- Создание локальной доверенной зоны
- Экспорт и импорт доверенной зоны
- Использование доверенного системного хранилища сертификатов
- Предустановленные исключения из проверки и доверенные приложения
- Профили исключений для промышленных программ

Постоянная защита файлов
Об области защиты и параметрах безопасности задачи
Стандартные области защиты
Стандартные уровни безопасности
Расширения файлов, проверяемые по умолчанию компонентом Постоянная защита файлов
Настройка компонента Постоянная защита файлов
Настройка области защиты для компонента Постоянная защита файлов
Настройка параметров безопасности вручную
Проверка контейнеров
Использование KSN
Включение использования Kaspersky Security Network
Статистика использования Kaspersky Security Network
Ограничения работы с Kaspersky Private Security Network
Настройка KSN Proxy
Защита от эксплойтов
Режимы защиты от эксплойтов
Включение и выключение Защиты от эксплойтов
Включение и выключение защиты памяти
Формирование списка защищаемых процессов
Откат вредоносных действий
Защита от шифрования
Включение и выключение защиты локальных папок от шифрования
Защита папок общего доступа от внешнего шифрования
Включение и выключение защиты папок общего доступа от внешнего шифрования
Формирование области защиты
Добавление доверенных компьютеров для внешнего шифрования данных
Настройка периода блокировки недоверенного компьютера
Экспорт и импорт списка исключений из защиты папок общего доступа от внешнего шифрования
Защита от сетевых угроз
Включение и настройка общих параметров Защиты от сетевых угроз
Создание исключения из блокирования
Экспорт и импорт списка исключений из защиты папок общего доступа от внешнего шифрования
AMSI-защита
Включение и выключение AMSI-защиты
Настройка параметров AMSI-защиты
Контроль запуска программ
О правилах контроля запуска программ
О Контроле пакетов установки
О формировании правил контроля запуска программ
Включение и настройка общих параметров Контроля запуска программ
Настройка Контроля пакетов установки
Работа с правилами контроля запуска программ
Добавление правил контроля запуска программ
Добавление условий срабатывания правила контроля запуска программ
Добавление исключений из области действия правила контроля запуска программ
Разрешение запуска всех приложений

Экспорт правил контроля запуска программ
Формирование TXT-файла с выборкой событий Kaspersky Security Center о заблокированных приложениях
Настройка групповой задачи Формирование правил контроля запуска программ
Создание правил с помощью групповой задачи Формирование правил контроля запуска программ
Контроль устройств
О правилах доступа к устройствам
Контроль доступа к устройствам по типу
Контроль подключения к Wi-Fi
Контроль печати
Контроль устройств ввода (HID)
Контроль доступа к мобильным устройствам
Мониторинг использования съемных дисков
Контроль доступа к Bluetooth-устройствам
Разграничение прав доступа пользователей к устройствам
О формировании правил контроля устройств
Добавление доверенных устройств
Экспорт и импорт списка доверенных устройств
Сетевой экран
О правилах сетевого экрана
Настройка Сетевого экрана
Настройка общих параметров Сетевого экрана
Создание и настройка правил Сетевого экрана
Включение и выключение правил Сетевого экрана
Защита от атак BadUSB
Контроль целостности системы
О правилах Контроля целостности системы
Контроль целостности системы в режиме реального времени
Проверка целостности системы по запросу
Экспорт и импорт правил Контроля целостности системы
Просмотр отчетов о работе Контроля целостности системы
Анализ журналов
Добавление пользовательских правил
Настройка предустановленных правил
Анализатор производительности
Проверка по требованию
О задачах проверки по требованию
Об области проверки и параметрах безопасности задачи
Стандартные области проверки
Проверка файлов в интернет-хранилище
Стандартные уровни безопасности
Проверка съемных дисков
Заданные по умолчанию параметры задач проверки по требованию
Управление задачами проверки по требованию
Создание задачи проверки по требованию
Выполнение задач проверки по требованию в фоновом режиме
Регистрация выполнения задачи Проверка важных областей
Настройка области проверки для задачи проверки по требованию

Настройка параметров задачи Проверка по требованию

Настройка проверки съемных дисков

Выбор стандартных уровней безопасности в задачах проверки по требованию

Настройка параметров безопасности вручную

Статистика задач проверки по требованию

Защита промышленной сети

О проверке целостности проектов ПЛК

Настройка задачи Проверка целостности проектов ПЛК

Настройка получения данных о проектах ПЛК

Настройка проверки целостности проектов ПЛК

Включение и выключение проверки целостности проектов ПЛК

О реестре конфигураций ПЛК

Настройка реестра ПЛК

Аудит безопасности

Ограничения для параметров задачи аудита безопасности

Поддерживаемые типы OVAL-проверок

Управление задачами аудита безопасности

Создание и настройка задачи аудита безопасности с параметрами по умолчанию

Настройка параметров задачи аудита безопасности с использованием базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП

Настройка параметров задачи аудита безопасности с использованием конфигурации безопасности и соответствий стандартам

Настройка параметров задачи аудита безопасности с использованием пользовательской базы правил из хранилища Kaspersky Security Center

Настройка параметров задачи аудита безопасности с использованием пользовательской базы из файла

Просмотр результатов выполнения задачи аудита безопасности

Экспорт результатов выполнения задачи аудита безопасности в отдельный файл

Создание отпечатка сертификата подписи для файлов с OVAL- или XCCDF-правилами

Создание инсталляционного пакета Kaspersky Security Center с пользовательскими OVAL- или XCCDF-правилами

Использование Kaspersky Security Gateway

Диагностические данные

Ограничения и известные ошибки для Kaspersky Security Gateway

Интерфейс Консоли Kaspersky Security Gateway

Настройка соединения с Kaspersky Security Center

Настройка соединения с Kaspersky Industrial CyberSecurity for Networks

Настройка протокола DCOM

Настройка параметров передачи данных с использованием протоколов связи

Настройка передачи данных по протоколу IEC 60870-5-104

Настройка передачи данных по протоколу OPC DA

Настройка передачи данных по протоколу OPC UA

Настройка передачи данных с помощью конфигурационного файла

Настройка дополнительных параметров Kaspersky Security Gateway

Просмотр событий Kaspersky Security Gateway

Управление полнодисковым шифрованием BitLocker

Запуск шифрования диска BitLocker

Расшифровка жесткого диска, защищенного BitLocker

Восстановление доступа к диску, защищенному BitLocker
Приостановка защиты BitLocker для обновления программного обеспечения
Интеграция со сторонними системами
Счетчики производительности для программы Системный монитор
Количество запросов, не обработанных из-за нехватки ресурсов
Количество запросов, отданных на обработку
Количество объектов, обрабатываемых за секунду
Количество элементов в очереди зараженных объектов
Общее количество отвергнутых запросов
Общее количество пропущенных запросов
Максимальное количество потоков диспетчера файловых перехватов
Среднее количество потоков диспетчера файловых перехватов
SNMP-счетчики и ловушки в Kaspersky Industrial CyberSecurity for Nodes
SNMP-счетчики Kaspersky Industrial CyberSecurity for Nodes
Счетчики производительности
Счетчик резервного хранилища
Общие счетчики
Счетчик обновлений
Счетчики постоянной защиты файлов
Счетчики AMSI-защиты
SNMP-ловушки Kaspersky Industrial CyberSecurity for Nodes и их параметры
Описания и возможные значения параметров SNMP-ловушек Kaspersky Industrial CyberSecurity for Nodes
Интеграция с WMI
Обновление баз и модулей Kaspersky Industrial CyberSecurity for Nodes
Об обновлении баз и модулей приложения
О задачах обновления
Схемы обновления баз и модулей Kaspersky Industrial CyberSecurity for Nodes
Настройка задачи обновления
SMU-обновление приложения
Безопасное копирование баз приложения
Безопасное обновление баз приложения
Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes
Статистика задачи Обновление
Решения Detection and Response
Kaspersky Industrial CyberSecurity Endpoint Detection and Response
Архитектура решения
Совместимость с приложениями "Лаборатории Касперского"
Развертывание и первоначальная настройка решения
Активация решения
Настройка отчета об угрозах для отображения деталей алертов
Добавление виджета EDR-алертов
Проверка работоспособности решения на устройствах
Переход на Kaspersky Industrial CyberSecurity Endpoint Detection and Response с расширенной функциональностью

- Действия по реагированию
  - Сетевая изоляция устройства
  - Поиск IOC
    - Требования к IOC-файлам
    - Расширенный сбор телеметрии для поиска IOC
    - Область поиска IOC в реестре (RegistryItem)
  - Запуск проверки важных областей
  - Запрет запуска объектов
  - Запуск процесса
  - Завершение процесса
  - Получение файла
  - Удаление файла
  - Помещение файла на карантин
    - Просмотр файлов на карантине
    - Отправка файла из карантина в Kaspersky TIP
  - Cloud Sandbox
- Работа с деталями алерта
  - О деталях алерта
  - Просмотр деталей алерта
  - Применение и снятие сетевой изоляции
  - Помещение файла на карантин из деталей алерта
  - Создание задачи поиска IOC из деталей алерта
  - Запрет запуска объекта из деталей алерта
  - Действия по реагированию для пользователей Active Directory из деталей алерта
    - Сброс пароля пользователя
    - Блокировка учетной записи пользователя
    - Добавление пользователя в группу безопасности
    - Удаление пользователя из группы безопасности
  - Назначение учебных курсов Kaspersky ASAP пользователям из деталей алерта
- Мониторинг и отчеты
  - Просмотр списка алертов
  - Просмотр информации о срабатывании правил запрета запуска
  - Просмотр списка изолированных устройств

Режим Endpoint Agent
- Установка Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent
- Совместимость со сторонними EPP-приложениями

Managed Detection and Response
- Настройка интеграции с MDR

Kaspersky Anti Targeted Attack Platform
- Настройка интеграции с KATA
- Настройка отправки телеметрии

Endpoint Detection and Response Expert (on-premises)
- Настройка интеграции с EDR Expert (on-premises)
- Настройка отправки телеметрии EDR Expert (on-premises)
- Исключения из телеметрии EDR Expert (on-premises)
- Экспорт и импорт фильтров событий EDR Expert (on-premises)
- YARA-проверка

- Исключения EDR-телеметрии
- Интеграция с Kaspersky Industrial CyberSecurity for Networks
  - Особенности работы и ограничения интеграции с Kaspersky Industrial CyberSecurity for Networks
  - Настройка мониторинга сетей Wi-Fi
- Мониторинг EDR-действий
- Kaspersky Endpoint Agent
  - Миграция конфигурации [KICS+KEA] на [KICS+встроенный Enpoint Agent]
  - Миграция политик и задач конфигурации [KICS+KEA] на [KICS+встроенный агент]

Интеграция с SIEM
- Фильтрация событий для отправки в SIEM
- Экспорт и импорт правил фильтрации событий телеметрии

Обнаружение аномалий с помощью Sigma-правил
- Особенности работы и ограничения обнаружения аномалий с помощью Sigma-правил
- Включение обнаружения аномалий с помощью Sigma-правил
- Добавление Sigma-правил в пользовательскую коллекцию
- Фильтрация Sigma-правил внутри коллекции правил
- Экспорт и импорт Sigma-правил пользовательской коллекции
- Изменение Sigma-правила
- Исключения в Sigma-правиле

Изолирование и резервное копирование объектов
- Изолирование возможно зараженных объектов. Карантин
  - Просмотр объектов на карантине
    - Сортировка объектов на карантине
    - Фильтрация объектов на карантине
  - Восстановление содержимого карантина
  - Удаление объектов с карантина
  - Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"
  - Настройка параметров карантина
- Резервное копирование объектов. Резервное хранилище
  - Просмотр объектов в резервном хранилище
    - Сортировка файлов в резервном хранилище
    - Фильтрация файлов в резервном хранилище
  - Восстановление файлов из резервного хранилища
  - Удаление файлов из резервного хранилища
  - Настройка параметров резервного хранилища
  - Статистика резервного хранилища
- Устранение необработанных угроз
- Блокировка доступа к сетевым ресурсам. Заблокированные сетевые сеансы
  - Список заблокированных сетевых сеансов
  - Управление списком заблокированных сетевых сеансов

Запись событий. Журналы Kaspersky Industrial CyberSecurity for Nodes
- Способы записи событий Kaspersky Industrial CyberSecurity for Nodes
- Настройка параметров журнала
  - Сортировка событий в журнале
  - Фильтрация событий в журнале
  - Удаление событий из журнала
  - Экспорт информации из журнала

Журнал системного аудита
Журналы работы компонентов и задач
Просмотр статистики и информации о задачах Kaspersky Industrial CyberSecurity for Nodes в журналах выполнения задач
Просмотр журнала событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий"
Способы уведомления администратора и пользователей
Настройка уведомлений администратора и пользователей
Настройка почтовых уведомлений
Настройка обмена информацией с Сервером администрирования
Настройка формирования инцидентов
Portable Auditor
Аппаратные и программные требования
Ограничения функциональности Portable Auditor
Создание Portable Auditor
Обновление Portable Auditor
Работа с Консолью Portable Auditor
Проверка устройств
Настройка задачи Поиск вредоносного ПО
Настройка задачи Аудит безопасности
Настройка задачи Запись сетевого трафика
Экспорт и импорт настроек задач
Просмотр информации о лицензии
Просмотр результатов проверки
О составе и хранении файлов, содержащих результаты работы Portable Auditor
Просмотр общего отчета о работе Portable Auditor
Обновление баз Portable Auditor
Настройка трассировки работы Portable Auditor и записи дампов памяти
Работа с Portable Auditor через командную строку
Экспорт результатов работы Portable Auditor с защищенного съемного диска
Блокировка доступа к защищенным съемным дискам
Управление Kaspersky Industrial CyberSecurity for Nodes из командной строки
APPCONTROL. Импорт правил контроля запуска программ
APPCONTROL /CONFIG. Настройка компонента Контроль запуска программ
APPCONTROL /GENERATE. Формирование правил контроля запуска программ.
CONFIG. Поддержка технологии AM-PPL
CREATEPORTABLE. Создание Portable Auditor
DEVCONTROL. Импорт правил контроля устройств
DUMP. Запись дампов памяти
EDR_EXPERT_ON_PREM. Интеграция с EDR Expert (on-premises)
EDRKATA. Интеграция с KATA
EXITPOLICY. Выключение политики на устройстве
EXPORT. Экспорт настроек приложения
FBRESET. Очистка базы iSwift
FIM /BASELINE. Мониторинг целостности системы на основе эталона
HELP. Вызов справки о командах
IMPORT. Импорт настроек приложения
KICS. Интеграция с Kaspersky Industrial CyberSecurity for Networks

ISOLATION. Управление Сетевой изоляцией
KSN. Использование KSN/KPSN
LICENSE. Активация приложения
MDR. Настройка интеграции с Managed Detection and Response
NETWORKBLOCKING. Управление Блокировкой соединений
OMSINFO. Создание JSON-файла с информацией о приложении
PASSWORD. Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля
PATCHCOMPATIBILITYRESET. Удаление патча из списка несовместимых патчей
PERFANALYZER. Экспорт результатов задачи Анализатор производительности
PREVENTION. Запрет запуска объектов
REMOTEACCESS. Управление настройками удаленного подключения Консоли приложения
RESETMDRMACHINEID. Сброс идентификатора устройства
RESTORE. Восстановление файлов
ROLLBACK. Откат последнего обновления
RTP. Постоянная защита файлов
SCAN. Проверка по требованию
SCAN-IOC. Поиск IOC
SCAN-OVAL. Аудит безопасности
SCANCRITICAL. Проверка важных областей
SERVERBINDINGDISABLE. Выключение защиты подключения к Серверу администрирования
SIEM. Интеграция с SIEM-системами
SIGMA. Обнаружение аномалий с помощью Sigma-правил
START. Запуск службы приложения
STARTPOLICY. Включение политики
STOP. Остановка службы приложения
TASK. Управление задачами
TELEMETRYFILTERS. Экспорт и импорт правил фильтрации событий телеметрии
TOKEN. Управление блокировкой доступа к защищенным съемным дискам
TRACE. Трассировка работы приложения
UPDATE. Обновление баз и модулей приложения
YARA. Запуск YARA-проверки
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Предоставление расширенной диагностической информации специалистам Службы технической поддержки
Трассировка работы приложения
О составе и хранении файлов трассировки
Запись дампов памяти
Защита файлов дампов и файлов трассировки
Получение данных об ОС (Kaspersky Get System Info)
Источники информации о Kaspersky Industrial CyberSecurity for Nodes
Приложения
Расширения файлов для быстрой проверки
Учетные записи пользователей в правилах компонентов приложения

Юридическая информация
Предоставление данных
Предоставление данных в рамках Лицензионного соглашения
Предоставление данных при использовании решений Detection and Response
Kaspersky Industrial CyberSecurity Endpoint Detection and Response
Kaspersky Endpoint Detection and Response Expert (on-premises)
Интеграция с Kaspersky Industrial CyberSecurity for Networks
Интеграция с SIEM
Предоставление данных при использовании Kaspersky Security Network
Соответствие законодательству Европейского союза (GDPR)
Информация о стороннем коде
Уведомления о товарных знаках

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes – это средство комплексной защиты серверов и рабочих станций в промышленных системах управления от информационных угроз.

Приложение контролирует работу компьютеров индустриальной сети предприятия с помощью следующих компонентов, функций и технологий:

- **Контроль запуска программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.

- **Контроль устройств**. Компонент позволяет контролировать регистрацию и использование внешних устройств в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время обмена файлами с подключаемым по USB флеш-накопителем или внешним устройством другого типа.

- **Проверка целостности проектов ПЛК**. Функция предназначена для проверки целостности проектов программируемых логических контроллеров (ПЛК), используемых в индустриальной сети.

Работа компонентов контроля основана на правилах:

- Контроль запуска программ использует правила контроля запуска программ.

- Контроль устройств использует правила доступа к устройствам и правила доступа к шинам подключения.

- Функция проверки целостности проектов ПЛК использует правила проверки целостности проектов ПЛК.

Каждый тип угроз обрабатывается отдельным компонентом. Можно включать и выключать компоненты независимо друг от друга, а также настраивать параметры их работы.

Приложение проверяет и защищает компьютеры индустриальной сети с помощью следующих компонентов:

- **Постоянная защита файлов**. Компонент позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте Kaspersky Industrial CyberSecurity for Nodes, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере и на всех присоединенных дисках. Компонент Постоянная защита файлов перехватывает каждое обращение к файлу и проверяет этот файл на присутствие вирусов и других программ, представляющих угрозу.

- **Контроль Wi-Fi**. Компонент отслеживает попытки подключения защищаемого устройства к сетям Wi-Fi и блокирует или разрешает подключения к обнаруженным сетям.

- **Сетевой экран**. В зависимости от режима работы компонент отслеживает фильтрацию трафика брандмауэром Windows, только фиксирует события о сетевой активности защищаемого компьютера в журнале работы компонента или фильтрует сетевой трафик в соответствии с настройками Сетевого экрана.

- **Защита от шифрования**. Компонент позволяет обнаруживать активность вредоносного шифрования сетевых файловых ресурсов защищаемого устройства со стороны удаленных компьютеров корпоративной сети.

- **Portable Auditor**. Этот компонент исследует изолированные устройства и проводит проверки состояния безопасности.

- **Защита от атак BadUSB**. Компонент позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

- **Мониторинг файловых операций**. Kaspersky Industrial CyberSecurity for Nodes обнаруживает изменения в файлах из области мониторинга, указанной в параметрах задачи. Эти изменения указывают на нарушение безопасности на защищаемом устройстве.

- **Мониторинг доступа к реестру**. Компонент позволяет отслеживать действия, выполняемые с указанными ветвями и ключами реестра в областях мониторинга, заданных в параметрах задачи.

- **Анализ журналов**. Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.

В дополнение к постоянной защите, реализуемой компонентами приложения, рекомендуется периодически выполнять проверку компьютера на присутствие вирусов и других программ, представляющих угрозу. Это нужно делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами, например, из-за установленного низкого уровня защиты или по другим причинам.

Чтобы поддерживать Kaspersky Industrial CyberSecurity for Nodes в актуальном состоянии, требуется обновление баз и модулей приложения, используемых в работе приложения. По умолчанию программа обновляется автоматически, но при необходимости вы можете вручную обновить базы и модули приложения.

Для защиты компьютеров используются следующие задачи:

- **Полная проверка**. Kaspersky Industrial CyberSecurity for Nodes выполняет тщательную проверку операционной системы, включая системную память, объекты, загружаемые при старте операционной системы, резервное хранилище операционной системы, а также все жесткие и съемные диски.

- **Выборочная проверка**. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, выбранные пользователем.

- **Проверка важных областей**. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, загрузка которых осуществляется при запуске операционной системы, системную память и объекты, которые могут быть заражены руткитами.

- **Обновление**. Kaspersky Industrial CyberSecurity for Nodes загружает обновленные базы и модули приложения. Обновление обеспечивает актуальность защиты компьютера от вирусов и других программ, представляющих угрозу.

Удаленное управление через Kaspersky Security Center

Kaspersky Security Center позволяет удаленно запускать и останавливать Kaspersky Industrial CyberSecurity for Nodes на клиентских компьютерах, управлять задачами и настраивать параметры работы приложения.

Служебные функции приложения

Kaspersky Industrial CyberSecurity for Nodes включает ряд служебных функций. Служебные функции предусмотрены для поддержки приложения в актуальном состоянии, расширения возможностей использования приложения и оказания помощи в работе.

- **Журналы**. В процессе работы приложения для каждого компонента и задачи приложения формируется отчет. Отчет содержит список событий, произошедших во время работы Kaspersky Industrial CyberSecurity for Nodes, и всех выполненных программой операций. В случае возникновения проблем отчеты можно отправлять в "Лабораторию Касперского", чтобы специалисты Службы технической поддержки могли подробнее изучить ситуацию.

- **Хранилища**. Если в ходе проверки компьютера на вирусы и другие приложения, представляющие угрозу, программа обнаруживает зараженные или возможно зараженные файлы, она блокирует эти файлы. Kaspersky Industrial CyberSecurity for Nodes перемещает возможно зараженные файлы в карантин – специальное хранилище. Копии вылеченных и удаленных файлов Kaspersky Industrial CyberSecurity for Nodes сохраняет в резервном хранилище. Файлы, которые не были обработаны по каким-либо причинам, Kaspersky Industrial CyberSecurity for Nodes помещает в список необработанных файлов. Вы можете проверять файлы, восстанавливать файлы в папку их исходного размещения, самостоятельно помещать файлы на карантин, а также очищать хранилище данных.

- **Уведомления**. Служба уведомлений позволяет пользователю быть в курсе событий о текущем состоянии защиты компьютера и о работе Kaspersky Industrial CyberSecurity for Nodes. Уведомления могут отображаться на экране или доставляться по электронной почте.

- **Kaspersky Security Network**. Участие пользователя в Kaspersky Security Network (KSN) позволяет повысить эффективность защиты компьютера за счет оперативного получения информации о репутации файлов, веб-ресурсов и программного обеспечения, полученной от пользователей во всем мире.

- **Защита от эксплойтов**. Вы можете защищать память процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.

- **Список заблокированных сетевых сеансов**. Вы можете заблокировать сетевые сеансы, пытающиеся получить доступ к общим сетевым папкам компьютера, при обнаружении вредоносной активности с их стороны.

- **Доверенная зона**. Вы можете сформировать список исключений из области защиты или проверки, который Kaspersky Industrial CyberSecurity for Nodes будет применять по умолчанию в задачах проверки по требованию и постоянной защиты файлов и в других задачах, если вы укажете их в параметрах исключений.

- **Поддержка**. Все зарегистрированные пользователи Kaspersky Industrial CyberSecurity for Nodes получают доступ к обновлению баз данных и модулей приложения, а также к консультациям специалистов Службы технической поддержки "Лаборатории Касперского" по электронной почте по вопросам, связанным с установкой, настройкой и использованием приложения.

Что нового

Обновление 5.0

В Kaspersky Industrial CyberSecurity for Nodes 5.0 реализованы следующие новые функции и улучшения:

- Для повышения уровня контроля учетных записей на защищаемых устройствах с использованием Kaspersky Industrial CyberSecurity for Networks в приложении реализован сбор информации о пользовательских сеансах. Мониторинг пользовательских сеансов доступен в Kaspersky Industrial CyberSecurity for Networks версии 5.0 и выше. Подробнее см. в справке Kaspersky Industrial CyberSecurity for Networks.

- Добавлена возможность сбора и отправки в Kaspersky Industrial CyberSecurity for Networks данных о сетях Wi-Fi, обнаруженных защищаемым устройством с установленным приложением, и данных об устройствах, подключенных к той же сети Wi-Fi, что и защищаемое устройство. Мониторинг сетей Wi-Fi доступен в Kaspersky Industrial CyberSecurity for Networks версии 5.0 и выше. Подробнее см. в справке Kaspersky Industrial CyberSecurity for Networks.

- Для пользователей Kaspersky Industrial CyberSecurity for Networks добавлены новые действия по реагированию: *Удалить файл*, *Запустить процесс, Завершить процесс*, *Заблокировать пользователя*, *Разблокировать пользователя*, *Завершить сессию пользователя*, *Сбросить пароль пользователя*, *Блокировать соединения*. Указанные действия по реагированию доступны в Kaspersky Industrial CyberSecurity for Networks версии 5.0 и выше. Подробнее см. в справке Kaspersky Industrial CyberSecurity for Networks.

- Портативный сканер переименован в Portable Auditor. Также в компоненте реализованы следующие изменения:

  - Добавлен полноценный графический интерфейс для управления Portable Auditor.

  - Добавлена поддержка Рутокен ЭЦП 3.0 Flash для создания Portable Auditor.

  - Увеличена скорость выполнения задач Portable Auditor с настройками по умолчанию.

- Добавлена возможность настройки запуска задач по расписанию только в указанные дни недели с заданным интервалом в неделях. Расписание доступно в Kaspersky Security Center версии 16.1 и выше.

- Добавлена возможность приостановки задач проверки по требованию в выбранном временном интервале, например, для выполнения регламентных работ.

- Оптимизирована работа с дисковой подсистемой защищаемого устройства за счет сокращения количества операций ввода-вывода (I/O).

- Добавлена возможность работы приложения на устройствах с устаревшими процессорами Celeron III и VIA C3.

- Для компонента Обнаружение аномалий с помощью Sigma-правил добавлена новая предустановленная коллекция правил Аудит обмена файлами по сети и через съемные носители. Коллекция позволяет регистрировать события чтения/записи/удаления файлов в сетевых папках, а также копирования файлов на съемные носители на локальном узле.

- Добавлена поддержка контроллера TREI-5B для задачи *Проверка целостности проектов ПЛК*.

- Добавлена поддержка следующих операционных систем:
  - Windows 11 26H2;
  - Windows 11 IoT 25H2;
  - Windows Server 2025.
- Добавлена поддержка аутентификации по токену для доменных учетных записей в Консоли приложения. Теперь для доступа к функциям приложения вы можете использовать не только имя пользователя и пароль, но и токен или смарт-карту.
- Для пользователей решений Endpoint Detection and Response добавлены новые события телеметрии. Новые события повышают качество обнаружения угроз с помощью EDR-решений от "Лаборатории Касперского".
- Исправлено поведение приложения при запуске задачи *Аудит безопасности* с наборами правил, содержащими неподдерживаемые типы OVAL-проверок. Теперь при обнаружении неподдерживаемых типов OVAL-проверок приложение не будет прерывать выполнение задачи, а информация о неподдерживаемых проверках будет отображена в виде ошибок в отчете.
- Добавлена поддержка расширенного аудита политик в Kaspersky Security Center Web Console версии 15.0 и выше. Теперь вы можете просматривать ревизии политик и сохранять ревизии политик в файл. Подробнее о работе с ревизиями см. в справке Kaspersky Security Center.
- Добавлены события *Операция с устройством запрещена до запуска Kaspersky Industrial CyberSecurity for Nodes* и *Подключение устройства заблокировано до запуска Kaspersky Industrial CyberSecurity for Nodes*. Теперь если блокировка устройства произошла до запуска приложения, соответствующее событие будет сформировано и отправлено на Сервер администрирования.
- Значение по умолчанию для интервала отправки запросов на синхронизацию на сервер Kaspersky Industrial CyberSecurity for Networks изменено с 5 минут на 1 минуту.
- При разработке этой версии Kaspersky Industrial CyberSecurity for Nodes мы учли изменения, которые вошли в следующие приватные патчи: PF23040, PF23051, PF23065, PF23087, PF23100, PF23106.

Обновление 4.5

В Kaspersky Industrial CyberSecurity for Nodes 4.5 реализованы следующие новые функции и улучшения:

- Значительно обновлен интерфейс Консоли приложения и плагинов управления приложением через Kaspersky Security Center.
- Поддержка операционной системы Windows 11 24H2.
- Добавлена возможность изменять порт, который используется для подключения Консоли приложения к компьютеру с установленным приложением.

- В *Доверенной зоне* добавлена возможность для:
  - редактирования профилей исключений для промышленных программ во время установки приложения и создания политики управления приложением через Kaspersky Security Center;
  - более тонкой настройки доверенных процессов;
  - использования хранилища доверенных сертификатов.
- Расширены настройки прав пользователей и групп на управление приложением.
- Добавлен компонент *Антируткит*. По умолчанию компонент включен, если включена Постоянная защита файлов. Компонент можно выключить во время установки приложения, с помощью задачи Изменение состава компонентов Kaspersky Industrial CyberSecurity for Nodes и в свойствах инсталляционного пакета приложения.
- В настройках *Защиты от эксплойтов* добавлена возможность автоматического определения защищаемых процессов.
- Добавлен компонент *Откат вредоносных действий*.
- Компонент *Защита от шифрования* контролирует как сетевые, так и локальные папки.
- Переработан компонент *Контроль запуска программ*:
  - Значительно изменена структура настроек компонента.
  - Для задания условий срабатывания правил контроля запуска программ и исключений теперь можно использовать тип носителя, KL-категории, группы KSN.
- Переработан компонент *Контроль устройств*:
  - По умолчанию *Контроль устройств* настроен на разрешение подключения всех устройств.
  - *Контроль Wi-Fi* больше не является отдельным компонентом, а являются частью Контроля устройств.
  - Добавлена возможность контролировать подключаемые устройства в зависимости от шины подключения.
  - Добавлена миграция настроек доступа к съемным дискам при обновлении с предыдущих версий приложения до версии 4.5.
- Компонент *Управление сетевым экраном* преобразован в *Сетевой экран*, который теперь не только взаимодействует с брандмауэром Windows, но и выполняет функции сетевого экрана.
- Функциональность компонентов *Мониторинг файловых операций* и *Мониторинг доступа к реестру* объединена в новый компонент – *Контроль целостности системы*. Это улучшение позволяет более эффективно отслеживать изменения в файловой системе и реестре Windows, повышая уровень защиты от несанкционированного изменения данных.
- Функциональность Kaspersky Endpoint Agent теперь интегрирована в приложение в виде встроенного агента Endpoint Agent (Detection and Response).
- Расширена настройка событий для отправки в SIEM. Теперь Kaspersky Industrial CyberSecurity for Nodes поддерживает отправку событий Windows Event Log.

- Приложение не поддерживает настройку расписания работы отдельных компонентов. Если компоненты включены, то они работают постоянно, пока работает приложение.
- Добавлена поддержка Kaspersky Security Center Windows 15.1.
- Добавлены групповые задачи:
  - Для выполнения функциональности Kaspersky Endpoint Agent: Аудит безопасности, Запуск процесса, Завершение процесса, Поиск IOC, Получение файла, Помещение файла на карантин, Удаление файла.
  - Другие задачи:
    - Защита подключения к Серверу администрирования;
    - Изменение состава компонентов Kaspersky Industrial CyberSecurity for Nodes;
    - Мониторинг целостности системы на основе эталона вместо Мониторинг целостности файлов на основе эталона;
    - Обновление вместо Копирование обновлений, Обновление баз программы и Обновление модулей программы;
    - Откат обновления вместо Откат обновления баз программы;
    - Удаление ключа.
- В сообщениях о сетевом обмене (события network communication) уровня L2, передаваемых в Kaspersky Industrial CyberSecurity for Networks, теперь передается IPv4-адрес сетевого интерфейса, на котором проходит трафик (поле adapter.address).
- Расширены возможности интеграции с решением Kaspersky Industrial CyberSecurity for Networks. Начиная с версии Kaspersky Industrial CyberSecurity for Nodes 4.5 поддерживаются следующие типы конфигураций:
  - ARP-таблица;
  - таблица маршрутизации;
  - политика паролей;
  - политика аудита;
  - политика расширенного аудита.
- В настройки интеграции с Kaspersky Industrial CyberSecurity for Networks добавлен неразборчивый режим для приложения и сетевых интерфейсов узла, позволяющий отправлять расширенную телеметрию в Kaspersky Industrial CyberSecurity for Networks.
- На сервер Kaspersky Industrial CyberSecurity for Networks теперь может передаваться информация о файловых операциях (чтение, запись, удаление) в общих папках и на подключаемых устройствах на локальном узле. Для получения данных о файловых операциях необходима коллекция соответствующих Sigma-правил. На основании получаемой информации Kaspersky Industrial CyberSecurity for Networks может определить случаи копирования файлов между сетевыми папками компьютеров с установленным Kaspersky Industrial CyberSecurity for Nodes или копирования файлов с сетевых папок на устройства, подключаемые к компьютерам под управлением Kaspersky Industrial CyberSecurity for Nodes.

- В Web Console в свойствах хоста с установленным приложением в разделе Detection and Response теперь можно посмотреть историю реагирования Kaspersky Industrial CyberSecurity for Nodes на угрозы совместно с историей реагирования других решений, которыми управляется хост.

- Для пользователей решений Endpoint Detection and Response (EDR) от "Лаборатории Касперского" появились следующие возможности и улучшения:

  - Наполнение деталей алерта новыми данными. Теперь детали алерта содержат больше информации об угрозе, включая действия приложения при реагировании на угрозы EDR.

  - Добавлена возможность управлять Сетевой изоляцией компьютера в деталях алерта. Также в деталях алерта вы можете задавать срок Сетевой изоляции компьютера и добавлять исключения.

  - Улучшено взаимодействие с IOC-файлами. Теперь вы можете просматривать содержимое IOC-файлов в интерфейсе Web Console и редактировать содержание. После загрузки IOC-файла приложение показывает отчет о применении IOC-терминов.

  - Улучшено реагирование на обнаруженные IOC. Теперь вы можете помещать файлы на карантин, обнаруженные при выполнении задачи *Поиск IOC*, прямо в результатах обнаружения IOC в свойствах задачи. Также в свойствах задачи вы можете изолировать компьютеры от сети.

  - Добавлена возможность создавать IOC-файлы прямо в свойствах задачи *Поиск IOC* на основе сформированных в TXT-файле списков хешей файлов, IP-адресов или DNS-имен.

  - Расширена область поиска для задачи *Поиск IOC*. Теперь вы можете формировать область поиска IOC в реестре (**Реестр Windows - RegistryItem**). В предыдущих версиях приложения вы могли использовать только предустановленную область поиска IOC в реестре.

- В компонент *Защита от сетевых угроз* добавлена возможность контролировать сетевой трафик на наличие сканирования портов и интенсивных сетевых запросов.

- В Консоли приложения в разделе **Серверы сбора телеметрии** теперь доступна настройка следующих интеграций:

  - Интеграция с Kaspersky Endpoint Detection and Response Expert (on-premise);

  - Интеграция с KICS for Networks;

  - Интеграция с SIEM.

- В рамках интеграции с KICS for Networks добавлена возможность отправлять телеметрию на сервер MQTT-брокера, встроенный в программный диод данных.

- Для задачи *Проверка целостности проектов ПЛК* добавлена поддержка ПЛК серии Allen-Bradley ControlLogix.

- Добавлена новая функция – *Анализатор производительности*. Анализатор производительности – это задача, которая собирает и анализирует информацию об обращениях к файлам и приложениям на устройстве. Вы можете использовать полученную информацию для формирования доверенной зоны, чтобы минимизировать влияние работы приложения на промышленное ПО.

- Для компонента Обнаружение аномалий с помощью Sigma-правил добавлены новые коллекции:

  - *Коллекция правил мониторинга пользовательской активности с использованием журналов Windows*. Коллекция позволяет регистрировать события добавления новых пользователей, повышение привилегий пользователей, входа пользователей в систему и другие.

  - *Коллекция правил для выявления подозрительной активности при эксплуатации ПО Siemens SIMATIC PCS7, Siemens STEP7, Siemens TIA Portal, Siemens WinCC.*

  - *Коллекция правил для выявления подозрительной активности при эксплуатации систем Yokogawa CENTUM VP, ProSafe-RS*.

- Добавлена проверка настройки компонентов контроля перед сохранением параметров. Проверка добавлена для компонентов Контроль запуска программ, Контроль устройств, Контроль целостности системы. Теперь приложение показывает предупреждение пользователю, если текущие настройки компонента контроля могут привести к повышенной нагрузке на компьютер или сбоям в работе системы. Например, если для Контроль запуска программ вы выбрали режим блокировки всех приложений, кроме разрешенных, и не добавили ни одного разрешающего правила, то приложение покажет предупреждение, так как это может привести к сбоям в работе системы.

- Добавлены новые компоненты:

  - *Managed Detection and Response для ICS*. Компонент обеспечивает взаимодействие с решением Kaspersky Managed Detection and Response для Industrial Control Sestems. *Kaspersky Managed Detection and Response (MDR)* – решение, которое автоматически обнаруживает и анализирует инциденты безопасности в промышленной инфраструктуре. Для этого MDR использует данные телеметрии, полученные от конечных точек, и машинное обучение. Данные об инцидентах MDR передает экспертам "Лаборатории Касперского". Далее эксперты могут самостоятельно обработать инцидент и, например, добавить новую запись в антивирусные базы.

  - *Защита от атак BadUSB*. Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру. Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, приложение предлагает пользователю ввести с этой клавиатуры код для авторизации клавиатуры.

  - *Полнодисковое шифрование BitLocker*. BitLocker – встроенная в операционную систему Windows технология шифрования. Kaspersky Industrial CyberSecurity for Nodes позволяет контролировать и управлять Bitlocker с помощью Kaspersky Security Center.

- Поддержка протокола *OPC UA* для передачи данных в SCADA-систему через Kaspersky Security Gateway. Теперь кроме протоколов IEC 60870-5-104 и OPC DA приложение поддерживает протокол OPC UA, который обеспечивает кроссплатформенную совместимость.

- Поддержка Windows XP и Windows XP SP1 для работы Портативного сканера. Портативный сканер может выполнять проверку изолированных устройств на присутствие вирусов и других программ, представляющих угрозу.

- Для задачи *Получение данных о проектах ПЛК* добавлена поддержка аутентификации на контроллерах Siemens SIMATIC S7-1200/1500. Теперь вы можете ввести пароль для подключения к этим моделям ПЛК в свойствах задачи.

Исправленные ошибки

В таблице ниже перечислены все ошибки, обнаруженные в предыдущих версиях Kaspersky Industrial CyberSecurity for Nodes и исправленные в текущей версии.

Список ошибок, исправленных в версии 5.0

Идентификатор	Описание ошибки
9527176	В Web Console не удается импортировать в политику правила Сетевого экрана, ранее экспортированные из Консоли приложения.
9986614	В Web Console и Консоли администрирования Kaspersky Security Center не удается импортировать список доверенных устройств из TXT-файла с выборкой событий Kaspersky Security Center о заблокированных устройствах, экспортированного из Web Console.
10094028	При создании Portable Auditor ошибочно отображается образец конфигурации Audit configuration sample profile в списке конфигураций безопасности и соответствия стандартам для операционных систем.
10700703	В интерфейсе компонентов Контроль целостности системы, Доверенная зона, Контроль запуска программ, Контроль устройств неочевидно, как выбрать элементы списка для выполнения команды **Экспортировать выбранное**. Расширено описание в справке приложения.
10720231	Не отображается счетчик доверенных устройств в разделе **Контроль устройств** в политике Консоли администрирования Kaspersky Security Center.
10729552	Не формируются события об операциях с файлами на съемных дисках, хотя запись таких событий включена.
10752491	В Web Console не удается импортировать список доверенных устройств из TXT-файла с выборкой событий Kaspersky Security Center о заблокированных устройствах, экспортированного из Консоли администрирования.
10753980	В результате выполнения задачи *Поиск вредоносного ПО* Portable Auditor ошибочно создает файл формата KLQ вместо защищенного паролем ZIP-архива.

Комплект поставки

В комплект поставки входит программа-приветствие, из которой вы можете выполнить следующие действия:

- запустить мастер установки Kaspersky Industrial CyberSecurity for Nodes;
- запустить мастер установки Консоли Kaspersky Industrial CyberSecurity for Nodes;
- запустить утилиту Kaspersky Virus Removal Tool;
- запустить установку Kaspersky Security Gateway;
- прочитать информацию о текущем выпуске Kaspersky Industrial CyberSecurity for Nodes;
- открыть справку Kaspersky Industrial CyberSecurity for Nodes 5.0;
- открыть справку Kaspersky Industrial CyberSecurity Endpoint Detection and Response;
- перейти на страницу Kaspersky Industrial CyberSecurity for Nodes на веб-сайте "Лаборатории Касперского";

- перейти на веб-сайт "Лаборатории Касперского";
- перейти на веб-сайт Службы технической поддержки.

Файлы комплекта поставки располагаются в разных папках в зависимости от их предназначения (см. таблицу ниже).

Файлы комплекта поставки Kaspersky Industrial CyberSecurity for Nodes

Файл	Назначение
autorun.inf	Файл автозапуска мастера установки Kaspersky Industrial CyberSecurity for Nodes при установке приложения с переносных носителей.
setupui.exe	Файл для запуска программы-приветствия.
kics_win.kud	Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки приложения через Kaspersky Security Center.
\client\kicstools.msi	Пакет установки для установщика Windows; устанавливает консоль Kaspersky Industrial CyberSecurity for Nodes на защищаемых устройствах.
\client\setup_kicstool.exe	Файл запуска мастера установки для Консоли Kaspersky Industrial CyberSecurity for Nodes. Запускается файл инсталляционного пакета kicstools.msi с указанными в мастере параметрами установки.
\client\license.txt	Файл с текстом Лицензионного соглашения и Политики конфиденциальности для Консоли управления Kaspersky Industrial CyberSecurity for Nodes.
\exec\bases.cab	Архив антивирусных баз, актуальных на момент выпуска приложения.
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	Файлы для удаления несовместимого программного обеспечения.
\exec\incompatible.txt	"Лаборатория Касперского" не гарантирует совместимость Kaspersky Industrial CyberSecurity for Nodes с приложениями из списка, которые перечислены в файле.
\exec\installer.ini	Файл, содержащий внутренние параметры дистрибутива.
\exec\kics.cab	Файлы для работы графического интерфейса приложения.
\exec\kics_win.kud	Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки приложения через Kaspersky Security Center.
\exec\kics_win.msi	Пакет установки службы Windows Installer; устанавливает Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве.
\exec\klcfginst.msi	Программа установки Плагина управления Kaspersky Industrial CyberSecurity for Nodes, доступного в Kaspersky Security Center. Установите Плагин управления на каждом защищаемом устройстве, на котором установлена Консоль администрирования Kaspersky Security Center, если вы планируете управлять Kaspersky Industrial CyberSecurity for Nodes через нее.
\exec\ksn_ru.txt	Файл с текстом положения о KSN.
\exec\license.txt	Файл с текстом Лицензионного соглашения и Политики конфиденциальности для Kaspersky Industrial CyberSecurity for Nodes.
\exec\package.kcat	Файл с подписями файлов комплекта поставки.
\exec\setup_kics.exe	Файл запуска мастера установки Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве; запускает файл инсталляционного пакета kics_win.msi с указанными в мастере параметрами установки.
\gateway\security_gateway.msi	Пакет установки службы Windows Installer; устанавливает Kaspersky Security Gateway.
\gateway\opc_redist.msi	Пакет установки службы Windows Installer; устанавливает OPC Core Components Redistributables.
\gateway\license.txt	Файл с текстом Лицензионного соглашения и Политики конфиденциальности для Kaspersky Security Gateway.
\kvrt\KVRT.exe	Установщик для Kaspersky Virus Removal Tool.
\setup\images	Папка с файлами для запуска приветственного экрана.

Файл	Назначение
\setup\setup.hta	Файл запуска программы-приветствия.
\setup\SETUP_STRINGS.JS	Файл со строковыми ресурсами приложения.

Вы можете запускать файлы, входящие в комплект поставки, с установочного компакт-диска. Если вы предварительно скопировали файлы на локальный диск, убедитесь, что сохранена структура файлов комплекта поставки.

Аппаратные и программные требования

Программные требования к защищаемым устройствам

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Для установки и корректной работы приложения на защищаемом устройстве под управлением операционной системы Windows XP требуется наличие установщика Windows версии 3.1.

Для установки и работы Kaspersky Industrial CyberSecurity for Nodes на защищаемых устройствах со встроенными операционными системами необходим компонент Диспетчер фильтров (Filter Manager).

Для корректной работы Kaspersky Industrial CyberSecurity for Nodes в Windows требуется поддержка SHA-2. Подробная информация приведена в базе знаний Службы технической поддержки.

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes на устройство под управлением одной из следующих 32- или 64-разрядных операционных систем Microsoft Windows:

Настольные операционные системы:

- Windows XP Professional SP2 32-разрядная/64-разрядная.
- Windows XP Professional SP3 32-разрядная.
- Windows Vista SP2 32-разрядная/64-разрядная.
- Windows 7 SP1 Home/Pro/Enterprise/Ultimate 32-разрядная/64-разрядная.
- Windows 8 Pro/Enterprise 32-разрядная/64-разрядная.
- Windows 8.1 Pro/Enterprise 32-разрядная/64-разрядная.
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.

- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 25H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 26H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.

Серверные операционные системы:

- Windows Server 2003 SP1 Standard/Enterprise 32-разрядная/64-разрядная.
- Windows Server 2008 R2 SP1 Foundation/Standard/Enterprise 64-разрядная.
- Windows Server 2008 R2 SP2 Foundation/Standard/Enterprise 64-разрядная.
- Windows Server 2008 SP2 Standard/Enterprise 64-разрядная.
- Windows Small Business Server 2011 Essentials/Standard 64-разрядная.
- Windows MultiPoint Server 2011 64-разрядная.
- Windows Server 2012 Foundation/Essentials/Standard 64-разрядная.
- Windows Server 2012 R2 Foundation/Essentials/Standard 64-разрядная.

- Windows Server 2016 Essentials/Standard 64-разрядная.
- Windows Server 2019 RS5 Essentials/Standard 64-разрядная.
- Windows Server 2022 21H2 64-разрядная.
- Windows Server 2022 версия 20348.350 64-разрядная.
- Windows Server 2025 версия 26100.1742 64-разрядная.

Встраиваемые системы:

- Windows XP Embedded Service Pack 3 32-разрядная.
- Windows Embedded POSReady 7 32-разрядная/64-разрядная.
- Windows Embedded Standard 7 Service Pack 1 32-разрядная/64-разрядная.
- Windows Embedded 8 Standard 32-разрядная/64-разрядная.
- Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1507 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1607 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1803 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1809 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1903 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 2004 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 20H2 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 21H1 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 21H2 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 22H2 32-разрядная/64-разрядная.
- Windows 11 IoT Enterprise Version 21H2 64-разрядная.
- Windows 11 IoT Enterprise Version 22H2 64-разрядная.
- Windows 11 IoT Enterprise Version 23H2 64-разрядная.
- Windows 11 IoT Enterprise Version 24H2 64-разрядная.
- Windows 11 IoT Enterprise Version 25H2 64-разрядная.

Аппаратные требования к защищаемым устройствам

Аппаратные требования к защищаемым устройствам

Тип ОС	Наименование ОС	Минимальные требования	Рекомендованные требования
Для рабочих станций	Windows XP x86	• Процессор: 1 ГГц одноядерный, не ниже Celeron III или VIA C3. • Оперативная память: 256 МБ. • Объем свободного места на диске: 2 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
	Windows XP x64 Windows 7/8 x86	• Процессор: 1.4 ГГц одноядерный, не ниже Pentium IV (x64). • Оперативная память: 256 МБ. • Объем свободного места на диске: 2 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
	Windows 7/8/10/11 x64	• Процессор: 1.4 ГГц одноядерный, не ниже Pentium IV (x64). • Оперативная память: 256 МБ. • Объем свободного места на диске: 2 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
Для серверов	Windows Server 2003 x86/x64 Windows Server 2008 x86	• Процессор: 1.4 ГГц одноядерный, не ниже Pentium IV (x64). • Оперативная память: 256 МБ. • Объем свободного места на диске: 4 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
	Windows Server 2016 x64 Windows Server 2012 x64 Windows Server 2008 x64 Windows Server 2019 x64 Windows Server 2022 x64	• Процессор: 1.4 ГГц одноядерный. • Оперативная память: 256 МБ. • Объем свободного места на диске: 4 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
Встраиваемые	Windows Embedded XP	• Процессор: 1.4 ГГц одноядерный, не ниже Pentium IV (x64). • Оперативная память: 256 МБ. • Объем свободного места на диске: 2 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.
	Windows 7/8/10 Embedded	• Процессор: 1.4 ГГц одноядерный, не ниже Pentium IV (x64). • Оперативная память: 256 МБ. • Объем свободного места на диске: 2 ГБ.	• Процессор: 2.4 ГГц четырехъядерный. • Оперативная память: 2 ГБ. • Объем свободного места на диске: 4 ГБ.

Поддерживаемые индустриальные системы

Kaspersky Industrial CyberSecurity for Nodes 5.0 защищает следующие программируемые логические контроллеры:

- Siemens™ SIMATIC™ S7-300;
- Siemens SIMATIC S7-400;
- Siemens SIMATIC S7-400H;
- Siemens SIMATIC S7-1200;
- Siemens SIMATIC S7-1500;

- Siemens SIPROTEC 4;
- Schneider Electric Modicon M340;
- Schneider Electric Modicon M580;
- устройства на базе CODESYS V3;
- OWEN PLC210;
- Fastwel CPM723-01;
- Prosoft Systems Regul R500;
- Emerson DeltaV;
- Rockwell Automation Allen-Bradley ControlLogix;
- TREI-5B.

Аппаратные и программные требования для Kaspersky Security Gateway

Общие аппаратные и программные требования:

- 1 ГБ свободного места на диске.
- Если в качестве поставщика данных выбран сервис klakaut, необходимо установить Сервер администрирования Kaspersky Security Center.

Настольные операционные системы:

- Windows 7 SP1 Pro/Enterprise/Ultimate 32-разрядная/64-разрядная.
- Windows 8 Pro/Enterprise 32-разрядная/64-разрядная.
- Windows 8.1 Pro/Enterprise 32-разрядная/64-разрядная.
- Windows 10 LTSC 2015 версия 1507 32-разрядная/64-разрядная.
- Windows 10 LTSC 2016 версия 1607 32-разрядная/64-разрядная.
- Windows 10 RS4 версия 1803 Home/Pro/Education/Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS5 версия 1809 Home/Pro/Education/Enterprise 32-разрядная/64-разрядная.
- Windows 10 LTSC 2019 версия 1809 32-разрядная/64-разрядная.
- Windows 10 19H1 версия 1903 Home/Pro/Education/Enterprise 32-разрядная/64-разрядная.
- Windows 10 20H1 версия 2004 Home/Pro/Education/Enterprise 32-разрядная/64-разрядная.
- Windows 10 20H2 версия 2009 Home/Pro/Education/Enterprise 32-разрядная/64-разрядная.
- Windows 10 21H1 Home/Pro/Education/Enterprise 32-разрядная/64-разрядная.

- Windows 10 LTSC 2021 версия 21H2 32-разрядная/64-разрядная.
- Windows 10 22H2 Home/Pro/Education/Enterprise 32-разрядная/64-разрядная.
- Windows 11 23H2 Home/Pro/Education/Enterprise 64-разрядная.
- Windows 11 22H2 Home/Pro/Education/Enterprise 64-разрядная.
- Windows 11 21H2 Home/Pro/Education/Enterprise 64-разрядная.
- Windows 11 22H2 Home/Pro/Education/Enterprise 64-разрядная.
- Windows 11 23H2 Home/Pro/Education/Enterprise 64-разрядная.
- Windows 11 24H2 Home/Pro/Education/Enterprise 64-разрядная.
- Windows 11 25H2 Home/Pro/Education/Enterprise 64-разрядная.
- Windows 11 26H2 Home/Pro/Education/Enterprise 64-разрядная.

Серверные операционные системы:

- Windows Server 2008 R2 Standard/Enterprise 32-разрядная/64-разрядная.
- Windows Server 2008 SP1 R2 Standard/Enterprise 32-разрядная/64-разрядная.
- Windows Server 2012 Essentials/Standard/Foundation/Datacenter 64-разрядная.
- Windows Server 2012 R2 Essentials/Standard/Foundation/Datacenter 64-разрядная.
- Windows Server 2016 Essentials/Standard/Datacenter 64-разрядная.
- Windows Server 2019 Essentials/Standard/Datacenter 64-разрядная.
- Windows Server 2022 21H2 64-разрядная.
- Windows Server 2022 версия 20348.350 64-разрядная.
- Windows Server 2025 версия 26100.1742 64-разрядная.

Поддерживаемые версии Kaspersky Security Center

Приложение Kaspersky Industrial CyberSecurity for Nodes совместимо с Kaspersky Security Center следующих версий:

- Kaspersky Security Center Linux версий 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3, 17.0. Поддерживается управление Kaspersky Industrial CyberSecurity for Nodes через Web Console.
- Kaspersky Security Center Windows версии 15.1. Поддерживается управление Kaspersky Industrial CyberSecurity for Nodes через Консоль администрирования Kaspersky Security Center и через Web Console.

- Kaspersky Security Center Windows 14.0. Поддерживается управление Kaspersky Industrial CyberSecurity for Nodes, установленном на устройствах с Microsoft Windows XP SP3, через Консоль администрирования Kaspersky Security Center и через Web Console.

- Kaspersky Security Center Windows 10.5. Поддерживается управление Kaspersky Industrial CyberSecurity for Nodes, установленном на устройства с Microsoft Windows XP SP2, через Консоль администрирования Kaspersky Security Center и через Web Console.

Для управления Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center требуется Агент администрирования Kaspersky Security Center.

Агент администрирования Kaspersky Security Center не входит в комплект поставки Kaspersky Industrial CyberSecurity for Nodes. Вы можете скачать его на странице загрузки приложений в разделе **Kaspersky Security Center**.

Kaspersky Virus Removal Tool

Утилита Kaspersky Virus Removal Tool предназначена для проверки и лечения зараженных компьютеров под управлением операционных систем семейства Microsoft Windows. Kaspersky Virus Removal Tool позволяет обнаружить вирусы, троянские программы и другие программы, представляющие угрозу на защищаемом устройстве, и выбрать действия для обнаруженных зараженных объектов.

Kaspersky Virus Removal Tool не требует установки. Вы можете запустить программу следующими способами:

- из папки kvrt\ запустить исполняемый файл kvrt.exe, включенный в комплект поставки Kaspersky Industrial CyberSecurity for Nodes 5.0;

- перейти по ссылке **Запустите Kaspersky Virus Removal Tool** в окне программы-приветствия.

Утилиту невозможно запустить через локальную Консоль или Плагин управления Kaspersky Industrial CyberSecurity for Nodes 5.0.

После лечения обнаруженного заражения требуется перезагрузка компьютера. Рекомендуем запускать Kaspersky Virus Removal Tool только во время технологических окон в работе промышленной сети.

Kaspersky Virus Removal Tool не является частью решения Kaspersky Industrial CyberSecurity for Nodes и не зависит от компонентов программы.

Обновление антивирусных баз выполняется независимо от обновлений Kaspersky Industrial CyberSecurity for Nodes 5.0. При запуске Kaspersky Virus Removal Tool программа самостоятельно оповещает о необходимости обновления. Для обновления утилиты требуется подключение к интернету.

Работа утилиты Kaspersky Virus Removal Tool регулируется отдельным Лицензионным соглашением, с которым вы можете ознакомиться на сайте технической поддержки.

Также на сайте технической поддержки представлена информация о системных требованиях к компьютеру, на котором запускается утилита, и подробные инструкции о работе с Kaspersky Virus Removal Tool.

Функциональные требования и ограничения

В этом разделе приведено описание дополнительных функциональных требований и существующих ограничений компонентов Kaspersky Industrial CyberSecurity for Nodes.

Установка и удаление приложения

- Для корректной работы Kaspersky Industrial CyberSecurity for Nodes в Windows требуется поддержка SHA-2.

- При установке приложения на экране может появиться предупреждение, если указанный путь к папке установки Kaspersky Industrial CyberSecurity for Nodes содержит более 150 символов. Это предупреждение не влияет на процесс установки: вы можете установить и запустить Kaspersky Industrial CyberSecurity for Nodes.

- Если вы хотите установить компонент поддержки протокола SNMP, перезапустите службу SNMP, если она запущена.

- Если вы хотите установить и запустить Kaspersky Industrial CyberSecurity for Nodes на устройстве со встроенной операционной системой, установите компонент Диспетчер фильтров.

- Установка Средств администрирования невозможна средствами групповых политик Microsoft Active Directory®.

- Если исключить узел Антивирусная защита из списка устанавливаемых компонентов приложения, он исчезнет из списка доступных компонентов после завершения установки. Для установки компонентов узла Антивирусная защита запустите мастер установки из инсталляционного пакета, поскольку инсталляционный пакет содержит полный список компонентов.

- Если установлена Консоль администрирования Kaspersky Industrial CyberSecurity for Nodes, мастер установки может предложить перезагрузить компьютер. В этом случае перезагрузка не обязательна. Достаточно завершить сеанс пользователя, установившего Консоль администрирования, и повторно выполнить вход в систему.

- При установке приложения на устройства под управлением операционных систем Windows XP и Windows Vista может потребоваться установка сертификата DigiCert Assured ID Root CA для обеспечения проверки подписи драйверов. При необходимости данный сертификат будет установлен в хранилище доверенных корневых сертификатов ОС автоматически из инсталляционного пакета приложения.

- При установке приложения на устройства под управлением операционных систем Windows XP и Windows Vista нужно проверить наличие корневого сертификата DigiCert High Assurance EV Root CA.

  Если данный корневой сертификат не установлен, приложение может работать некорректно. Рекомендуется установить сертификат как можно скорее.

- Установка приложения завершается с ошибкой, если путь к папке установки приложения совпадает с путем к хотя бы одной из следующих папок: баз приложения, резервного хранилища, для восстановления объектов из карантина, журналов, хранилища для временных файлов.

- Если для управления Kaspersky Industrial CyberSecurity for Nodes вы используете решение Kaspersky Security Center Cloud Console, запрещено обновлять приложение локально. При локальном обновлении приложения невозможно принять условия Соглашения об обработке данных для Kaspersky Security Center Cloud Console.

Контроль целостности системы

По умолчанию компонент Контроль целостности системы не проверяет изменения в системных папках и в служебных файлах файловой системы, чтобы информация о стандартных изменениях файлов, постоянно осуществляемых операционной системой, не попадала в отчет выполнения задачи. Нельзя добавить эти папки в область мониторинга.

Следующие папки и файлы исключены из области мониторинга:

- Служебные файлы NTFS с идентификатором файла от 0 до 33
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\

- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\Windows\TaskScheduler\

Приложение исключает папки верхнего уровня.

Компонент не осуществляет мониторинг изменений в файлах, которые происходят в обход файловой системы ReFS/NTFS (изменения, сделанные через BIOS, LiveCD и т.д.).

Сетевой экран

- Требуется указать несколько адресов. В противном случае невозможна работа с IPv6.
- Текущие правила Сетевого экрана поддерживают основные сценарии взаимодействия между защищаемыми устройствами и Сервером администрирования. Для использования функций Kaspersky Security Center в полном объеме необходимо настроить правила для портов. Информация о номерах портов, протоколах и их функциях приведена в Базе знаний Kaspersky Security Center.
- После установки приложения и настройки правил Сетевого экрана приложение контролирует изменение правил и групп правил Брандмауэра Windows, когда компонент Сетевой экраном запущен. Чтобы обновить статус и добавить необходимые правила Брандмауэра Windows, перезапустите компонент Сетевой экран.
- При запуске Сетевого экрана запрещающие правила и правила, контролирующие исходящий трафик, автоматически удаляются из параметров Брандмауэра Windows.
- Не допускается использование символов `*` и `?` в имени правила Сетевого экрана для приложений и пути к приложению.
- Если выбран режим Сетевого экрана *Отслеживать статус работы брандмауэра Windows*, в операционной системе Windows в настройках Брандмауэра (**Параметры** → **Обновление и безопасность** → **Безопасность Windows** → **Брандмауэр и защита сети**) отображается, что Сетевой экран Kaspersky Industrial CyberSecurity for Nodes выключен. При нажатии на кнопку включения Сетевого экрана его режим работы изменяется на *Блокировать*.
- На компьютерах под управлением Windows 7 и Windows Server 2008 R2 правила Сетевого экрана, настроенные для службы TermService на основе имени сервиса, не ограничивают доступ через RDP.
- При работе Сетевого экрана в режиме **Блокировать** приложение препятствует получению IP-адреса от DHCP-сервера. Для получения компьютером IP-адреса вам необходимо настроить разрешающие правила Сетевого экрана для системного процесса svchost.exe.

Ограничения в устаревших версиях Windows

- В Windows XP версии SP2 невозможно заблокировать удаленные устройства и настроить параметры списка заблокированных сетевых сеансов. В этой версии Windows параметр **Блокировать доступ к общим сетевым ресурсам для сетевых сеансов, проявляющих вредоносную активность** неактивен.

- Установка Kaspersky Industrial CyberSecurity for Nodes:

  - На компьютерах под управлением Windows XP SP2 Professional (32-разрядная/64-разрядная), Windows Server 2003 и Windows Server 2003 R2 при установке приложения через Kaspersky Security Center необходимо в папку инсталляционного пакета приложения поместить исполняемый файл setup.exe из инсталляционного пакета Агента администрирования версии 10.5.1781 и установить приватный патч для Kaspersky Security Center.

  - На компьютерах под управлением Windows XP SP3 Professional (32-разрядная) и Windows XP Embedded SP3 (32-разрядная) при установке приложения через Kaspersky Security Center необходимо в папку инсталляционного пакета приложения поместить исполняемый файл setup.exe из инсталляционного пакета Агента администрирования версии 14.0.0.20023 и установить приватный патч для Kaspersky Security Center.

    Обратитесь в Службу технической поддержки для получения необходимых файлов и инструкций.

- Для управления программой Kaspersky Industrial CyberSecurity for Nodes с помощью Kaspersky Security Center:

  - на компьютерах под управлением Windows XP SP2 Professional (32-разрядная/64-разрядная), Windows Server 2003 и Windows Server 2003 R2 необходимо использовать Агент администрирования Kaspersky Security Center версии 10.5.1781;

  - на компьютерах под управлением Windows XP SP3 Professional (32-разрядная) и Windows XP Embedded SP3 (32-разрядная) необходимо использовать Агент администрирования Kaspersky Security Center версии 14.0.0.20023.

- Отправка телеметрии на диод данных по протоколу MQTT недоступна на компьютерах под управлением Windows XP.

- Для корректной работы задачи *Анализатор производительности* компьютер, на котором запускается задача, должен быть под управлением ОС Windows Vista или выше.

Интеграция с Kaspersky Security Center

- При получении пакетов обновлений Сервер администрирования проверяет обновления баз перед отправкой обновлений на защищаемые сетевые устройства. Сервер администрирования Kaspersky Security Center не проверяет обновления модулей приложения.

- Убедитесь, что установлены необходимые флажки в окне параметров взаимодействия с Сервером администрирования Kaspersky Security Center, при использовании компонентов, передающих динамические данные в Kaspersky Security Center с помощью сетевых списков (карантин, резервное хранилище).

- Агент администрирования версии 10.5 не передает информацию об установленных компонентах приложения Серверу администрирования Kaspersky Security Center. В связи с этим в Консоли администрирования Kaspersky Security Center и Web Console в параметрах устройства с установленным Агентом администрирования версии 10.5 не отображаются установленные компоненты Kaspersky Industrial CyberSecurity for Nodes и их параметры.

- Если на устройстве установлен Агент администрирования Kaspersky Security Center версии 10.5, то с помощью Web Console невозможно скачать файлы, помещенные в резервное хранилище.

- Если Kaspersky Industrial CyberSecurity for Nodes установлено с включенным режимом пониженного потребления ресурсов Агентом администрирования Kaspersky Security Center (значение по умолчанию, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`) и далее установлен Агент администрирования, то Kaspersky Industrial CyberSecurity for Nodes не создает исключение для Агента администрирования в Брандмауэре Windows и Брандмауэр Windows блокирует работу Агента администрирования.

- Если Kaspersky Industrial CyberSecurity for Nodes установлено с включенным режимом пониженного потребления ресурсов Агентом администрирования Kaspersky Security Center (значение по умолчанию, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`), то изменения сетевых списков отображаются в Консоли администрирования Kaspersky Security Center с задержкой около десяти минут.

- При поиске управляемых устройств в Консоли администрирования Kaspersky Security Center на вкладке **Компоненты приложения** могут одновременно отображаться несколько вариантов названия одного и того же компонента приложения, в том числе названия, соответствующие предыдущим версиям Kaspersky Industrial CyberSecurity for Nodes. Также названия некоторых компонентов могут дублироваться.

  Для поиска по компоненту вам достаточно выбрать один из отображаемых вариантов. Подробнее о поиске устройств см. в справке Kaspersky Security Center.

Прочие ограничения

Проверка по требованию и Постоянная защита файлов

- Проверка подключенных устройств, работающих по протоколу MTP, не поддерживается.

- Проверка архивов невозможна без проверки SFX-архивов: если проверка архивов включена в параметрах защиты Kaspersky Industrial CyberSecurity for Nodes, приложение автоматически проверяет объекты как в архивах, так и в SFX-архивах. Возможна проверка SFX-архивов без проверки архивов.

- Если одновременно установлен флажок **Углубленный анализ запускаемых процессов (запуск процессов блокируется до окончания анализа)** и включено **Использование KSN**, все запущенные процессы, получившие в качестве аргумента веб-адрес, будут заблокированы, даже если был выбран режим "Информировать". Чтобы избежать блокировки процесса, выберите один из вариантов:

  - Отключите **Использование KSN**.

  - Снимите флажок **Углубленный анализ запускаемых процессов (запуск процессов блокируется до окончания анализа)**.

  Рекомендуемый вариант: снимите флажок **Углубленный анализ запускаемых процессов (запуск процессов блокируется до окончания анализа)**.

Лицензирование

- В мастере установки не поддерживается активация приложения с помощью ключа, если ключ был создан с помощью команды SUBST или если указан сетевой путь к файлу ключа.
- Если вы планируете использовать прокси-сервер Kaspersky Security Center для активации продукта на клиентском устройстве, отключите VDI-оптимизацию на этом устройстве при установке Агента администрирования Kaspersky Security Center.

Обновление

- В процессе установки и удаления патчей Kaspersky Industrial CyberSecurity for Nodes, установленного на устройствах под управлением Windows XP, из-за особенностей операционной системы может потребоваться выполнение перезагрузки устройства.
- После установки критических обновлений модулей Kaspersky Industrial CyberSecurity for Nodes, по умолчанию значок приложения будет скрыт.
- KLRAMDISK не поддерживается на защищаемых устройствах с операционными системами Windows XP и Windows Server® 2003.
- В случае ошибки установки патча для Kaspersky Industrial CyberSecurity for Nodes выполняется откат патча с последующим запросом перезагрузки операционной системы.

Интерфейс

- При использовании фильтров в Консоли приложения учитывается регистр для карантина, резервного хранилища, журнала системного аудита и журналов выполнения задач.
- При настройке области защиты и области проверки в Консоли приложения можно использовать только одну маску и только в конце пути. Примеры использования маски: `C:\Temp\Temp*`, `C:\Temp\Temp???.doc`, `C:\Temp\Temp*.doc`. Это ограничение не распространяется на настройку доверенной зоны.
- В Консоли приложения в разделе **Серверы сбора телеметрии** не отображается время запуска задач. Колонка **Время запуска** пуста.
- В Консоли администрирования Kaspersky Security Center и Консоли приложения не отображаются всплывающие подсказки для текстовых элементов интерфейса длиннее 256 символов.
- В Консоли администрирования Kaspersky Security Center в окне **Выбор пользователя или группы пользователей** отображаются только первые 50 000 пользователей из списка пользователей Kaspersky Security Center. Подробнее см. в справке Kaspersky Security Center.

Безопасность

- Если в операционной системе активирован Контроль учетных записей, учетные записи пользователей должны входить в группу администраторов KICS Administrators, чтобы можно было открывать Консоль приложения двойным щелчком мыши на значке приложения в области уведомлений панели задач. В противном случае для входа придется использовать учетную запись с правами открывать Диагностическое окно или оснастку Microsoft Management Console (MMC).

- Если активирован Контроль учетных записей пользователей, недоступно удаление приложения из окна Microsoft Windows "Программы и компоненты".

Защита от эксплойтов

- Защита от эксплойтов недоступна, если библиотеки apphelp.dll не загружены в текущей конфигурации сетевого окружения.

- Компонент Защита от эксплойтов несовместим с утилитой EMET от Microsoft на защищаемых устройствах с операционной системой Microsoft Windows 10. Kaspersky Industrial CyberSecurity for Nodes блокирует EMET, если компонент Защита от эксплойтов установлен на защищаемом устройстве с установленной утилитой EMET.

- Компонент Защита от эксплойтов несовместим с ядром базы данных SQL Server® 2012. Если Kaspersky Industrial CyberSecurity for Nodes устанавливается на компьютер с MS SQL Server 2012, необходимо добавить библиотеку sqlos.dll сервера баз данных в список исключений в задаче Защита от эксплойтов.

Detection and Response

- Если в процессе реагирования на угрозу возникает ошибка, связанная с доступом к сетевой папке, такая ошибка не будет отображаться в истории реагирования на угрозы (Web Console → свойства хоста с установленным приложением → раздел **Detection and Response** → **История реагирования**).

- Просмотр истории реагирования на угрозы недоступен для защищаемых устройств под управлением Windows XP с установленным Агентом администрирования версии 10.5.1781.

- Kaspersky Industrial CyberSecurity for Nodes версии 4.5 не поддерживает следующие события телеметрии EDR Expert (on-premises):

  - LDAP Attribute Change;
  - GPO Change;
  - SCCM Local Config Mismatch;
  - SCCM Config Change;
  - SCCM Deployment Task;
  - Smb Connection Open.

  Начиная с версии Kaspersky Industrial CyberSecurity for Nodes 5.0, приложение поддерживает все эти события телеметрии EDR Expert (on-premises), кроме LDAP Attribute Change.

- Миграция конфигурации [KICS+KEA] на [KICS+встроенный агент] может завершиться с ошибкой удаления приложения Kaspersky Endpoint Agent. Ошибка удаления приложения исправлена в последней версии Kaspersky Endpoint Agent. Для удаления Kaspersky Endpoint Agent перезагрузите компьютер и создайте задачу удаления приложения.

- Конфигурация [KICS+KEA+встроенный агент] не поддерживается. Такая конфигурация нарушает взаимодействие между приложениями и решением Detection and Response, которое развернуто в вашей организации. Также использование Kaspersky Endpoint Agent и встроенного агента на одном компьютере может привести к дублированию телеметрии и повышенной нагрузке на компьютер и сеть. После миграции на конфигурацию [KICS+встроенный агент] убедитесь, что приложение Kaspersky Endpoint Agent удалено с компьютера. Если Kaspersky Endpoint Agent продолжает работу после миграции, удалите приложение вручную (например, с помощью задачи *Удаленная деинсталляция приложения*).

  Установщик позволяет развернуть Kaspersky Endpoint Agent на компьютере с Kaspersky Industrial CyberSecurity for Nodes и встроенным агентом. Также Kaspersky Endpoint Agent и встроенный агент могут быть установлены на одном компьютере в результате выполнения задачи *Изменение состава компонентов приложения*. Поведение зависит от версий Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Endpoint Agent.

Настройка событий

Параметры события *Подозрительная файловая операция в контролируемой области*, которые можно настроить в разделе **Настройка событий** политики Kaspersky Security Center, применяются также к следующим событиям:

- *Разрешенная файловая операция в контролируемой области, выполненная доверенным пользователем*.
- *Запрещенная файловая операция в контролируемой области*.
- *Только статистика: запрещенная файловая операция в контролируемой области*.
- *Подозрительная файловая операция в контролируемой области*.

Диагностическое окно

Для работы диагностического окна на компьютерах под управлением Windows XP необходимо, чтобы работала Служба терминалов.

Контроль устройств

При удалении и последующей установке приложения без перезагрузки Контроль устройств может оставаться включенным. Для восстановления корректной работы компонента Контроль устройств перезагрузите компьютер.

Работа в Безопасном режиме Windows

Не поддерживается работа приложения в Безопасном режиме Windows (Safe Mode).

Типовые схемы развертывания

Kaspersky Industrial CyberSecurity for Nodes является частью решения Kaspersky Industrial CyberSecurity.

Решение Kaspersky Industrial CyberSecurity включает следующие утилиты и программы:

- Kaspersky Security Gateway.
- Kaspersky Industrial CyberSecurity for Nodes.
- Kaspersky Industrial CyberSecurity for Networks.
- Kaspersky Security Center.

Программы Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes работают на разных уровнях *выделенной сети*. Выделенная сеть Kaspersky Industrial CyberSecurity – это часть промышленной сети, которая включает компьютеры, предназначенные для работы программ Kaspersky Industrial CyberSecurity для защиты промышленных систем и вспомогательного оборудования (например, коммутаторов).

Программа Kaspersky Industrial CyberSecurity for Networks выполняет мониторинг и анализ трафика промышленной сети. Программа Kaspersky Industrial CyberSecurity for Nodes, установленная на узле промышленной сети, защищает компьютер от известных угроз компьютерной безопасности и контролирует целостность проектов ПЛК, включенных в область проверки.

Вы можете управлять программами Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes, развернутыми в одной выделенной сети, с помощью единой Консоли администрирования Kaspersky Security Center. Вы также можете настроить передачу диагностических данных, полученных от программ Kaspersky Industrial CyberSecurity for Networks и Kaspersky Industrial CyberSecurity for Nodes, из Kaspersky Security Center в систему SCADA с помощью программы Kaspersky Security Gateway.

Kaspersky Industrial CyberSecurity for Nodes включает:

- *Функциональный модуль* – фиксирует информацию о состоянии узлов промышленной сети, а также выполняет защиту узлов от информационных угроз.
- *Консоль* – является локальным графическим интерфейсом пользователя. С помощью Консоли Kaspersky Industrial CyberSecurity for Nodes вы можете управлять работой программы на узлах промышленной сети. Консоль может устанавливаться на компьютере с установленной программой Kaspersky Industrial CyberSecurity for Nodes или на любом другом компьютере защищаемой сети. В этом случае управление программой с помощью Консоли выполняется удаленно. Вы также можете управлять несколькими компьютерами, которые защищены Kaspersky Industrial CyberSecurity for Nodes, с помощью одной Консоли.

Kaspersky Industrial CyberSecurity for Nodes фиксирует события безопасности на защищаемых узлах и передает их в Консоль приложения и Консоль администрирования Kaspersky Security Center. Доступ к локальной Консоли приложения и к Консоли администрирования Kaspersky Security Center осуществляется с рабочего места специалиста, наблюдающего за технологическим процессом на предприятии, а также с рабочего места специалиста по информационной безопасности.

В примере развертывания Kaspersky Industrial CyberSecurity for Nodes в составе решения Kaspersky Industrial CyberSecurity (см. рис. ниже) выделенная сеть показана синим цветом, компоненты промышленной сети показаны красным цветом. Вариант схемы развертывания зависит от особенностей конкретной промышленной сети, в которой планируется установка программ решения Kaspersky Industrial CyberSecurity.

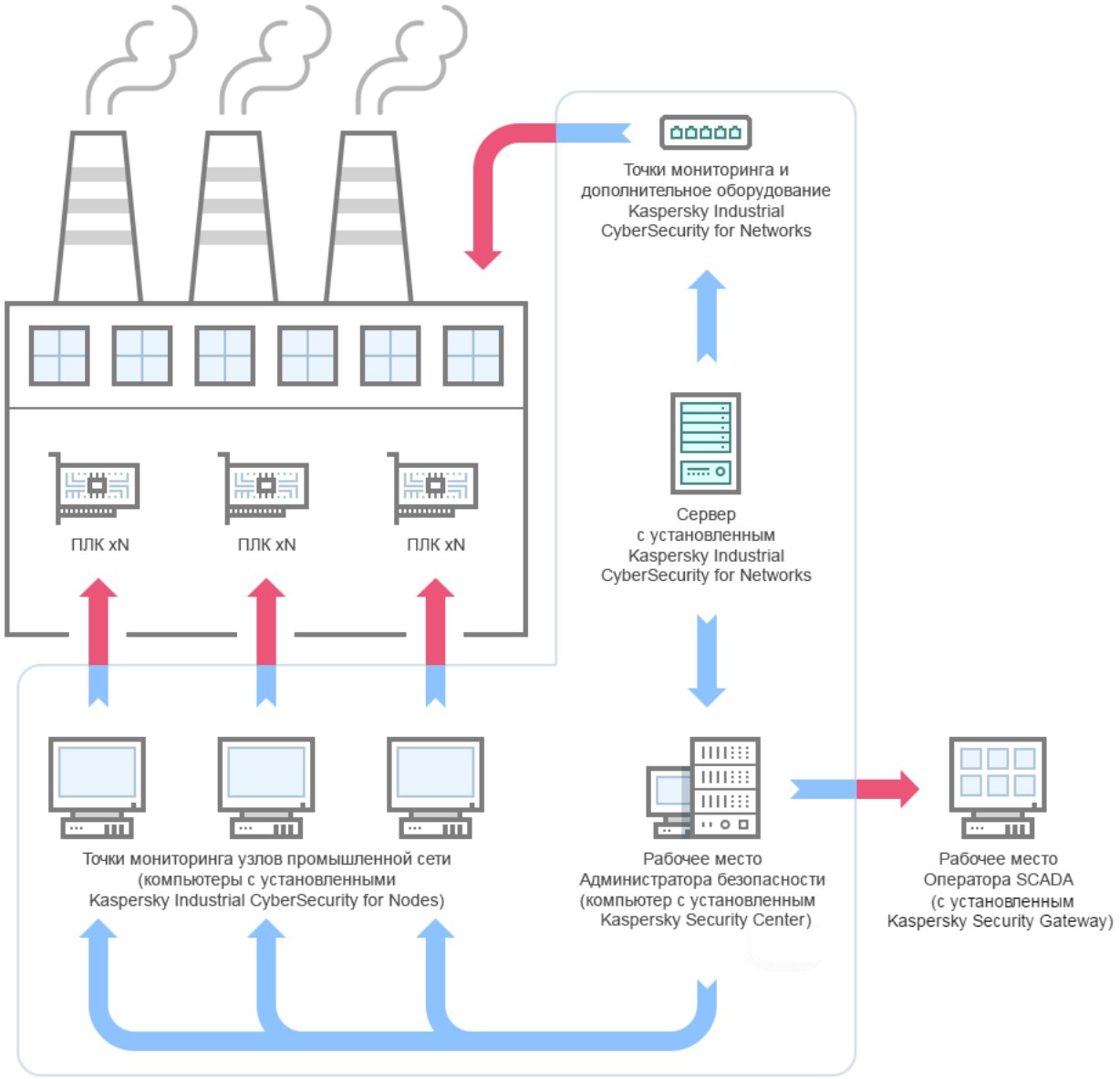


Схема развертывания Kaspersky Industrial CyberSecurity for Nodes

Совместимость с другими приложениями

Приложение Kaspersky Industrial CyberSecurity for Nodes в конфигурации *Полная функциональность* несовместимо с приложениями, которые входят в состав систем защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Также Kaspersky Industrial CyberSecurity for Nodes может быть несовместимо с другими приложениями и с некоторыми приложениями "Лаборатории Касперского". Для проверки совместимости Kaspersky Industrial CyberSecurity for Nodes использует список ПО, составленный в "Лаборатории Касперского". Этот список сформирован в файле incompatible.txt. Файл добавлен в комплект поставки.

При обнаружении приложения из списка в файле incompatible.txt установщик останавливает установку Kaspersky Industrial CyberSecurity for Nodes. Вам необходимо удалить стороннее антивирусное приложение. Некоторые приложения из списка установщик может удалить автоматически.

Если на компьютере установлен Брандмауэр Windows, установщик выключает его для дальнейшей установки Kaspersky Industrial CyberSecurity for Nodes.

Если несмотря на риски вам нужно установить на один компьютер приложение Kaspersky Industrial CyberSecurity for Nodes и приложение из списка в файле incompatible.txt, вы можете пропустить проверку компьютера на совместимость с установленными сторонними антивирусными приложениями. Для этого вам нужно передать в установщик параметры `SKIPPRODUCTCHECK=1` и `SKIPPRODUCTUNINSTALL=1`.

Пример:

```
setup_kics.exe /s EULA=1 PRIVACYPOLICY=1 SKIPPRODUCTCHECK=1 SKIPPRODUCTUNINSTALL=1
```

Приложение Kaspersky Industrial CyberSecurity for Nodes в конфигурации *Endpoint Agent* может быть установлено на одном компьютере с EPP-приложениями от сторонних поставщиков.

Установка и удаление приложения

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

Планирование установки

В этом разделе описаны средства администрирования Kaspersky Industrial CyberSecurity for Nodes, особенности установки и удаления Kaspersky Industrial CyberSecurity for Nodes с помощью мастера установки, из командной строки, с помощью Kaspersky Security Center и через групповые политики Active Directory.

В случае установки Kaspersky Industrial CyberSecurity for Nodes после удаления Kaspersky Embedded Systems Security для Windows или Kaspersky Endpoint Security для Windows необходимо перезагрузить компьютер.

Перед началом установки Kaspersky Industrial CyberSecurity for Nodes составьте план основных этапов установки.

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Industrial CyberSecurity for Nodes и для настройки приложения.
2. Определите, какие программные компоненты требуется установить.
3. Выберите способ установки.

Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров и управления Kaspersky Industrial CyberSecurity for Nodes. В качестве средств администрирования Kaspersky Industrial CyberSecurity for Nodes вы можете использовать Консоль приложения, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

Консоль Kaspersky Industrial CyberSecurity for Nodes

Консоль Kaspersky Industrial CyberSecurity for Nodes представляет собой самостоятельную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes через Консоль приложения, установленную на защищаемом устройстве или на другом устройстве в сети организации.

Вы можете добавить несколько оснасток Kaspersky Industrial CyberSecurity for Nodes в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких устройств, на которых установлено приложение Kaspersky Industrial CyberSecurity for Nodes.

Утилита командной строки

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes из командной строки защищаемого устройства.

Утилита командной строки входит в набор программных компонентов Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств в вашей организации, вы можете управлять Kaspersky Industrial CyberSecurity for Nodes через Консоль администрирования Kaspersky Security Center.

Вам потребуется установить следующие компоненты:

- **Модуль интеграции с Агентом администрирования Kaspersky Security Center**. Этот компонент входит в группу программных компонентов Kaspersky Industrial CyberSecurity for Nodes. Он позволяет Kaspersky Industrial CyberSecurity for Nodes взаимодействовать с Агентом администрирования. Установите модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемое устройство.

- **Агент администрирования Kaspersky Security Center**. Установите его на каждом защищаемом устройстве. Этот компонент будет обеспечивать взаимодействие между приложением Kaspersky Industrial CyberSecurity for Nodes, установленном на защищаемом устройстве, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.

- **Плагин управления Kaspersky Industrial CyberSecurity for Nodes**. Дополнительно на защищаемом устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, установите Плагин управления Kaspersky Industrial CyberSecurity for Nodes для работы через Консоль администрирования. Плагин обеспечивает интерфейс управления приложением через Kaspersky Security Center. Файл установки Плагина управления \exec\klcfginst.exe входит в комплект поставки Kaspersky Industrial CyberSecurity for Nodes.

Выбор способа установки

После определения программных компонентов для установки Kaspersky Industrial CyberSecurity for Nodes, необходимо выбрать способ установки приложения.

Выберите способ установки в зависимости от архитектуры сети и следующих условий:

- Потребуется ли вам задать специальные параметры установки Kaspersky Industrial CyberSecurity for Nodes или вы будете использовать рекомендуемые параметры установки.

- Будут ли параметры установки едиными для всех защищаемых устройств или индивидуальными для каждого защищаемого устройства.

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes как в интерактивном режиме с помощью мастера установки, так и в режиме без взаимодействия с пользователем, запустив файл пакета установки с заданными параметрами из командной строки. Вы можете выполнить централизованную удаленную установку Kaspersky Industrial CyberSecurity for Nodes: через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Security Center.

Вы можете установить и настроить Kaspersky Industrial CyberSecurity for Nodes на отдельном защищаемом устройстве и сохранить его параметры в конфигурационный файл, чтобы затем использовать созданный файл для установки Kaspersky Industrial CyberSecurity for Nodes на другие защищаемые устройства. Однако это невозможно при установке приложения через групповые политики Active Directory.

Запуск мастера установки

С помощью мастера установки вы можете установить:

- Компоненты Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве по ссылке из приложения-приветствия, которая запускается с помощью файла setupui.exe, или напрямую с помощью файла \exec\setup_kics.exe, входящих в комплект поставки.

- Консоль Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве или другом устройстве в локальной сети по ссылке из приложения-приветствия, которая запускается с помощью файла setupui.exe, или напрямую с помощью файла \client\setup_kicstools.exe, входящих в комплект поставки.

Запуск из командной строки файла пакета установки с параметрами установки

Запустив файл пакета установки без ключей, вы установите Kaspersky Industrial CyberSecurity for Nodes с параметрами установки по умолчанию. С помощью ключей Kaspersky Industrial CyberSecurity for Nodes вы можете изменять параметры установки.

Вы можете установить Консоль приложения на защищаемом устройстве или на рабочем месте администратора.

Вы также можете использовать команды для установки Kaspersky Industrial CyberSecurity for Nodes и Консоли приложения.

Централизованная установка через Kaspersky Security Center

Если вы используете Kaspersky Security Center для управления антивирусной защитой устройств в сети, вы можете установить Kaspersky Industrial CyberSecurity for Nodes на несколько устройств с помощью задачи удаленной установки.

Защищаемые устройства, на которых вы хотите установить Kaspersky Industrial CyberSecurity for Nodes с помощью Kaspersky Security Center, могут находиться как в одном домене с Kaspersky Security Center, так и в другом домене, а также вообще не принадлежать ни к одному домену.

Централизованная установка через групповые политики Active Directory

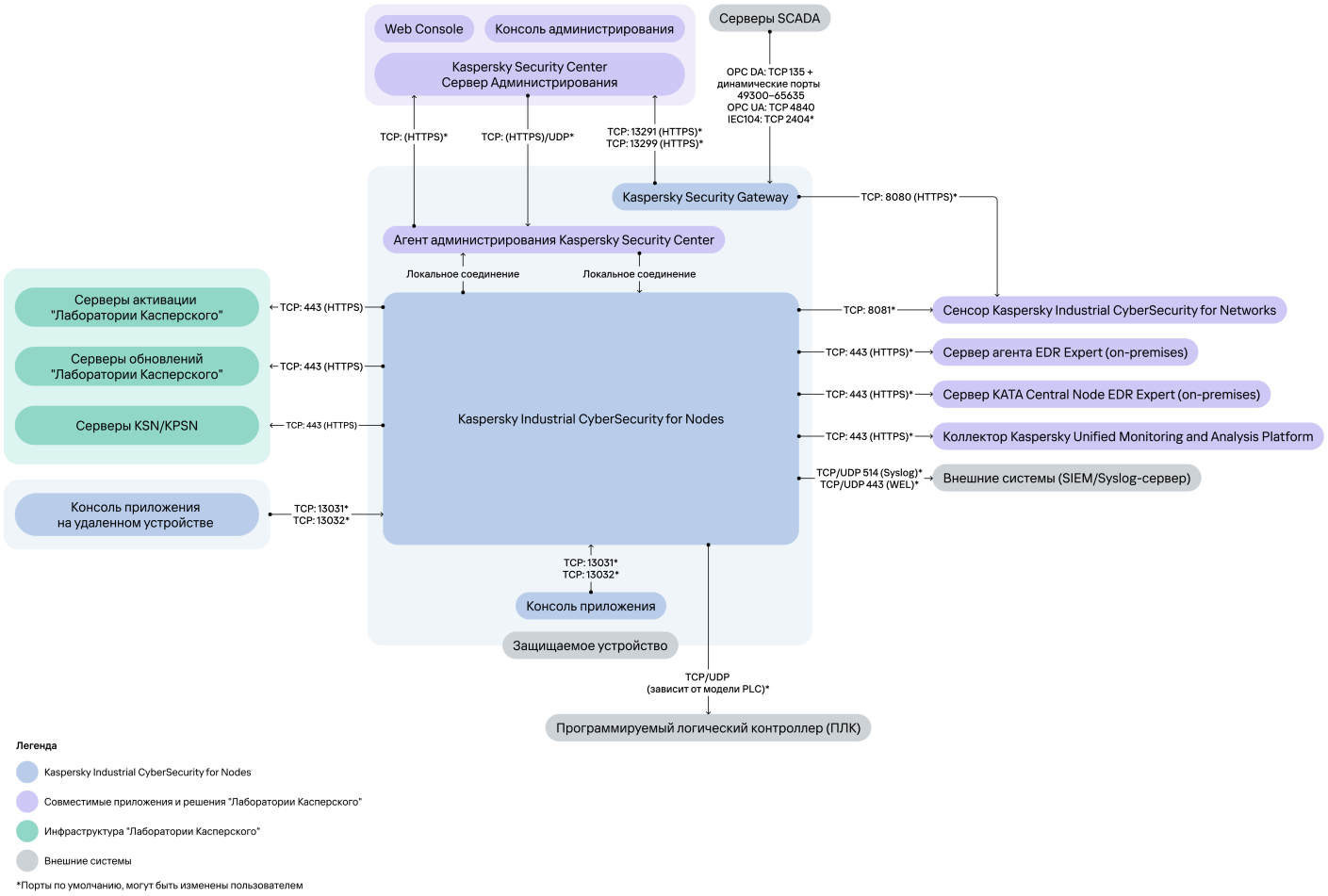
С помощью групповых политик Active Directory вы можете устанавливать Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве. Вы можете установить Консоль приложения на защищаемом устройстве или рабочем месте администратора.

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes, используя только параметры установки по умолчанию.

Защищаемые устройства, на которых приложение Kaspersky Industrial CyberSecurity for Nodes было установлено с помощью групповых политик Active Directory, должны находиться в том же домене и в том же подразделении организации. Установка выполняется при запуске защищаемого устройства, перед входом в Microsoft Windows.

Используемые порты

Для установки и работы компонентов Kaspersky Industrial CyberSecurity for Nodes в настройках сетевого оборудования или программного обеспечения, используемого для контроля сетевого трафика, требуется открыть порты, указанные на схеме ниже.



Порты, используемые Kaspersky Industrial CyberSecurity for Nodes

Назначение используемых портов описано в таблице ниже.

Назначение используемых портов

Назначение	Участники обмена данными		Порт по умолчанию	Возможность настройки порта	Протокол
	Источник	Получатель			
Управление Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center	Сервер администрирования Kaspersky Security Center	Агент администрирования Kaspersky Security Center	См. справку Kaspersky Security Center	Да	TCP (HTTPS), UDP (см. справку Kaspersky Security Center)
	Агент администрирования Kaspersky Security Center	Сервер администрирования Kaspersky Security Center			

Назначение	Участники обмена данными		Порт по умолчанию	Возможность настройки порта	Протокол
	Источник	Получатель			
Управление приложением через Консоль Kaspersky Industrial CyberSecurity for Nodes	Консоль приложения	Kaspersky Industrial CyberSecurity for Nodes	13031, 13032	Да	TCP
	Консоль приложения на удаленном устройстве	Kaspersky Industrial CyberSecurity for Nodes	13031, 13032	Да	TCP
Обновление баз и модулей Kaspersky Industrial CyberSecurity for Nodes	Kaspersky Industrial CyberSecurity for Nodes	Серверы обновлений "Лаборатории Касперского"	443	Нет	TCP (HTTPS)
Активация Kaspersky Industrial CyberSecurity for Nodes	Kaspersky Industrial CyberSecurity for Nodes	Серверы активации "Лаборатории Касперского"	443	Нет	TCP (HTTPS)
Использование KSN	Kaspersky Industrial CyberSecurity for Nodes	Серверы KSN/KPSN	443	Нет	TCP (HTTPS)
Интеграция с Kaspersky Industrial CyberSecurity for Networks	Kaspersky Industrial CyberSecurity for Nodes	Сенсор Kaspersky Industrial CyberSecurity for Networks	8081	Да	TCP
Использование Kaspersky Security Gateway	Kaspersky Security Gateway	Kaspersky Security Center Сервер администрирования	13291, 13299	Да	TCP (HTTPS)
	Kaspersky Security Gateway	Сенсор Kaspersky Industrial CyberSecurity for Networks	8080	Да	TCP (HTTPS)
	Серверы SCADA	Kaspersky Security Gateway	OPC DA: 135 + динамический диапазон портов 49300-65635 OPC UA: 4840 IEC104: 2404	Да	TCP
Интеграция с Endpoint Detection and Response Expert (on-premises)	Kaspersky Industrial CyberSecurity for Nodes	EDR Expert (on-premises) Сервер агента	443	Да	TCP (HTTPS)
	Kaspersky Industrial CyberSecurity for Nodes	EDR Expert (on-premises) Сервер KATA Central Node	443	Да	TCP (HTTPS)
	Kaspersky Industrial CyberSecurity for Nodes	Коллектор KUMA	443	Да	TCP (HTTPS)

Назначение	Участники обмена данными		Порт по умолчанию	Возможность настройки порта	Протокол
	Источник	Получатель			
Защита промышленной сети	Kaspersky Industrial CyberSecurity for Nodes	Siemens SIMATIC S7-300	102	Да	TCP
		Siemens SIMATIC S7-400			
		Siemens SIMATIC S7-400H			
		Siemens SIMATIC S7-1200			
		Siemens SIMATIC S7-1500			
		Siemens SIPROTEC 4	50000	Да	UDP
		Schneider Electric Modicon M340	502	Да	TCP
		Schneider Electric Modicon M580			
		Устройства на базе CODESYS V3	11740	Да	TCP
		OWEN PLC210			
		Fastwel CPM723-01			
		Prosoft Systems Regul R500			
		Emerson DeltaV	23 (Telnet), 18550	Да	TCP
		Rockwell Automation Allen-Bradley ControlLogix;	44818	Да	TCP
		TREI-5B	6000	Да	TCP
Интеграция с SIEM	Kaspersky Industrial CyberSecurity for Nodes	SIEM/Syslog-сервер	Syslog: 514 WEL: 443	Да	TCP / UDP (настраиваемый)

Установка и удаление приложения с помощью мастера

В этом разделе описана установка и удаление Kaspersky Industrial CyberSecurity for Nodes и Консоли приложения с помощью мастера установки, а также приведена информация о дополнительных параметрах Kaspersky Industrial CyberSecurity for Nodes и действиях при установке.

Установка с помощью мастера установки

В следующих разделах содержится информация об установке Kaspersky Industrial CyberSecurity for Nodes и Консоли приложения.

Чтобы установить и начать использовать Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. Установите Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве.
2. На устройства, с которых вы планируете управлять Kaspersky Industrial CyberSecurity for Nodes, установите Консоль приложения.

3. Если вы установили Консоль приложения не на защищаемом устройстве, а на другом устройстве сети, выполните дополнительную настройку, чтобы пользователи Консоли приложения могли удаленно управлять Kaspersky Industrial CyberSecurity for Nodes.

4. Выполните действия после установки Kaspersky Industrial CyberSecurity for Nodes.

Установка Kaspersky Industrial CyberSecurity for Nodes

Перед установкой Kaspersky Industrial CyberSecurity for Nodes выполните следующие действия:

1. Убедитесь, что на защищаемом устройстве не установлены другие антивирусные приложения.

2. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на защищаемом устройстве.

После выполнения описанных выше действий перейдите к процедуре установки. Следуя инструкциям мастера установки, задайте параметры установки Kaspersky Industrial CyberSecurity for Nodes.

Можно более детально ознакомиться с параметрами установки (удаления).

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с помощью мастера установки:

1. На защищаемом устройстве запустите файл setupui.exe.

2. В открывшемся окне в разделе **Установка** перейдите по ссылке **Установить Kaspersky Industrial CyberSecurity for Nodes 5.0**.

3. В открывшемся окне приветствия мастера установки Kaspersky Industrial CyberSecurity for Nodes нажмите на кнопку **Далее >**.

   Откроется окно **Лицензионное соглашение**.

4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.

5. Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящих Лицензионных соглашений** 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 Политику конфиденциальности**.

   Если вы не примите Лицензионное соглашение и (или) Политику конфиденциальности, установка будет прервана.

6. Нажмите на кнопку **Далее >**.

   Откроется окно **Выборочная установка**. Выберите компоненты, которые вы хотите установить.

   - **Полная функциональность**

     По умолчанию все компоненты Kaspersky Industrial CyberSecurity for Nodes, кроме Счетчиков производительности и Endpoint Agent, включены в список рекомендуемых к установке.

Компонент Поддержка SNMP-протокола Kaspersky Industrial CyberSecurity for Nodes отображается в списке устанавливаемых компонентов, только если на защищаемом устройстве установлена служба SNMP (Microsoft Windows).

- **Endpoint Agent**

  При выборе этого варианта Kaspersky Industrial CyberSecurity for Nodes будет установлен в конфигурации Endpoint Agent. Более подробную информацию о данной конфигурации см. в этом разделе.

7. Нажмите на кнопку **Далее >**.

8. В окне **Выбор папки для установки приложения** выполните следующие действия:

   - Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Industrial CyberSecurity for Nodes.

   - Если требуется, нажмите на кнопку **Обзор** для просмотра информации о доступном пространстве на локальных жестких дисках.

9. Нажмите на кнопку **Далее >**.

10. В окне **Изменение папок, используемых по умолчанию** вы можете изменить путь к папкам, используемым приложением.

    Установка приложения завершается с ошибкой, если путь к папке установки приложения совпадает с путем к хотя бы одной из следующих папок: баз приложения, резервного хранилища, для восстановления объектов из карантина, журналов, хранилища для временных файлов.

11. В окне **Дополнительные настройки** вы можете исключить из области защиты и проверки объекты и папки и настроить параметры Постоянной защиты файлов.

    Если необходимо, выберите профиль исключений для промышленной программы – набор правил конфигурации в формате XML, предназначенных для добавления процессов и файлов промышленной программы в списки доверенных процессов и исключений, а также для настройки правил и параметров Контроля запуска программ.

    Если режим работы Постоянной защиты файлов не выбран, вы не можете перейти на следующий шаг Мастера установки приложения.

12. Нажмите на кнопку **Далее >**.

13. В окне **Импорт параметров из конфигурационного файла** укажите путь к конфигурационному файлу, если вы хотите импортировать параметры Kaspersky Industrial CyberSecurity for Nodes из имеющегося конфигурационного файла, созданного в предыдущей версии приложения.

14. Нажмите на кнопку **Далее >**.

15. В окне **Настройки удаленного доступа**, если необходимо, измените номера TCP-портов, используемых для удаленного подключения Консоли приложения к компьютеру с установленным приложением.

    Номер порта по умолчанию для подключения с учетными данными Windows – 13032, для подключения с учетными данными вручную созданных пользователей – 13031. Диапазон возможных номеров портов: 1 – 65535.

Чтобы запретить подключение с использованием учетных данных пользователей, созданных вручную, снимите флажок **С учетными данными вручную созданных пользователей**.

16. Нажмите на кнопку **Далее >**.

17. В окне **Активация программы** выполните одно из следующих действий:

    - Если вы хотите активировать приложение, укажите путь к файлу ключа Kaspersky Industrial CyberSecurity for Nodes.
    - Если вы хотите активировать приложение позже, нажмите на кнопку **Далее >**.
    - Если вы предварительно сохранили файл ключа в папке \exec комплекта поставки, имя этого файла отобразится в поле **Ключ**.

    После добавления файла ключа в окне отобразится информация о лицензии. В Kaspersky Industrial CyberSecurity for Nodes отображается расчетная дата истечения срока действия лицензии. Срок действия лицензии отсчитывается с момента добавления ключа, а истекает не позднее даты окончания срока действия файла ключа.

18. Нажмите на кнопку **Далее >**, чтобы добавить файл ключа в приложение.

19. В окне **Подготовка к установке приложения**, если необходимо, выключите функцию **Защищать процесс установки приложения**. Защита установки включает в себя защиту от подмены дистрибутива вредоносными приложениями, блокирование доступа к папке установки Kaspersky Industrial CyberSecurity for Nodes и блокирование доступа к разделу системного реестра с ключами приложения. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку приложения (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).

20. Если необходимо, добавьте путь к файлу kavshell.exe в системную переменную %PATH% для удобства использования интерфейса командной строки.

21. Нажмите на кнопку **Установить**.

    Мастер приступит к установке Kaspersky Industrial CyberSecurity for Nodes. По завершении установки откроется окно **Завершение работы мастера установки приложения**.

22. Нажмите на кнопку **Готово**.

Установка Консоли Kaspersky Industrial CyberSecurity for Nodes

Следуя инструкциям мастера установки, настройте параметры установки Консоли приложения. Вы можете прервать установку на любом этапе работы мастера. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Чтобы установить Консоль Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на устройстве.

2. На защищаемом устройстве запустите файл setupui.exe.

   Откроется окно приложения-приветствия.

3. Перейдите по ссылке **Установить Консоль Kaspersky Industrial CyberSecurity for Nodes**.

   Откроется окно приветствия мастера установки.

4. Нажмите на кнопку **Далее >**.

5. Если вы согласны с условиями и положениями Лицензионных соглашений и Политики конфиденциальности, установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящих Лицензионных соглашений** 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 Политику конфиденциальности**

6. В окне **Выбор папки для установки приложения**, если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.

7. Нажмите на кнопку **Далее >**.

8. В окне **Подготовка к установке приложения** нажмите на кнопку **Установить**.

   Мастер приступит к установке Консоли Kaspersky Industrial CyberSecurity for Nodes.

9. Нажмите на кнопку **Готово**.

Консоль приложения будет установлена.

Если вы установили Консоль приложения не на защищаемом устройстве, а на другом устройстве сети, выполните дополнительную настройку.

Дополнительная настройка после установки Консоли приложения на другое устройство

Если вы установили Консоль приложения не на защищаемом устройстве, а на другом устройстве сети, выполните следующие действия для того, чтобы пользователи могли удаленно управлять Kaspersky Industrial CyberSecurity for Nodes:

- Используйте учетную запись пользователя, у которого в настройках приложения есть разрешение на удаленное подключение. По умолчанию такое разрешение есть у всех пользователей, входящих в группы Administrators и KICS Administrators.

- На удаленном устройстве в параметрах брандмауэра Windows откройте порт TCP 13032 для подключения с использованием учетных записей системных пользователей Windows и порт TCP 13031 для подключения с использованием учетных записей, созданных вручную в настройках приложения. Также разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes – avp.exe. Вы можете выполнить данную настройку, используя ключ `ADDWFEXCLUSION=1` при установке приложения из командной строки.

При необходимости удаленного запуска Kaspersky Industrial CyberSecurity for Nodes дополнительно выполните следующие действия:

Учетная запись пользователя, от имени которого выполняется удаленный запуск приложения, должна входить в группу Администраторы. Убедитесь, что для данной учетной записи настроены необходимые права на управление Kaspersky Industrial CyberSecurity for Nodes и на управление службой Kaspersky Industrial CyberSecurity for Nodes Service.

- На удаленном устройстве в параметрах брандмауэра Windows включите правило **Общий доступ к файлам и принтерам (входящий трафик SMB)** (порт TCP 445). Также рекомендуется открыть порт TCP 135 для ускорения подключения к устройству.
- Для удаленных устройств под управлением Windows Vista и выше, не входящих в домен или управляемых локальной учетной записью, **отключите удаленный контроль учетных записей пользователей (UAC).**

  1. Откройте редактор реестра на компьютере.
  2. В редакторе реестра перейдите в раздел HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.
  3. Откройте параметр LocalAccountTokenFilterPolicy.

     Если параметр LocalAccountTokenFilterPolicy отсутствует в данном разделе, вам необходимо создать параметр DWORD (32 бита) с таким названием (подробнее см. на сайте Службы технической поддержки Microsoft).
  4. Установите для него значение `1` и нажмите на кнопку **OK**.

     Отключение удаленного UAC не влияет на локальный UAC.

- Если устройство, на котором установлена Консоль приложения, или защищаемое устройство находятся под управлением Windows 8.1 или более ранней версии ОС, **включите поддержку общего доступа к файлам SMB 1.0/CIFS на устройствах под управлением Windows 10 и выше.**

  - В приложении "Компоненты Windows":

    1. Выберите **Пуск** → **Панель управления** → **Программы** → **Включение или отключение компонентов Windows**.
    2. В окне **Компоненты Windows** установите флажок **Поддержка общего доступа к файлам SMB 1.0/CIFS**.
    3. Нажмите на кнопку **OK**.

- В среде Windows PowerShell:

  1. Запустите Windows PowerShell от имени администратора.

  2. Выполните команду:

```
Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

Аналогичные шаги следует выполнить для настройки любого другого программного или аппаратного сетевого экрана.

Если Консоль приложения открыта во время настройки соединения между защищаемым устройством и устройством, на котором установлена Консоль приложения, выполните следующие действия:

1. Закройте Консоль приложения.
2. Дождитесь завершения процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes – avp.exe.
3. Перезапустите Консоль приложения.

   Будут применены новые параметры соединения.

Действия после установки Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes запускает задачи защиты и проверки сразу после установки, если вы активировали приложение. Если во время установки Kaspersky Industrial CyberSecurity for Nodes был установлен флажок **Включить Постоянную защиту файлов после установки приложения (рекомендуется)** (по умолчанию), приложение проверяет объекты файловой системы устройства при доступе к ним. Если при выборочной установке был установлен компонент Проверка скриптов, Kaspersky Industrial CyberSecurity for Nodes будет выполнять проверку программного кода всех скриптов при их запуске. Каждую пятницу в 20:00 Kaspersky Industrial CyberSecurity for Nodes выполняет задачу *Проверка важных областей*.

После установки Kaspersky Industrial CyberSecurity for Nodes рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз приложения. После установки Kaspersky Industrial CyberSecurity for Nodes проверяет объекты с использованием баз, которые входили в состав приложения при поставке.

  Рекомендуется сразу же обновить базы Kaspersky Industrial CyberSecurity for Nodes, так как базы могли устареть.

  Далее приложение будет обновлять базы каждый час согласно расписанию, установленному в задаче по умолчанию.

- Выполнить Проверку важных областей, если перед установкой Kaspersky Industrial CyberSecurity for Nodes на устройстве не было установлено антивирусное приложение с включенной функцией постоянной защиты файлов.

- Настроить уведомления администратора о событиях Kaspersky Industrial CyberSecurity for Nodes.

Запуск и настройка задачи Обновление баз и модулей приложения

Чтобы обновить базы приложения после установки, выполните следующие действия:

1. В свойствах задачи *Обновление* настройте соединение с источником обновлений.
2. Запустите задачу *Обновление*.

В вашей сети может быть не настроен протокол Web Proxy Auto-Discovery Protocol (WPAD) для автоматического распознавания параметров прокси-сервера в локальной сети. В этом случае может потребоваться проверка подлинности при доступе к прокси-серверу.

Чтобы указать дополнительные параметры прокси-сервера и параметры проверки подлинности для доступа к прокси-серверу, выполните следующие действия:

1. В Консоли приложения откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Свойства приложения**.
3. В открывшемся окне выберите вкладку **Настройки сети**.
4. В разделе **Настройки прокси-сервера** нажмите на кнопку **Настройка** и в открывшемся окне установите флажок **Использовать указанный прокси-сервер**.
5. В поле **Адрес** укажите адрес прокси-сервера, а в поле **Порт** укажите номер порта прокси-сервера.
6. При необходимости снимите флажок **Не использовать прокси-сервер для локальных адресов**. Если функция включена, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленным приложением Kaspersky Industrial CyberSecurity for Nodes, происходит напрямую, прокси-сервер не используется. По умолчанию функция включена.
7. В разделе **Настройки аутентификации на прокси-сервере** выберите требуемый метод аутентификации из раскрывающегося списка:
   - **Не использовать аутентификацию**.
   - **NTLM-аутентификация**. NTLM-аутентификация с помощью учетной записи текущего пользователя (значение по умолчанию).
   - **NTLM-аутентификация с именем пользователя и паролем.** NTLM-аутентификация с помощью учетных данных, заданных вручную.
   - **Kerberos-аутентификация**. Kerberos-аутентификация с помощью учетной записи текущего пользователя.

     Для обеспечения корректной работы Kerberos-аутентификации при использовании CNAME-записей для адреса прокси-сервера вам необходимо зарегистрировать имя субъекта-службы (SPN) для каждой CNAME-записи.

- **Kerberos-аутентификация с именем пользователя и паролем**. Kerberos-аутентификация с использованием учетных данных, заданных вручную.
- **Имя пользователя и пароль**. Аутентификация с использованием учетных данных, заданных вручную.

Если требуется, укажите имя пользователя и пароль.

Если выбрана Kerberos-аутентификация, Kaspersky Industrial CyberSecurity for Nodes может в зависимости от настроек прокси-сервера осуществлять аутентификацию как по протоколу Kerberos, так и по протоколу NTLM.

8. Нажмите **OK**.

Чтобы запустить задачу Обновление, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Обновление**.
2. В контекстном меню вложенного узла **Обновление баз** выберите пункт **Запуск**.

Задача *Обновление* будет запущена.

После того как задача успешно завершится, вы сможете посмотреть дату выпуска последних установленных обновлений баз в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes**.

Проверка важных областей

После того как вы обновили базы Kaspersky Industrial CyberSecurity for Nodes, проверьте защищаемое устройство на наличие вредоносных приложений с помощью задачи *Проверка важных областей*.

Чтобы запустить задачу Проверка важных областей, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Проверка по требованию**.
2. В контекстном меню вложенного узла **Проверка важных областей** выберите команду **Запуск**.

Задача будет запущена; в панели результатов отобразится статус задачи **Выполняется**.

Чтобы просмотреть журнал выполнения задачи,

в панели результатов узла **Проверка важных областей** перейдите по ссылке **Открыть журнал выполнения**.

Изменение состава компонентов и восстановление Kaspersky Industrial CyberSecurity for Nodes

Вы можете добавлять или удалять компоненты Kaspersky Industrial CyberSecurity for Nodes. Вам нужно предварительно остановить задачу Постоянная защита файлов, если вы хотите удалить компонент Постоянная защита файлов. В остальных случаях останавливать задачу Постоянная защита файлов или службу Kaspersky Industrial CyberSecurity for Nodes Service не требуется.

Если доступ к управлению приложением защищен паролем, Kaspersky Industrial CyberSecurity for Nodes запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

Чтобы изменить состав компонентов Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. В **Панели управления** Windows выберите **Программы и компоненты**. Откроется окно **Изменение или Удаление**.

2. Выберите **Kaspersky Industrial CyberSecurity for Nodes**, нажмите на правую кнопку мыши и выберите **Изменить**.

   Откроется окно мастера установки приложения **Изменение, восстановление или удаление приложения**.

3. Выберите **Изменение**.

   Откроется окно **Выборочная установка**. Выберите **Полная функциональность** и нажмите на кнопку **Далее >**.

4. В списке доступных компонентов в окне **Выборочная установка** выберите компоненты, которые требуется добавить или удалить из состава Kaspersky Industrial CyberSecurity for Nodes. Для этого выполните следующие действия:

   - Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите:

     - пункт **Компонент будет установлен на локальный жесткий диск**, если требуется установить отдельный компонент;

     - пункт **Компонент и его подкомпоненты будут установлены полностью**, если требуется установить группу компонентов.

   - Чтобы удалить установленные ранее компоненты, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите пункт **Компонент будет недоступен**.

   Нажмите на кнопку **Далее >**.

5. В окне **Подготовка к установке приложения** подтвердите изменение состава компонентов приложения, нажав на кнопку **Установить**.

6. В окне, открывшемся по завершении установки, нажмите на кнопку **Готово**.

   Состав компонентов Kaspersky Industrial CyberSecurity for Nodes будет изменен в соответствии с заданными параметрами.

Если в работе Kaspersky Industrial CyberSecurity for Nodes возникли проблемы (Kaspersky Industrial CyberSecurity for Nodes завершается аварийно, задачи завершаются аварийно или не запускаются), можно попробовать восстановить Kaspersky Industrial CyberSecurity for Nodes. Вы можете выполнить восстановление с сохранением текущих значений параметров Kaspersky Industrial CyberSecurity for Nodes или выбрать режим, при котором все параметры Kaspersky Industrial CyberSecurity for Nodes примут значения по умолчанию.

Чтобы восстановить Kaspersky Industrial CyberSecurity for Nodes после аварийного завершения работы приложения или задач, выполните следующие действия:

1. В **Панели управления** Windows выберите **Программы и компоненты**. Откроется окно **Изменение или Удаление**.

2. Выберите **Kaspersky Industrial CyberSecurity for Nodes**, нажмите на правую кнопку мыши и выберите **Изменить**.

3. Откроется окно мастера установки приложения **Изменение, восстановление или удаление приложения**.

4. Выберите вариант **Восстановление**.

   Откроется окно **Восстановление Kaspersky Industrial CyberSecurity for Nodes**. Нажмите на кнопку **Далее >**.

5. Подождите пока завершится операция восстановления и в открывшемся окне нажмите на кнопку **Готово.**

   Приложение Kaspersky Industrial CyberSecurity for Nodes будет восстановлено с указанными параметрами.

Удаление с помощью мастера установки

В этом разделе приведены инструкции по удалению Kaspersky Industrial CyberSecurity for Nodes и Консоли приложения с защищаемого устройства с помощью мастера установки/удаления.

Удаление Kaspersky Industrial CyberSecurity for Nodes

Файлы дампа и трассировки не удаляются при удалении Kaspersky Industrial CyberSecurity for Nodes. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки.

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Industrial CyberSecurity for Nodes с защищаемого устройства с помощью мастера установки/удаления.

После удаления Kaspersky Industrial CyberSecurity for Nodes с защищаемого устройства может потребоваться перезагрузка. Перезагрузку можно отложить.

Удаление, восстановление и установка приложения через панель управления Windows невозможны.

Kaspersky Industrial CyberSecurity for Nodes запрашивает ввод учетных данных пользователя при попытке удаления или изменения состава программных компонентов в мастере установки. Вам необходимо ввести учетные данные пользователя с соответствующими правами. Если для учетной записи пользователя, от имени которого выполняется удаление, установлен пустой пароль Windows, необходимо до выполнения удаления отключить функцию **Запрашивать пароль для подтверждения критических действий**.

Чтобы удалить Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. В **Панели управления** Windows выберите **Программы и компоненты**. Откроется окно **Изменение или Удаление**.
2. Выберите **Kaspersky Industrial CyberSecurity for Nodes**, нажмите на правую кнопку мыши и выберите **Изменить**.
3. Откроется окно мастера установки приложения **Изменение, восстановление или удаление приложения**.
4. Выберите пункт **Удаление**.

   Откроется окно **Сохранение объектов**.
5. Если требуется, в окне **Сохранение объектов** выполните следующие действия:

   В блоке **Сохранение объектов** укажите какие объекты или настройки необходимо сохранить. По умолчанию флажки сняты.

   - Установите флажок **Информация об активации**.
   - Установите флажок **Файлы резервного хранилища**.
   - Установите флажок **Настройки работы приложения**.

   В блоке **Экспорт объектов** укажите какие объекты необходимо экспортировать. По умолчанию флажки сняты.

   - Установите флажок **Экспортировать объекты на карантине**, чтобы приложение Kaspersky Industrial CyberSecurity for Nodes экспортировало объекты, помещенные на карантин. По умолчанию флажок снят.
   - Установите флажок **Экспортировать объекты резервного хранилища**, чтобы экспортировать объекты из резервного хранилища Kaspersky Industrial CyberSecurity for Nodes. По умолчанию флажок снят.
   - Нажмите на кнопку **Сохранить** и укажите папку, в которую требуется экспортировать объекты. По умолчанию экспорт объектов осуществляется в папку %ProgramData%\Kaspersky Lab\KICS.5.0\QB.

     Нажмите на кнопку **Далее**.

6. В окне **Подтверждение удаления приложения** подтвердите удаление, нажав на кнопку **Удалить**.
7. В окне, открывшемся по завершении удаления, нажмите на кнопку **Готово**.

Приложение Kaspersky Industrial CyberSecurity for Nodes будет удалено с защищаемого устройства.

Удаление Консоли Kaspersky Industrial CyberSecurity for Nodes

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Консоль приложения с защищаемого устройства с помощью мастера установки/удаления.

После удаления Консоли приложения перезагрузка защищаемого устройства не требуется.

Чтобы удалить Консоль приложения, выполните следующие действия:

1. В **Панели управления** Windows выберите **Программы и компоненты**. Откроется окно **Изменение или Удаление.**
2. Выберите Консоль **Kaspersky Industrial CyberSecurity for Nodes**, нажмите на правую кнопку мыши и выберите **Изменить**.

   Откроется окно мастера **Изменение, восстановление или удаление приложения**.
3. Выберите пункт **Удаление.**

   Откроется окно **Подтверждение удаления приложения**. Нажмите на кнопку **Удалить**.
4. В окне, открывшемся по завершении удаления, нажмите на кнопку **ОК**.

Операция удаления будет завершена; окно мастера установки будет закрыто.

Установка и удаление приложения из командной строки

Этот раздел содержит описание особенностей установки и удаления Kaspersky Industrial CyberSecurity for Nodes из командной строки, примеры команд для установки и удаления Kaspersky Industrial CyberSecurity for Nodes из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Industrial CyberSecurity for Nodes из командной строки.

Об установке и удалении Kaspersky Industrial CyberSecurity for Nodes из командной строки

Файлы дампа и трассировки не удаляются при удалении Kaspersky Industrial CyberSecurity for Nodes. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки.

Вы можете установить или удалить Kaspersky Industrial CyberSecurity for Nodes, а также добавить или удалить его компоненты, запустив файл инсталляционного пакета \exec\kics_win.msi из командной строки и указав параметры установки с помощью ключей.

Вы можете установить Консоль Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве или на другом устройстве в сети, чтобы работать с приложением локально или удаленно. Для этого используйте пакет установки \client\kicstools.msi.

Выполняйте установку с правами учетной записи, входящей в группу администраторов на защищаемом устройстве, на котором установлено приложение.

Если вы запустите на защищаемом устройстве файл \exec\kics_win.msi без дополнительных ключей, Kaspersky Industrial CyberSecurity for Nodes будет установлен с параметрами установки по умолчанию.

Вы можете задать набор устанавливаемых компонентов с помощью ключа ADDLOCAL, перечислив в качестве его значений коды выбранных компонентов или наборов компонентов.

Коды программных компонентов Kaspersky Industrial CyberSecurity for Nodes для службы установщика Windows

Файл \exec\kics_win.msi предназначен для установки Kaspersky Industrial CyberSecurity for Nodes.

Файл \client\kicstools.msi предназначен для установки Консоли Kaspersky Industrial CyberSecurity for Nodes.

В таблице ниже содержатся коды и описание программных компонентов Kaspersky Industrial CyberSecurity for Nodes.

Описание программных компонентов Kaspersky Industrial CyberSecurity for Nodes

Компонент	Код	Функции компонента
Постоянная защита файлов	`FileThreatProtection`	Этот компонент выполняет антивирусную проверку файлов на защищаемом устройстве при обращении к этим файлам.
AMSI-защита	`AMSI`	Этот компонент предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. Интерфейс Antimalware Scan Interface (AMSI) позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Industrial CyberSecurity for Nodes для дополнительной проверки и получать результаты проверки этих объектов.
Защита от шифрования	`BehaviorDetection`	Этот компонент вносит в список заблокированных узлов имена удаленных устройств, проявляющих вредоносную активность.

Компонент	Код	Функции компонента
Защита от эксплойтов	`ExploitPrevention`	Этот компонент обеспечивает управление параметрами защиты процессов в памяти устройства.
Откат вредоносных действий	`RemediationEngine`	Этот компонент позволяет Kaspersky Industrial CyberSecurity for Nodes отменять действия, произведенные вредоносными приложениями в операционной системе.
Сетевой экран	`Firewall`	Этот компонент предоставляет возможность управления брандмауэром Windows через графический интерфейс Kaspersky Industrial CyberSecurity for Nodes.
Защита от сетевых угроз	`NetworkThreatProtection`	Этот компонент выполняет проверку входящего сетевого трафика на наличие активности, характерной для сетевых атак. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, Kaspersky Industrial CyberSecurity for Nodes блокирует сетевую активность со стороны атакующего компьютера.
Контроль запуска программ	`ApplicationControl`	Этот компонент отслеживает попытки запуска программ пользователями и разрешает или запрещает их в соответствии с заданными правилами контроля запуска программ.
Контроль устройств	`DeviceControl`	Этот компонент отслеживает попытки подключения внешних устройств к защищаемому устройству и запрещает или разрешает их использование в соответствии с заданными правилами контроля устройств.
Модуль интеграции с Агентом администрирования Kaspersky Security Center	`AdminKitConnector`	Этот компонент обеспечивает связь Kaspersky Industrial CyberSecurity for Nodes с Агентом администрирования Kaspersky Security Center. Вы можете установить этот компонент на защищаемом устройстве, если вы планируете управлять приложением через Kaspersky Security Center.
Анализ журналов	`LogInspector`	Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.
Контроль целостности системы	`SystemIntegrityMonitor`	Этот компонент включает в себя все функции Мониторинга файловых операций, а также позволяет контролировать изменения в реестре и подключение внешних устройств.
Endpoint Detection and Response (Industrial CyberSecurity)	`EDR`	Компонент обеспечивает интеграцию с решением Kaspersky Industrial CyberSecurity Endpoint Detection and Response.
Endpoint Detection and Response Expert (on-premises)	`AntiAPT`	Компонент обеспечивает интеграцию с решением Endpoint Detection and Response, который входит в состав решения Kaspersky Anti Targeted Attack Platform.
Защита от атак BadUSB	`BadUSBAttackPrevention`	Компонент позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.
Managed Detection and Response	`MDR`	Компонент обеспечивает интеграцию с решением Kaspersky Managed Detection and Response.
Интеграция с KICS for Networks	`KicsForNetworks`	Компонент обеспечивает интеграцию с решением Kaspersky Industrial CyberSecurity for Networks.
Portable Auditor	`PortableScanner`	Этот компонент позволяет выполнять проверку изолированных устройств на присутствие вирусов и других программ, представляющих угрозу, записывать входящий и исходящий трафик проверяемых устройств в течение указанного времени и выполнять аудит безопасности устройств.
Получение данных о проектах ПЛК	`KicsPlcFeature`	Этот компонент позволяет получать данные об актуальных проектах ПЛК, используемых в промышленной сети.
Проверка целостности проектов ПЛК	`KicsPlcFeature`	Этот компонент позволяет проверять целостность проектов ПЛК, используемых в промышленной системе.
Проверка по требованию	`Ods`	Этот компонент устанавливает системные файлы Kaspersky Industrial CyberSecurity for Nodes и файлы, реализующие задачи проверки по требованию (проверка объектов защищаемого устройства, выполняемая по требованию).
Использование KSN	`Ksn`	Этот компонент обеспечивает защиту на основе облачных технологий "Лаборатории Касперского". Компонент реализует отправку запросов и получение заключений от службы Kaspersky Security Network.

Компонент	Код	Функции компонента
Обнаружение аномалий с помощью Sigma-правил	`SigmaMonitoring`	Этот компонент анализирует данные внутренних событий и журналов событий на предмет аномалий с помощью Sigma-правил.
Интеграция с SIEM	`SiemTelemetry`	Компонент позволяет настроить интеграцию с SIEM-сервером.

Настройки установки и восстановления приложения и ключи командной строки для службы установщика Windows

В этом разделе описаны настройки для установки и восстановления Kaspersky Industrial CyberSecurity for Nodes. В разделе также указаны ключи для изменения настроек установки и возможные значения этих ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды `msiexec` службы установщика Windows при установке Kaspersky Industrial CyberSecurity for Nodes из командной строки.

Настройки установки и ключи командной строки для установщика Windows

- Согласие с условиями Лицензионного соглашения.

  Возможны следующие значения ключа командной строки `EULA=<value>`:

  - `0` – вы отклоняете условия Лицензионного соглашения (значение по умолчанию).
  - `1` – вы принимаете условия Лицензионного соглашения.

- Согласие с условиями Политики конфиденциальности.

  Возможны следующие значения ключа командной строки `PRIVACYPOLICY=<value>`:

  - `0` – вы отклоняете условия Политики конфиденциальности (значение по умолчанию).
  - `1` – вы принимаете условия Политики конфиденциальности.

- Выбор режима использования приложения.

  Возможны следующие значения ключа командной строки `STANDALONEMODE=<value>`:

  - `0` – Полная функциональность (значение по умолчанию);
  - `1` – Endpoint Agent.

- Папка, в которую будут сохранены файлы Kaspersky Industrial CyberSecurity for Nodes при установке. Вы можете указать другую папку.

Значение по умолчанию для ключа командной строки `INSTALLDIR=<full path to the folder>`:

- В Microsoft Windows 32-разрядных версий:
  - Kaspersky Industrial CyberSecurity for Nodes: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0
  - Консоль Kaspersky Industrial CyberSecurity for Nodes: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console 5.0.0
- В Microsoft Windows 64-разрядных версий: %ProgramFiles(x86)% и далее аналогично путям для 32-разрядных версий Microsoft Windows.

- Запуск задачи *Постоянная защита файлов* сразу после запуска Kaspersky Industrial CyberSecurity for Nodes.

  Возможны следующие значения ключа командной строки `RUNRTP=<value>`:

  - `1` – запустить (значение по умолчанию).
  - `0` – не запускать.

- Режим работы задачи *Постоянная защита файлов*.

  Возможны следующие значения ключа командной строки `RTP_BLOCKING=<value>`:

  - `1` – Рекомендуемый (значение по умолчанию).
  - `0` – Информировать.

- Добавление процессов и файлов промышленных программ в списки доверенных процессов и исключений, а также настройка правил Контроля запуска программ. Процессы и файлы добавляются в исключения с помощью ключа командной строки `ADDEXCLUSION=<exclusion profile name 1>;<exclusion profile name 2>;...;<exclusion profile name n>`. Имена поддерживаемых профилей исключений перечислены по ссылке.

- Путь к файлу ключа (`LICENSEKEYPATH`). По умолчанию установщик Windows пытается найти файл с расширением .key в папке \exec комплекта поставки. Если в папке \exec имеется несколько файлов ключа, установщик Windows выбирает файл ключа с самой поздней датой истечения срока действия. Можно предварительно сохранить файл ключа в папке \exec или указать другой путь к файлу ключа с помощью параметра `LICENSEKEYPATH`.

  Возможны следующие значения ключа командной строки `LICENSEKEYPATH`:

  - Полный путь к файлу ключа с его названием.
  - Путь к папке, в которой хранятся файлы ключа.

  Вы можете добавить ключ после установки Kaspersky Industrial CyberSecurity for Nodes с помощью выбранного вами средства администрирования, например, через Консоль приложения. Если вы не добавите ключ во время установки приложения, после установки Kaspersky Industrial CyberSecurity for Nodes не будет функционировать.

- Путь к конфигурационному файлу. Kaspersky Industrial CyberSecurity for Nodes импортирует параметры из указанного конфигурационного файла, созданного в приложении. Kaspersky Industrial CyberSecurity for Nodes не импортирует из конфигурационного файла пароли, например пароли учетных записей для запуска задач или пароли для соединения с прокси-сервером. После импорта параметров вам нужно ввести все пароли вручную. Если вы не укажете конфигурационный файл, после установки приложение начнет работать с параметрами по умолчанию.

  Значение по умолчанию для параметра `CONFIGPATH=<configuration file name>` не указано.

- Режим задачи *Проверка при старте операционной системы* (`SCANSTARTUP_BLOCKING`). Если установка Kaspersky Industrial CyberSecurity for Nodes выполнялась без ключа `SCANSTARTUP_BLOCKING`, параметру **Область проверки** в задаче *Проверка при старте операционной системы* назначаются следующие значения:

  - Действия над зараженными и другими обнаруженными объектами: **Информировать**.
  - Действия над возможно зараженными объектами: **Информировать**.

  Если установка Kaspersky Industrial CyberSecurity for Nodes выполнялась с использованием ключа `SCANSTARTUP_BLOCKING`, параметру **Область проверки** в задаче *Проверка при старте операционной системы* назначаются следующие значения:

  - Действия над зараженными и другими обнаруженными объектами: **Выполнять рекомендуемое действие**.
  - Действия над возможно зараженными объектами: **Выполнять рекомендуемое действие**.

  Задача *Проверка при старте операционной системы* создается автоматически. По умолчанию применяется режим **Информировать**. В этом случае после развертывания Kaspersky Industrial CyberSecurity for Nodes на устройствах можно включить задачу *Проверка при старте операционной системы*, если во время проверки не было обнаружено проблем с сервисами операционной системы. Если приложение определяет, что критические сервисы операционной системы являются зараженными или возможно зараженными, режим **Информировать** позволяет выяснить причину и решить проблему. Если приложение применяет режим **Выполнять рекомендуемое действие**, выполняется действие **Лечить. Удалять, если не удалось вылечить**, лечение или удаление системных файлов могут привести к критическим проблемам при запуске операционной системы.

- Настройка функции Защита сервисов операционной системы.

  Если эта функция включена, сторонние приложения не могут совершать действия в отношении процессов операционной системы. Возможны следующие значения ключа командной строки `PROTECTOSSERVICES=<value>`:

  - `1` – защита сервисов операционной системы включена (значение по умолчанию);
  - `0` – защита сервисов операционной системы выключена.

- Настройка портов, используемых для удаленного подключения Консоли приложения к компьютеру с установленным приложением.

  Порт для подключения с учетными данными Windows настраивается с помощью ключа `UIPORT=<port number>`. Диапазон возможных номеров порта: 1 – 65535. Если задан номер, выходящий за границы указанного интервала, используется номер порта по умолчанию. Значение по умолчанию – 13032.

При необходимости вы можете закрыть порт для подключения с учетными данными вручную созданных пользователей с помощью ключа `ENABLEUIKLPORT=<value>`:

- `1` – порт открыт (значение по умолчанию);
- `0` – порт закрыт.

Значение по умолчанию для данного порта – 13031. Вы можете изменить номер порта с помощью ключа `UIKLPORT=<port>`. Диапазон возможных номеров порта: 1 – 65535.

- Параметр включения сетевых соединений для удаленного управления Kaspersky Industrial CyberSecurity for Nodes с помощью Консоли приложения, установленной на другом компьютере.

  Возможны следующие значения ключа командной строки `ADDWFEXCLUSION=<value>`:

  - `1`. Если указано это значение, в брандмауэре Windows будут открыты TCP-порты, заданные для удаленного подключения Консоли приложения к компьютеру с установленным приложением (ключи `UIPORT=<port>` и `UIKLPORT=<port>`), и разрешены сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Industrial CyberSecurity for Nodes – avp.exe.

    Читайте также о дополнительной настройке при установке приложения на другое устройство.

  - `0`. Если указано это значение, ничего не происходит.

- Выключение проверки на наличие несовместимого программного обеспечения. Используйте этот параметр, чтобы включить или выключить проверку на наличие несовместимого программного обеспечения при установке приложения на защищаемое устройство в фоновом режиме. Независимо от значения данного параметра, при установке Kaspersky Industrial CyberSecurity for Nodes приложение всегда предупреждает о других версиях приложения, установленных на этом же защищаемом устройстве.

  Возможны следующие значения ключа командной строки `SKIPPRODUCTCHECK=<value>` (также вы можете использовать ключ `SKIPINCOMPATIBLESW=<value>`):

  - `0` – выполняется проверка на несовместимое программное обеспечение (значение по умолчанию).
  - `1` – проверка на наличие несовместимого программного обеспечения не выполняется.

- Выключение автоматического удаления несовместимого программного обеспечения.

  Если передан ключ `SKIPPRODUCTUNINSTALL=1`, Kaspersky Industrial CyberSecurity for Nodes не удаляет несовместимое программное обеспечение. Если значение не передано, Kaspersky Industrial CyberSecurity for Nodes автоматически пытается удалить несовместимое программное обеспечение.

  > При установке Kaspersky Industrial CyberSecurity for Nodes с помощью установщика msiexec удаление несовместимого ПО не выполняется. Для автоматического удаления ПО, с которым могут быть проблемы совместимости, используйте файл setup_kics.exe.

- Создание уникального идентификатора компьютера (Sensor ID) при установке или обновлении приложения.

Sensor ID используется в решении Kaspersky Anti Targeted Attack Platform для идентификации компьютеров, которые отправляют телеметрию на сервер. При создании Sensor ID приложение использует алгоритм, который учитывает конфигурацию компьютера, например, серийный номер материнской платы. В некоторых случаях, например, при использовании приложения в виртуальной среде, Sensor ID может повторяться. Таким образом, Kaspersky Anti Targeted Attack Platform не может идентифицировать компьютер, с которого отправлена телеметрия. Для создания уникального Sensor ID вам нужно задать параметр `ENABLEUNIQUESENSORID=1`. В результате приложение будет использовать другой алгоритм для создания Sensor ID, который учитывает другие данные о компьютере. Это позволяет обеспечить уникальность Sensor ID.

По умолчанию параметр не задан. Приложение наследует Sensor ID в следующих случаях:

- обновление версии приложения;
- миграция конфигурации [KICS+KEA] на [KICS+встроенный агент].

При восстановлении приложения установщик пытается наследовать Sensor ID. Если восстановить Sensor ID не удалось, приложение создает новый Sensor ID.

- Выключение проверки установленного обновления операционной системы KB5007186.

  После установки обновления KB5007186 приложение продолжает работать в прежнем режиме, безопасность системы не нарушается, но становится недоступным минорное обновление версии приложения. Перед установкой приложения установщик проверяет наличие установленных обновлений операционной системы. Обнаружив обновление KB5007186, установщик останавливает установку приложения. Используйте ключ командной строки `SKIPKB5007186CHECK`, чтобы выключить или включить проверку установщиком наличия обновления операционной системы KB5007186.

  Возможны следующие значения ключа командной строки `SKIPKB5007186CHECK=<value>`:

  - `0` – установщик проверяет наличие установленного обновления операционной системы KB5007186;
  - `1` – установщик не проверяет наличие установленного обновления операционной системы KB5007186.

  По умолчанию значение ключа не задано, что соответствует значению `0`.

- Пропуск установки корневого сертификата DigiCert Assured ID Root CA в хранилище доверенных корневых сертификатов ОС.

  Если при установке приложения передан ключ `SKIPINSTALLROOTCACERTIFICATES`, корневой сертификат DigiCert Assured ID Root CA не устанавливается. По умолчанию сертификат устанавливается автоматически из инсталляционного пакета приложения.

- Настройка блокировки доступа к съемным дискам Рутокен. Если блокировка включена, на устройстве с установленным приложением пользователю доступны только создание Portable Auditor и выполнение задач *Безопасное копирование баз приложения* и *Безопасное обновление баз приложения*, доступ к защищенному съемному диску стандартными средствами операционной системы заблокирован.

  Возможны следующие значения ключа командной строки `TOKENPROTECTION=<value>`:

  - `0` – блокировка отключена (значение по умолчанию);
  - `1` – блокировка включена.

Настройки восстановления и ключи командной строки для установщика Windows

- Восстановление содержимого карантина.

Возможны следующие значения ключа командной строки `RESTOREQTN=<value>`:

- `0` – удалить содержимое карантина (значение по умолчанию).
- `1` – восстановить содержимое карантина в папку, указанную в качестве значения параметра `RESTOREPATH`, во вложенную подпапку `\QB`.

- Восстановление содержимого резервного хранилища.

  Возможны следующие значения ключа командной строки `RESTOREBCK=<value>`:

  - `0` – удалить содержимое резервного хранилища (значение по умолчанию).
  - `1` – восстановить содержимое резервного хранилища в папку, указанную в качестве значения параметра `RESTOREPATH`, во вложенную папку `\QB`.

- Ввод текущего пароля для подтверждения операции восстановления (при включенной функции защиты паролем).

  Значение по умолчанию для ключа `UNLOCK_PASSWORD=<specified password>` не задано.

- Папка для восстановленных объектов. Восстановленные объекты будут сохранены в указанной папке.

  Значение по умолчанию для ключа командной строки `RESTOREPATH=<full path to the folder>` – `%ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KICS.5.0.0\QB\Restored`.

Примеры команд установки Kaspersky Industrial CyberSecurity for Nodes

В этом разделе приведены примеры команд для установки Kaspersky Industrial CyberSecurity for Nodes.

На защищаемом устройстве запускайте файл kics_win.msi из комплекта поставки.

Подробная информация об использовании стандартных команд и ключей установщика Windows содержится в документации, предоставляемой корпорацией Microsoft.

Примеры установки Kaspersky Industrial CyberSecurity for Nodes из файла setup_kics.exe

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с параметрами по умолчанию без взаимодействия с пользователем:

```
\exec\setup_kics.exe EULA=1 PRIVACYPOLICY=1
```

Чтобы установить компоненты, например Контроль устройств:

```
\exec\setup_kics.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0
```

При установке Kaspersky Industrial CyberSecurity for Nodes на компьютеры с сетевыми устройствами и SCSI-устройствами, вызывающими сбой системы после установки приложения, с этой командой можно использовать следующие дополнительные ключи:

```
/p SKIP_NETWORK_UPPERFILTERS=<1|0>
```

Включает (1) или выключает (0) перехват соединений сетевых адаптеров.

```
/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>
```

Включает (1) или выключает (0) перехват соединений SCSI-адаптеров.

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes и активировать приложения с помощью файла ключа:

```
setup_kics.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

Чтобы изменить порт, используемый для удаленного подключения Консоли приложения к компьютеру, на котором установлено приложение, с учетными данными пользователей Windows:

```
setup_kics.exe /pUIPORT=<port number>
```

Диапазон возможных номеров порта: 1 – 65535. Значение по умолчанию 13032.

Список команд для установки: запуск msi-файла

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с параметрами по умолчанию без взаимодействия с пользователем:

```
msiexec /i kics_win.msi /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с параметрами по умолчанию и показать интерфейс установки:

```
msiexec /i kics_win.msi /qf EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с рекомендованными параметрами установки и включить ротацию файлов трассировки при достижении ими заданного максимального количества:

```
msiexec /i kics_win.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1 PRIVACYPOLICY=1
```

Параметр `TRACE_FOLDER` является обязательным.

Для параметра `TRACE_MAX_ROLL_COUNT` действуют следующие правила:

- Если параметр указан, включается ротация файлов трассировки при достижении ими максимального количества, указанного в параметре. Доступный диапазон значений параметра: от 1 до 999.
- Если в качестве максимального количества файлов трассировки указано значение 0, ротация файлов трассировки будет отключена.

- Если параметр указан, но его значение недопустимо или превышает диапазон допустимых значений от 1 до 999 файлов, ротация файлов трассировки включается с заданным по умолчанию значением максимального количества файлов трассировки, равным 5.

- Если параметр не указан:

  - Если на устройстве уже настроена ротация файлов трассировки, ее параметры не изменяются. Приложение будет игнорировать вводимые параметры.

  - Если ротация файлов трассировки на устройстве не настроена, параметр ротации будет включен с заданным по умолчанию значением максимального количества файлов трассировки, равным 5.

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes и активировать приложение с помощью файла ключа C:\0000000A.key:

```
msiexec /i kics_win.msi     LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes с предварительной проверкой активных процессов и загрузочных секторов локальных дисков:

```
msiexec /i kics_win.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes в папку установки C:\KICS:

```
msiexec /i kics_win.msi INSTALLDIR=C:\KICS /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes и сохранить файл журнала установки с именем kics.log в папку, где хранится msi-файл Kaspersky Industrial CyberSecurity for Nodes:

```
msiexec /i kics_win.msi/l*v kics.log /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Консоль Kaspersky Industrial CyberSecurity for Nodes:

```
msiexec /i kicstools.msi /qn EULA=1
```

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes и активировать приложение с помощью файла ключа C:\0000000A.key, а также настроить Kaspersky Industrial CyberSecurity for Nodes в соответствии с параметрами в конфигурационном файле C:\settings.xml:

```
msiexec /i kics_win.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить исправление, если приложение Kaspersky Industrial CyberSecurity for Nodes защищено паролем:

```
msiexec /p "<MSP file path>" UNLOCK_PASSWORD=<password>
```

Действия после установки Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes запускает задачи защиты и проверки сразу после установки, если вы активировали приложение. Если во время установки Kaspersky Industrial CyberSecurity for Nodes был установлен флажок **Включить Постоянную защиту файлов после установки приложения (рекомендуется)**, приложение проверяет объекты файловой системы устройства при доступе к ним. Если при выборочной установке был установлен компонент Проверка скриптов, Kaspersky Industrial CyberSecurity for Nodes будет выполнять проверку программного кода всех скриптов при их запуске. Каждую пятницу в 20:00 Kaspersky Industrial CyberSecurity for Nodes выполняет задачу *Проверка важных областей*.

После установки Kaspersky Industrial CyberSecurity for Nodes рекомендуется выполнить следующие действия:

- Запустить задачу обновления Kaspersky Industrial CyberSecurity for Nodes. После установки Kaspersky Industrial CyberSecurity for Nodes проверяет объекты с использованием баз, которые входили в его состав при поставке. Рекомендуется сразу же обновить базы Kaspersky Industrial CyberSecurity for Nodes. Для этого вам нужно запустить задачу *Обновление*. Далее обновление будет выполняться каждый час согласно расписанию, установленному по умолчанию.

  Например, вы можете запустить задачу *Обновление*, выполнив следующую команду:

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
  ```

  При этом обновления баз Kaspersky Industrial CyberSecurity for Nodes будут загружены с серверов обновлений "Лаборатории Касперского".

- Запустить задачу *Проверка важных областей*, если перед установкой Kaspersky Industrial CyberSecurity for Nodes на устройстве не было установлено антивирусное приложение с включенной функцией постоянной защиты файлов.

  Вы можете запустить задачу *Проверка важных областей* с помощью командной строки, выполнив следующую команду:

  ```
  KAVSHELL SCANCRITICAL /W:scancritical.log
  ```

  Эта команда сохраняет журнал выполнения задачи в файле scancritical.log в текущей папке.

- Настроить уведомления администратора о событиях Kaspersky Industrial CyberSecurity for Nodes.

Добавление и удаление компонентов. Примеры команд

Компонент Проверка по требованию устанавливается автоматически. Вам не нужно указывать его в списке значений ключа ADDLOCAL, добавляя или удаляя компоненты Kaspersky Industrial CyberSecurity for Nodes.

Чтобы добавить компонент Контроль запуска программ к ранее установленным компонентам, выполните следующую команду:

```
msiexec /i kics_win.msi ADDLOCAL=Oas,AppCtrl /qn
```

или

```
\exec\setup_kics.exe /s /p ADDLOCAL=Oas,AppCtrl
```

Если вы перечислите не только компоненты, которые требуется установить, но и уже установленные компоненты, Kaspersky Industrial CyberSecurity for Nodes переустановит указанные установленные компоненты.

Чтобы удалить установленные компоненты, выполните следующую команду:

```
msiexec /i kics_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,Bases,Core,CoreBLFiles,CoreFolders,CoreWPFiles,DevCtrl,Driver
ADD_ADV=IDS,RegMonitor REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Удаление Kaspersky Industrial CyberSecurity for Nodes. Примеры команд

Чтобы удалить Kaspersky Industrial CyberSecurity for Nodes с защищаемого устройства в тихом режиме, выполните следующую команду:

```
msiexec /x kics_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

или

```
msiexec /x {DF1C0C50-2E34-4B22-A07D-133E3DC961C7} KLLOGIN=<user name> KLPASSWD=<password> /qn
```

или

```
setup_kics.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

где `<user name>` – имя и логин пользователя с необходимыми для удаления правами.

Если для учетной записи пользователя, от имени которого выполняется удаление, установлен пустой пароль Windows, необходимо до выполнения удаления отключить функцию **Запрашивать пароль для подтверждения критических действий**.

Чтобы удалить Консоль Kaspersky Industrial CyberSecurity for Nodes в тихом режиме, выполните следующую команду:

```
msiexec /x kicstools.msi /qn
```

или

```
msiexec /x {5209F134-35AD-4A12-85B9-257FA5B52917} /qn
```

Коды возврата

Установщик приложения может возвращать коды возврата, описанные в этой статье.

В таблице ниже приведено описание кодов возврата командной строки.

Коды возврата

Код	Описание
27100	На компьютере обнаружены диски с установленным тестовым Агентом аутентификации.
27101	На компьютере обнаружены диски с установленным тестовым Агентом аутентификации.
27102	Ошибка при поиске зашифрованных дисков.
27200	Невозможно выгрузить приложение из оперативной памяти.
27201	Ошибка при старте процесса avp.exe. Возможно ваш компьютер заражен.
27204	Ошибка при кешировании пакета установки.
27205	Ошибка при миграции информации о лицензии.
27206	Ошибка при удалении информации о лицензии.
27207	Ошибка при удалении несовместимого ПО.
27208	Ошибка при проверке ПО на совместимость.
27209	Ошибка при распаковке архива.
27210	Ошибка при настройке самозащиты.
27211	Ошибка при включении самозащиты.
27212	Невозможно определить информацию о версии операционной системы.
27213	Ошибка при определении папки запуска.
27214	Ошибка при проверке папки установки.
27215	Ошибка при настройке службы.
27216	Ошибка при подготовке обновления библиотеки klcp.
27217	Ошибка при обновлении библиотеки klcp.
27218	Ошибка при настройке параметров драйвера kl1.
27219	Ошибка при настройке драйвера klelam.
27220	Ошибка при настройке драйвера klwfp.
27221	Ошибка при настройке совместимости драйверов.
27222	Ошибка при удалении ключей реестра.
27223	Ошибка при попытке перезапуска системы.
27224	Ошибка при установке драйверов.
27225	Ошибка при миграции настроек драйверов.
27226	Ошибка при остановке драйвера.
27227	Ошибка при блокировке старта драйвера.
27228	Ошибка при проверке подписи файла.
27230	Ошибка при подготовке настроек драйвера kldl.
27231	Ошибка при конфигурировании настроек драйвера kldl.
27300	Ошибка при установке драйвера.

Код	Описание
27301	Ошибка при удалении драйвера.
27302	Ошибка при установке сетевых компонентов.
27303	Регистрационная информация для драйвера не соответствует или неполная. Пожалуйста, перезагрузите операционную систему и попробуйте еще раз.
27305	Ошибка при отключении драйвера.
27310	Не удалось установить файл каталога, подписанный цифровой подписью.
27311	Не удалось удалить файл каталога, подписанный цифровой подписью.
27312	Не удалось установить сертификаты.
27313	Не удалось удалить сертификаты.
27320	Ошибка при настройке службы.
27321	Ошибка при снятии защиты с службы.
27350	Патч <имя патча> не предназначен для локализации приложения <имя приложения>.
27352	Патч для полнодискового шифрования не может быть удален.
27353	Патч <имя патча 1> может быть установлен только совместно с патчем <имя патча 2>.
27354	Необходимо перезагрузить компьютер для применения патчей перед изменением/восстановлением приложения.
27355	Не удалось заблокировать управление полнодисковым шифрованием. Необходимо завершить шифрование, чтобы установить обновление для полнодискового шифрования.
27356	Невозможно установить патч.
27357	В пакете установки обнаружены отозванные патчи. Установка будет прервана.
27360	Невозможно зарегистрировать патч.
27361	Ошибка при выставлении свойств установки патча.
27363	Патч содержит библиотеки шифрования, несовместимые с установленными.
27370	Ошибка при подготовке к распаковке .NET 8.0.
27371	Ошибка распаковки .NET 8.0.
27372	Удалена регистрационная информация о предыдущей версии приложения. Пожалуйста, перезапустите установку приложения.
27373	Ошибка при удалении регистрационной информации о предыдущей версии приложения.
27374	Приложение обновляется. Пожалуйста, попробуйте позже.
27375	Пароль или имя пользователя для удаления приложения не заданы либо неверны.
27376	Не удается удалить Kaspersky Endpoint Agent. Пожалуйста, удалите его самостоятельно или снимите в настройках пароль для удаления. После этого запустите установку приложения еще раз.
27377	Не удается удалить Kaspersky Security для Windows Server. Пожалуйста, удалите его самостоятельно или снимите в настройках пароль для удаления. После этого запустите установку приложения еще раз.
27378	Недостаточно места на диске.
27379	Не удалось установить приложение, так как выбраны несовместимые компоненты. Пожалуйста, измените набор компонентов и запустите установку еще раз.
27380	Выбран недопустимый файл конфигурации.
27381	Выбран недопустимый лицензионный ключ.
27382	Ошибка при создании группы администрирования приложения.
27383	Вы выбрали неверную папку. Название папки для установки приложения не должно превышать ограничение в 160 символов.
27384	Вы выбрали неверную папку или диск. Приложение должно быть установлена на локальный жесткий диск.
27385	Вы выбрали неверную папку. Приложение не может быть установлено в корневую папку.
27386	Вы выбрали неверную папку. Приложение не может быть установлено в папку 'Windows' или вложенные в нее папки.
27387	Вы выбрали неверную папку. Приложение не может быть установлено в папку, в которую вложена папка 'Temp'.

Код	Описание
27388	Вы выбрали неверную папку. Приложение не может быть установлено непосредственно в папку 'Program Files'.
27389	Вы выбрали неверную папку. Приложение не может быть установлено на виртуальный диск.
27390	Вы выбрали неверную папку или диск. Приложение не может быть установлено в папку, куда была установлена предыдущая версия приложения.
27391	Вы выбрали папку или диск, где уже есть файлы. Приложение не может быть установлено в папку, где уже есть файлы, так как после включения функции "Самозащита" могут возникнуть проблемы с доступом к этим файлам.
27392	Приложение не может быть установлено в папку, содержащую точки повторной обработки (Reparse Points). Пожалуйста, выберите другую папку для установки приложения.
27393	Приложение не может быть установлено в папку, в названии которой используется ';'. Пожалуйста, выберите другую папку для установки приложения.
27394	Вы выбрали неверную папку. Недопустимо указывать корневую папку.
27395	Вы выбрали неверную папку. Недопустимо указывать папку 'Windows' или вложенные в нее папки.
27396	Вы выбрали неверную папку. Недопустимо указывать непосредственно папку 'Program Files'.
27397	Вы выбрали неверную папку. Недопустимо указывать папку, в которую вложена папка 'Temp'.
27400	Ошибка при подготовке файлов к обновлению.
27450	Cab-файл не может быть установлен.
27451	Ошибка при удалении.
27452	Ошибка при удалении файлов.
27453	Ошибка при перемещении файлов.
27454	Невозможно создать файлы реестра.
27455	Невозможно определить информацию о версии операционной системы.
27456	Невозможно запланировать восстановление значений реестра.
27457	Невозможно получить хорошо известные идентификаторы безопасности (SIDs).
27460	Ошибка при создании дескрипторов защиты.
27461	Ошибка при восстановлении дескрипторов защиты.
27462	Не удалось создать правила для сетевого экрана Microsoft Windows.
27463	Не удалось удалить правила для сетевого экрана Microsoft Windows.

Установка и удаление приложения с помощью Kaspersky Security Center

Этот раздел содержит информацию об установке Kaspersky Industrial CyberSecurity for Nodes с помощью Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center, а также описание действий после установки Kaspersky Industrial CyberSecurity for Nodes.

Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки приложение Kaspersky Industrial CyberSecurity for Nodes будет установлено с одинаковыми параметрами на несколько защищаемых устройств.

Можно объединить все защищаемые устройства в одну группу администрирования и создать групповую задачу установки Kaspersky Industrial CyberSecurity for Nodes на защищаемые устройства этой группы.

Вы можете создать задачу удаленной установки Kaspersky Industrial CyberSecurity for Nodes для набора защищаемых устройств, не объединенных в одну группу администрирования. При создании этой задачи нужно сформировать список отдельных защищаемых устройств, на которые вы хотите установить Kaspersky Industrial CyberSecurity for Nodes.

Подробная информация о задаче удаленной установки приведена в справке Kaspersky Security Center.

Права для установки или удаления Kaspersky Industrial CyberSecurity for Nodes

Учетная запись, которую вы укажете в задаче удаленной установки (удаления), должна входить в группу администраторов на каждом из защищаемых устройств во всех случаях, кроме следующих ситуаций:

- На защищаемых устройствах, на которых вы хотите установить Kaspersky Industrial CyberSecurity for Nodes, уже установлен Агент администрирования Kaspersky Security Center (независимо от того, в каком домене находятся защищаемые устройства и принадлежат ли они к какому-либо домену).

  Если Агент администрирования еще не установлен на защищаемых устройствах, вы можете установить его вместе с Kaspersky Industrial CyberSecurity for Nodes с помощью задачи удаленной установки. Перед установкой Агента администрирования убедитесь, что учетная запись, которую вы укажете в задаче, входит в группу администраторов на каждом защищаемом устройстве.

- Все защищаемые устройства, на которые вы хотите установить Kaspersky Industrial CyberSecurity for Nodes, находятся в одном домене с Сервером администрирования и Сервер администрирования зарегистрирован под учетной записью Администратор домена (**Domain Admin**), если эта учетная запись обладает правами локального администратора на защищаемых устройствах домена.

По умолчанию задача удаленной установки методом **Форсированная установка** запускается с правами той учетной записи, под которой работает Сервер администрирования.

В групповых задачах и в задачах для набора защищаемых устройств, в которых был выбран метод форсированной установки (удаления), учетная запись должна обладать следующими правами на защищаемом устройстве:

- правом на удаленный запуск приложений;
- доступом к папке общего доступа **Admin$**;
- правом **Вход в качестве службы**.

Установка Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center

Установка Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center состоит из следующих этапов:

1. **Создание инсталляционного пакета**

   Инсталляционный пакет – набор файлов, формируемый для удаленной установки приложения "Лаборатории Касперского" при помощи Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения его работоспособности сразу после установки. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива приложения.

Как создать инсталляционный пакет в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Дополнительно → Удаленная установка → Инсталляционные пакеты**.

2. В панели результатов нажмите на кнопку **Создать инсталляционный пакет**.

Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

Шаг 1. Выбор типа инсталляционного пакета

Выберите вариант **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

Шаг 2. Определение имени инсталляционного пакета

Введите имя инсталляционного пакета, например *Kaspersky Industrial CyberSecurity for Nodes*.

Шаг 3. Выбор дистрибутива приложения для установки

Выберите файл kics_win.kud из комплекта поставки Kaspersky Industrial CyberSecurity for Nodes в качестве файла инсталляционного пакета.

При необходимости установите флажок **Скопировать обновления из хранилища в инсталляционный пакет**, чтобы обновить антивирусные базы в инсталляционном пакете.

Шаг 4. Лицензионное соглашение и Политика конфиденциальности

Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения 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(а) и понимаю Политику конфиденциальности**.

Вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности для продолжения установки.

Инсталляционный пакет будет создан и добавлен в Kaspersky Security Center. С помощью инсталляционного пакета вы можете установить Kaspersky Industrial CyberSecurity for Nodes на компьютеры сети организации или обновить версию приложения.

Чтобы изменить набор устанавливаемых компонентов Kaspersky Industrial CyberSecurity for Nodes и настроить параметры по умолчанию в созданном инсталляционном пакете, выполните следующие действия:

1. В Kaspersky Security Center разверните узел **Удаленная установка**.

2. В панели результатов вложенного узла **Инсталляционные пакеты** откройте контекстное меню созданного инсталляционного пакета Kaspersky Industrial CyberSecurity for Nodes и выберите пункт **Свойства**.

3. В окне **Свойства: <название инсталляционного пакета>** перейдите в раздел **Настройка**.

4. Выберите тип установки приложения:

   Если выбрана конфигурация **Установить защиту на основе антивирусных баз**, все компоненты Kaspersky Industrial CyberSecurity for Nodes, кроме компонентов Сетевой экран и Счетчики производительности, включены по умолчанию.

   При установке программы в конфигурации **Установить защиту на основе антивирусных баз** поверх версии программы, в которой не используется сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически расширен за счет добавления следующих компонентов:

   - Постоянная защита файлов.
   - Проверка по требованию.
   - Защита от сетевых угроз.

   > Компоненты, отвечающие за обновления, не входят в конфигурацию **Установить защиту на основе разрешенных списков**.

   Если выбрана конфигурация **Установить защиту на основе разрешенных списков**, то по умолчанию включены следующие компоненты:

   - Защита от эксплойтов.
   - Контроль запуска программ.
   - Значок области уведомлений.

   При установке программы в конфигурации **Установить защиту на основе разрешенных списков** поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов:

   - Постоянная защита файлов.
   - Проверка по требованию.
   - Компоненты, отвечающие за обновления.

   Рекомендуем устанавливать эту конфигурацию для защиты устройств с ограниченными ресурсами. В этом случае вы сможете активировать программу на длительный срок, а компонент Контроль запуска программ обеспечит защиту компьютера.

   - **Полная функциональность**

     По умолчанию все компоненты Kaspersky Industrial CyberSecurity for Nodes, кроме Счетчиков производительности и Endpoint Agent, включены в список рекомендуемых к установке.

     Компонент Поддержка SNMP-протокола Kaspersky Industrial CyberSecurity for Nodes отображается в списке устанавливаемых компонентов, только если на защищаемом устройстве установлена служба SNMP (Microsoft Windows).

- **Endpoint Agent**

  При выборе этого варианта Kaspersky Industrial CyberSecurity for Nodes будет установлен в конфигурации Endpoint Agent. Более подробную информацию о данной конфигурации см. в этом разделе.

5. Укажите список исключений для промышленных систем, нажав на кнопку **Настроить**.

6. В блоке **Выбор компонентов** установите флажки рядом с названиями компонентов Kaspersky Industrial CyberSecurity for Nodes, которые вы хотите установить.

7. В блоке **Режим работы Постоянной защиты файлов** установите флажок **Включить Постоянную защиту файлов после установки приложения** и выберите режим работы компонента.

8. При необходимости измените номера TCP-портов, используемых для удаленного подключения Консоли приложения к компьютеру с установленным приложением.

   Номер порта по умолчанию для подключения с учетными данными Windows – 13032, для подключения с учетными данными вручную созданных пользователей – 13031. Диапазон возможных номеров портов: 1 – 65535.

   Чтобы запретить подключение с учетными данными пользователей, созданных вручную, снимите флажок **С учетными данными вручную созданных пользователей**.

9. Чтобы указать папку назначения, отличную от папки, установленной по умолчанию, укажите имя папки и путь к ней в блоке **Задать пути при установке приложения**, нажав на кнопку **Настройка**.

10. Для установки приложения с заранее заданными параметрами загрузите конфигурационный файл.

11. Сохраните внесенные изменения.

Как создать инсталляционный пакет в Web Console

1. Выполните одно из следующих действий:

   - В главном окне Web Console выберите **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

   - В главном окне Web Console выберите **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов, загруженных в Kaspersky Security Center.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

Шаг 1. Выбор типа инсталляционного пакета

Выберите вариант **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

Мастер создаст инсталляционный пакет из дистрибутива, размещенного на серверах "Лаборатории Касперского". Список обновляется автоматически по мере выпуска новых версий приложений.

Также вы можете создать инсталляционный пакет из файла.

Шаг 2. Инсталляционные пакеты

Выберите инсталляционный пакет Kaspersky Industrial CyberSecurity for Nodes. Запустится процесс создания инсталляционного пакета. Во время создания инсталляционного пакета необходимо принять условия Лицензионного соглашения и Политики конфиденциальности.

Вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности для продолжения установки.

Инсталляционный пакет будет создан и добавлен в Kaspersky Security Center. С помощью инсталляционного пакета вы можете установить Kaspersky Industrial CyberSecurity for Nodes на компьютеры сети организации или обновить версию приложения.

Чтобы изменить набор устанавливаемых компонентов Kaspersky Industrial CyberSecurity for Nodes и настроить параметры по умолчанию в созданном инсталляционном пакете, выполните следующие действия:

1. В окне **Инсталляционные пакеты** нажмите на название созданного инсталляционного пакета Kaspersky Industrial CyberSecurity for Nodes.
2. В открывшемся окне перейдите на вкладку **Параметры**.
3. Выберите раздел **Компоненты защиты**.
4. Выберите тип установки приложения:

   Если выбрана конфигурация **Установить защиту на основе антивирусных баз**, все компоненты Kaspersky Industrial CyberSecurity for Nodes, кроме компонентов Сетевой экран и Счетчики производительности, включены по умолчанию.

   При установке программы в конфигурации **Установить защиту на основе антивирусных баз** поверх версии программы, в которой не используется сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически расширен за счет добавления следующих компонентов:

   - Постоянная защита файлов.
   - Проверка по требованию.
   - Защита от сетевых угроз.

   Компоненты, отвечающие за обновления, не входят в конфигурацию **Установить защиту на основе разрешенных списков**.

   Если выбрана конфигурация **Установить защиту на основе разрешенных списков**, то по умолчанию включены следующие компоненты:

   - Защита от эксплойтов.
   - Контроль запуска программ.
   - Значок области уведомлений.

При установке программы в конфигурации **Установить защиту на основе разрешенных списков** поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов:

- Постоянная защита файлов.
- Проверка по требованию.
- Компоненты, отвечающие за обновления.

Рекомендуем устанавливать эту конфигурацию для защиты устройств с ограниченными ресурсами. В этом случае вы сможете активировать программу на длительный срок, а компонент Контроль запуска программ обеспечит защиту компьютера.

- **Полная функциональность**

  По умолчанию все компоненты Kaspersky Industrial CyberSecurity for Nodes, кроме Счетчиков производительности и Endpoint Agent, включены в список рекомендуемых к установке.

  Компонент Поддержка SNMP-протокола Kaspersky Industrial CyberSecurity for Nodes отображается в списке устанавливаемых компонентов, только если на защищаемом устройстве установлена служба SNMP (Microsoft Windows).

- **Endpoint Agent**

  При выборе этого варианта Kaspersky Industrial CyberSecurity for Nodes будет установлен в конфигурации Endpoint Agent. Более подробную информацию о данной конфигурации см. в этом разделе.

5. Укажите список исключений для промышленных систем, нажав на кнопку **Настроить**.
6. В разделе **Выбор компонентов для установки** установите флажки рядом с названиями компонентов Kaspersky Industrial CyberSecurity for Nodes, которые вы хотите установить.
7. В блоке **Режим работы Постоянной защиты файлов** установите флажок **Включить Постоянную защиту файлов после установки приложения (рекомендуется)** и выберите режим работы компонента.
8. При необходимости измените номера TCP-портов, используемых для удаленного подключения Консоли приложения к компьютеру с установленным приложением.

   Номер порта по умолчанию для подключения с учетными данными Windows – 13032, для подключения с учетными данными вручную созданных пользователей – 13031. Диапазон возможных номеров портов: 1 – 65535.

   Чтобы запретить подключение с учетными данными пользователей, созданных вручную, снимите флажок **Порт для удаленного подключения с учетными данными вручную созданных пользователей**.
9. Выберите раздел **Настройки установки**.

10. В блоке **Дополнительные настройки** настройте параметры:

    - **Добавить путь к приложению в переменную окружения %PATH%**. Вы можете добавить путь установки в переменную %PATH% для удобства управления приложением с помощью командной строки.

    - **Выполнять рекомендуемое действие во время проверки при запуске ОС**. Если флажок установлен, задача *Проверка при старте операционной системы* будет выполняться в режиме **Выполнять рекомендуемое действие**.

    - **Использовать режим пониженного потребления ресурсов Агентом администрирования Kaspersky Security Center**. Режим низкого потребления ресурсов позволяет ограничить использование оперативной памяти Агента администрирования на защищаемом устройстве. По умолчанию режим низкого потребления ресурсов выключен.

    - **Показывать значок в панели задач**. Если флажок установлен, после установки Kaspersky Industrial CyberSecurity for Nodes значок приложения появится в области уведомлений панели задач Microsoft Windows.

11. При необходимости выключите функцию **Защищать процесс установки приложения**.

12. При необходимости измените папки по умолчанию, создаваемые на защищаемом устройстве при установке приложения.

13. Для установки приложения с заранее заданными параметрами нажмите на ссылку **Добавить конфигурационный файл** и загрузите конфигурационный файл.

    При работе с инсталляционными пакетами в Kaspersky Security Center Web Console поддерживается загрузка конфигурационных файлов размером не более 4 МБ. Если вы работаете с инсталляционными пакетами в Консоли администрирования Kaspersky Security Center, такого ограничения нет.

14. Сохраните внесенные изменения.

2 Создание задачи удаленной установки

Для удаленной установки Kaspersky Industrial CyberSecurity for Nodes предназначена задача *Удаленная установка приложения*. Задача *Удаленная установка приложения* позволяет развернуть инсталляционный пакет приложения на все компьютеры организации.

Как создать задачу удаленной установки в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве консоли выберите папку **Задачи**.

   Откроется список задач.

3. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Сервер администрирования Kaspersky Security Center → Удаленная установка приложения**.

Шаг 2. Выбор инсталляционного пакета

В списке инсталляционных пакетов выберите пакет Kaspersky Industrial CyberSecurity for Nodes. Если в списке отсутствует инсталляционный пакет Kaspersky Industrial CyberSecurity for Nodes, вы можете создать пакет в мастере.

Вы можете настроить параметры инсталляционного пакета в Kaspersky Security Center, например, выбрать компоненты приложения, которые будут установлены на компьютер.

Также с Kaspersky Industrial CyberSecurity for Nodes будет установлен Агент администрирования. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

Шаг 3. Дополнительно

Выберите инсталляционный пакет Агента администрирования. Выбранная версия Агента администрирования будет установлена вместе с Kaspersky Industrial CyberSecurity for Nodes.

Шаг 4. Параметры

Настройте следующие дополнительные параметры приложения:

- **Принудительно скачать инсталляционный пакет**. Выберите средства установки приложения:
  - **С помощью Агента администрирования**. Доставку инсталляционного пакета Kaspersky Industrial CyberSecurity for Nodes на клиентские компьютеры выполняет Агент администрирования. Если Агент администрирования не установлен, выполнение задачи завершится ошибкой. В этом случае вам нужно добавить инсталляционный пакет Агента администрирования в задачу *Удаленная установка приложения* и включить доставку файлов средствами операционной системы. Тогда Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Industrial CyberSecurity for Nodes устанавливается средствами Агента администрирования.
  - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.
  - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

- **Поведение устройств, управляемых другими Серверами администрирования**. Выберите способ установки Kaspersky Industrial CyberSecurity for Nodes. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одного и того же приложения на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

- **Не устанавливать приложение, если оно уже установлено**. Снимите этот флажок, если вы хотите, например, установить приложение более ранней версии.

Шаг 5. Выбор параметра перезагрузки операционной системы

Выберите действие, которое будет выполняться, если потребуется перезагрузка компьютера. При установке Kaspersky Industrial CyberSecurity for Nodes перезагрузка не требуется. Перезагрузка требуется, только если перед установкой необходимо удалить несовместимые приложения. Также перезагрузка может потребоваться при обновлении версии приложения.

Шаг 6. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которые будет установлено приложение Kaspersky Industrial CyberSecurity for Nodes. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.

- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. На нераспределенных устройствах не установлен Агент администрирования. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 7. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Industrial CyberSecurity for Nodes средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 8. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 9. Определение названия задачи

Введите название задачи, например, *Установка Kaspersky Industrial CyberSecurity for Nodes для Windows 5.0*.

Шаг 10. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. Установка приложения будет выполнена в тихом режиме. После установки в области уведомлений компьютера пользователя будет добавлен значок . Если значок имеет вид , убедитесь, что вы активировали приложение.

Как создать задачу удаленной установки в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Security Center**.
2. В раскрывающемся списке **Тип задачи** выберите **Удаленная установка приложения**.
3. В поле **Название задачи** введите короткое описание, например, *Установка Kaspersky Industrial CyberSecurity for Nodes для менеджеров*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор компьютеров для установки

На этом шаге выберите компьютеры, на которые будет установлено приложение Kaspersky Industrial CyberSecurity for Nodes, в соответствии с выбранным вариантом области действия задачи.

Шаг 3. Настройка параметров инсталляционного пакета

На этом шаге настройте параметры инсталляционного пакета:

1. Выберите инсталляционный пакет Kaspersky Industrial CyberSecurity for Nodes для Windows (5.0).
2. Выберите инсталляционный пакет Агента администрирования.

   Выбранная версия Агента администрирования будет установлена вместе с Kaspersky Industrial CyberSecurity for Nodes. *Агент администрирования* обеспечивает взаимодействие между Сервером администрирования и клиентским компьютером. Если на компьютере уже установлен Агент администрирования, установка не повторяется.

3. В блоке **Принудительно скачать инсталляционный пакет** выберите средства установки приложения:

   - **С помощью Агента администрирования**. Доставку инсталляционного пакета Kaspersky Industrial CyberSecurity for Nodes на клиентские компьютеры выполняет Агент администрирования. Если Агент администрирования не установлен, выполнение задачи завершится ошибкой. В этом случае вам нужно добавить инсталляционный пакет Агента администрирования в задачу *Удаленная установка приложения* и включить доставку файлов средствами операционной системы. Тогда Агент администрирования будет установлен средствами операционной системы. Далее Kaspersky Industrial CyberSecurity for Nodes устанавливается средствами Агента администрирования.

   - **Средствами операционной системы с помощью точек распространения**. Инсталляционный пакет передается на клиентские компьютеры средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения. Подробнее о работе точек распространения см. в справке Kaspersky Security Center.

   - **Средствами операционной системы с помощью Сервера администрирования**. Доставка файлов на клиентские компьютеры будет осуществляться средствами операционной системы с помощью Сервера администрирования. Этот вариант можно выбрать, если на клиентском компьютере не установлен Агент администрирования, но клиентский компьютер находится в той же сети, что и Сервер администрирования.

4. В поле **Максимальное количество одновременных загрузок** установите ограничение количества запросов к Серверу администрирования для загрузки инсталляционного пакета. Ограничение запросов позволит избежать перегрузки сети.

5. В поле **Максимальное количество попыток установок** установите ограничение попыток установить приложение. Если установка Kaspersky Industrial CyberSecurity for Nodes завершается с ошибкой, задача автоматически запускает установку повторно.

6. Если требуется, снимите флажок **Не устанавливать приложение, если оно уже установлено**. Это позволит, например, установить приложение более ранней версии.

7. Если требуется, снимите флажок **Предварительно проверять тип операционной системы перед загрузкой**. Это позволит избежать загрузки дистрибутива приложения, если операционная система компьютера не соответствует программным требованиям. Если вы уверены, что операционная система компьютера соответствует программным требованиям, проверку можно пропустить.

8. Если требуется, установите флажок **Назначить установку инсталляционного пакета в групповых политиках Active Directory**. Установка Kaspersky Industrial CyberSecurity for Nodes выполняется средствами Агента администрирования или средствами Active Directory вручную. Для установки Агента администрирования задача удаленной установки должна быть запущена с правами администратора домена.

9. Если требуется, установите флажок **Предлагать пользователю закрыть работающие приложения**. Установка Kaspersky Industrial CyberSecurity for Nodes требует ресурсов компьютера. Для удобства пользователя мастер установки приложения предлагает закрыть работающие приложения перед началом установки. Это позволит избежать замедление в работе других приложений и возможных сбоев в работе компьютера.

10. В блоке **Поведение устройств, управляемых другими Серверами администрирования** выберите способ установки Kaspersky Industrial CyberSecurity for Nodes. Если в сети установлено более одного Сервера администрирования, эти Серверы могут видеть одни и те же клиентские компьютеры. Это может привести, например, к удаленной установке одного и того же приложения на одном и том же клиентском компьютере с нескольких Серверов администрирования и к другим конфликтам.

Шаг 4. Выбор учетной записи для запуска задачи

Выберите учетную запись для установки Агента администрирования средствами операционной системы. В этом случае для доступа к компьютеру требуются права администратора. Вы можете добавить несколько учетных записей. Если у учетной записи нет необходимых прав, мастер установки использует следующую учетную запись. Для установки Kaspersky Industrial CyberSecurity for Nodes средствами Агента администрирования выбирать учетную запись не требуется.

Шаг 5. Завершение создания задачи

Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача. Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**. Установка приложения будет выполнена в тихом режиме. После установки в области уведомлений компьютера пользователя будет добавлен значок . Если значок имеет вид , убедитесь, что вы активировали приложение.

Подробная информация о формировании инсталляционного пакета и создании задачи удаленной установки содержится в справке Kaspersky Security Center.

Действия после установки Kaspersky Industrial CyberSecurity for Nodes

После установки Kaspersky Industrial CyberSecurity for Nodes рекомендуется обновить базы Kaspersky Industrial CyberSecurity for Nodes на устройствах, а также выполнить Проверку важных областей устройств, если до установки Kaspersky Industrial CyberSecurity for Nodes на устройствах не были установлены антивирусные приложения с включенной функцией постоянной защиты.

Если защищаемые устройства, на которых установлено приложение Kaspersky Industrial CyberSecurity for Nodes, объединены в одну группу администрирования в Kaspersky Security Center, можно выполнить эти задачи следующими способами:

1. Создать задачу *Обновление* для группы защищаемых устройств, на которых установлено приложение Kaspersky Industrial CyberSecurity for Nodes. Установить Сервер администрирования Kaspersky Security Center в качестве источника обновлений.

2. Создать групповую задачу проверки по требованию со статусом *Проверка важных областей*. Kaspersky Security Center оценивает состояние безопасности каждого защищаемого устройства группы по результатам выполнения этой задачи, а не по результатам задачи *Проверка важных областей*.

3. Создать новую политику для группы защищаемых устройств. В свойствах политики в разделе **Настройка приложения** выключить запуск по расписанию локальных системных задач проверки по требованию и задачи *Обновление* на защищаемых устройствах группы администрирования в подразделе **Запуск локальных системных задач**.

Вы можете также настроить уведомления администратора о событиях Kaspersky Industrial CyberSecurity for Nodes.

Установка Консоли приложения через Kaspersky Security Center

Подробная информация о создании инсталляционного пакета и задачи удаленной установки содержится в справке Kaspersky Security Center.

Чтобы установить Консоль приложения с помощью задачи удаленной установки, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center разверните узел **Дополнительно**.

2. Разверните вложенный узел **Удаленная установка**.

3. Создайте инсталляционный пакет:

   a. В панели результатов вложенного узла **Инсталляционные пакеты** нажмите на кнопку **Создать инсталляционный пакет**.

   b. В окне **Мастер создания инсталляционного пакета** выберите пункт **Создать инсталляционный пакет для указанного исполняемого файла** в качестве типа пакета.

   c. Введите имя инсталляционного пакета.

   d. В папке комплекта поставки Kaspersky Industrial CyberSecurity for Nodes выберите файл \client\setup_kicstool.exe и установите флажок **Копировать всю папку в инсталляционный пакет**.

e. В поле **Параметры запуска исполняемого файла (необязательно)** укажите значение параметров EULA=1 и PRIVACYPOLICY=1:

```
/s /p "EULA=1 PRIVACYPOLICY=1"
```

В противном случае установка компонентов невозможна.

f. Если необходимо, в поле **Параметры запуска исполняемого файла (необязательно)** укажите значение параметра ADDLOCAL, чтобы изменить набор устанавливаемых компонентов, и значение параметра INSTALLDIR, чтобы указать папку назначения, отличную от заданной по умолчанию. Например, чтобы выполнить автономную установку Консоли приложения в папку C:\KasperskyConsole, используйте следующие ключи командной строки:

```
/s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
```

4. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Консоли приложения на выбранные защищаемые устройства (группу администрирования).

5. Настройте параметры задачи.

6. Запустите задачу удаленной установки.

Консоль приложения будет установлена на указанные в задаче защищаемые устройства.

Удаление Kaspersky Industrial CyberSecurity for Nodes через Kaspersky Security Center

Файлы дампа и трассировки не удаляются при удалении Kaspersky Industrial CyberSecurity for Nodes. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки.

Если доступ к управлению Kaspersky Industrial CyberSecurity for Nodes на устройствах сети защищен паролем, введите пароль при создании задачи удаления нескольких приложений. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, приложение Kaspersky Industrial CyberSecurity for Nodes будет успешно удалено с устройств, где доступ к управлению приложением защищен паролем, совпавшим с введенным значением. Приложение Kaspersky Industrial CyberSecurity for Nodes не будет удалено с других защищаемых устройств.

Чтобы удалить Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center создайте и запустите задачу удаления приложения.

2. В задаче выберите метод удаления (аналогично выбору метода установки, см. предыдущий раздел) и укажите учетную запись, с правами которой Сервер администрирования будет обращаться к защищаемым устройствам. Вы можете удалить Kaspersky Industrial CyberSecurity for Nodes только с параметрами удаления по умолчанию.

Изменение состава компонентов приложения с помощью Kaspersky Security Center

Для изменения состава компонентов Kaspersky Industrial CyberSecurity for Nodes после установки приложения предназначена задача *Изменение состава компонентов приложения*.

Изменение компонентов приложения в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Industrial CyberSecurity for Nodes (5.0)** → **Изменение состава компонентов приложения**.

Шаг 2. Параметры задачи изменения компонентов приложения

Выберите компоненты приложения, которые будут доступны на компьютере пользователя. Настройте дополнительные параметры задачи (см. таблицу ниже).

При изменении конфигурации приложения на Endpoint Agent для работы с MDR убедитесь, что все компоненты, обеспечивающие получение телеметрии, включены.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или во время простоя компьютера.

Шаг 5. Определение названия задачи

Введите название задачи, например, *Добавление компонента Контроль приложений*.

Шаг 6. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Изменение состава компонентов приложения в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes 5.0.0**.
2. В раскрывающемся списке **Тип задачи** выберите **Изменение состава компонентов Kaspersky Industrial CyberSecurity for Nodes**.
3. В поле **Название задачи** введите короткое описание, например, *Добавление компонента Контроль приложений*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Например, выберите отдельную группу администрирования или сделайте выборку.

Шаг 3. Завершение создание задачи

1. Установите флажок **Открыть окно свойств задачи после ее создания** и завершите работу мастера.
2. В свойствах задачи перейдите на вкладку **Параметры приложения**.
3. Выберите компоненты приложения, которые будут доступны на компьютере пользователя. Настройте дополнительные параметры задачи (см. таблицу ниже).

   При изменении режима приложения на Endpoint Agent для работы с MDR убедитесь, что все компоненты, обеспечивающие получение телеметрии, включены.

В результате на компьютерах пользователей будет изменен состав компонентов Kaspersky Industrial CyberSecurity for Nodes.

Дополнительные параметры задачи

Параметр	Описание
Профиль исключения для промышленных систем	В рамках задачи *Изменение состава компонентов приложения* вы можете только добавлять в доверенную зону исключения из проверки и доверенные приложения.
Использовать пароль для изменения состава компонентов	Как правило, для ограничения доступа к Kaspersky Industrial CyberSecurity for Nodes администраторы включают Защиту паролем. В таком случае для изменения состава компонентов приложения вам нужно ввести учетные данные пользователя с разрешением **Удаление / изменение / восстановление приложения**. Например, вы можете использовать учетную запись KLAdmin.
Проверять на наличие несовместимых приложений сторонних производителей	По умолчанию Kaspersky Industrial CyberSecurity for Nodes проверяет установленные приложения на совместимость. Список несовместимого ПО приведен в файле incompatible.txt, входящем в комплект поставки приложения. Если проверка на наличие несовместимого ПО включена, Kaspersky Industrial CyberSecurity for Nodes прекращает выполнение задачи при обнаружении приложения из списка. Вы можете выключить проверку установленного ПО, если поставщик стороннего ПО указал в своей документации совместимость с системами защиты конечных точек (англ. Endpoint Protection Platform, EPP).
Удалять несовместимые приложения сторонних производителей	Функция автоматического удаления приложений из списка incompatible.txt перед изменением состава компонентов. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes пытается удалить приложения, с которыми могут быть проблемы совместимости, для продолжения выполнения задачи. По умолчанию функция включена.

Установка и удаление приложения через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Industrial CyberSecurity for Nodes через групповые политики Active Directory, а также информацию о действиях, которые требуется выполнить после установки Kaspersky Industrial CyberSecurity for Nodes через групповые политики.

Установка Kaspersky Industrial CyberSecurity for Nodes через групповые политики Active Directory

Вы можете установить Kaspersky Industrial CyberSecurity for Nodes на несколько защищаемых устройств с помощью групповой политики Active Directory. Консоль приложения можно установить аналогичным образом.

Защищаемые устройства, на которые вы хотите установить Kaspersky Industrial CyberSecurity for Nodes или Консоль приложения, должны находиться в одном домене и в одной организационной единице.

Операционные системы защищаемых устройств, на которые вы хотите установить Kaspersky Industrial CyberSecurity for Nodes с помощью политики, должны быть одной разрядности (32-разрядные или 64-разрядные).

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes, используйте пакет установки kics_win.msi. Чтобы установить Консоль приложения, используйте пакет установки kicstools.msi.

Подробная информация об использовании групповых политик Active Directory содержится в документации, предоставляемой корпорацией Microsoft.

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes или Консоль приложения:

1. Сохраните kics_win.msi в папку общего доступа на контроллере домена.
2. Сохраните файл ключа для активации приложения в эту же общую папку на контроллере домена.
3. В этой же папке общего доступа на контроллере домена создайте файл install_props.json, содержащий приведенные ниже строки. Это означает, что вы соглашаетесь с условиями Лицензионного соглашения и Политики конфиденциальности.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```

4. На контроллере домена создайте новую политику для группы, в которую объединены защищаемые устройства.
5. С помощью **Редактора объектов групповых политик** создайте новый инсталляционный пакет в узле **Конфигурация компьютеров**. Укажите путь к msi-файлу Kaspersky Industrial CyberSecurity for Nodes или Консоли приложения в формате UNC (Universal Naming Convention).
6. Установите флажок установщика Windows **Всегда устанавливать с повышенными правами** как в узле **Конфигурация компьютеров**, так и в узле **Конфигурация пользователей** выбранной группы.
7. Примените изменения с помощью команды `gpupdate / force`.

Приложение Kaspersky Industrial CyberSecurity for Nodes будет установлено на защищаемые устройства группы после их перезагрузки.

Действия после установки Kaspersky Industrial CyberSecurity for Nodes

После установки Kaspersky Industrial CyberSecurity for Nodes на защищаемых устройствах рекомендуется сразу обновить базы приложения и выполнить проверку важных областей компьютера. Эти действия можно выполнить из Консоли приложения.

Вы можете также настроить уведомления администратора о событиях Kaspersky Industrial CyberSecurity for Nodes.

Удаление Kaspersky Industrial CyberSecurity for Nodes через групповые политики Active Directory

Файлы дампа и трассировки не удаляются при удалении Kaspersky Industrial CyberSecurity for Nodes. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки.

Если вы установили Kaspersky Industrial CyberSecurity for Nodes или Консоль приложения в группе защищаемых устройств, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Industrial CyberSecurity for Nodes или Консоль приложения.

Вы можете удалить приложение только с параметрами удаления по умолчанию.

Подробная информация об использовании групповых политик Active Directory содержится в документации, предоставляемой корпорацией Microsoft.

Если доступ к управлению приложением защищен паролем, удаление Kaspersky Industrial CyberSecurity for Nodes через групповые политики Active Directory невозможно.

Чтобы удалить Kaspersky Industrial CyberSecurity for Nodes (или Консоль приложения), выполните следующие действия:

1. На контроллере домена выберите организационную единицу, с защищаемых устройств которой вы хотите удалить Kaspersky Industrial CyberSecurity for Nodes или Консоль приложения.

2. Выберите политику, созданную для установки Kaspersky Industrial CyberSecurity for Nodes, и в **Редакторе объектов групповых политик**, в узле **Установка программ** (**Конфигурация компьютеров** > **Параметры программ** > **Установка программ**) откройте контекстное меню пакета установки Kaspersky Industrial CyberSecurity for Nodes (Консоли приложения) и выберите команду **Все задачи** > **Удалить**.

3. Выберите метод удаления **Немедленно удалить приложения из учетных записей пользователей и компьютеров**.

4. Примените изменения с помощью команды `gpupdate /force`.

   Приложение Kaspersky Industrial CyberSecurity for Nodes будет удалено с защищаемых устройств после их перезагрузки, перед входом в Microsoft Windows.

Журналы установки и удаления Kaspersky Industrial CyberSecurity for Nodes

Если вы выполняете установку (удаление) Kaspersky Industrial CyberSecurity for Nodes или Консоли приложения с помощью мастера установки (удаления), служба установщика Windows создает журнал установки (удаления). Файл журнала с именем kl-install-<uid>.log (где <uid> – это уникальный восьмизначный идентификатор журнала) сохраняется в папку %temp% пользователя, с правами учетной записи которого был запущен файл setup_kics.exe или setup_kicstool.exe.

Если вы выполняете установку или удаление Kaspersky Industrial CyberSecurity for Nodes из командной строки, по умолчанию файл журнала установки не создается.

Чтобы установить Kaspersky Industrial CyberSecurity for Nodes и создать файл журнала на диске C:\, выполните следующую команду:

```
msiexec /i kics_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

Изменения в системе после установки Kaspersky Industrial CyberSecurity for Nodes

При совместной установке Kaspersky Industrial CyberSecurity for Nodes и Консоли Kaspersky Industrial CyberSecurity for Nodes, служба установщика Windows выполняет на защищаемом устройстве следующие изменения:

- создает папки Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве и на устройстве, на котором установлена Консоль приложения;
- регистрирует службы Kaspersky Industrial CyberSecurity for Nodes;
- создает группу пользователей Kaspersky Industrial CyberSecurity for Nodes;
- регистрирует в системном реестре ключи Kaspersky Industrial CyberSecurity for Nodes;
- создает системную задачу Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect, которая отображается в Планировщике задач Windows.
- создает правила брандмауэра Windows.

Эти изменения описаны ниже.

Папки Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве

При установке Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве создаются следующие папки:

- Заданная по умолчанию папка установки Kaspersky Industrial CyberSecurity for Nodes, содержащая исполняемые файлы Kaspersky Industrial CyberSecurity for Nodes. По умолчанию используется следующая папка установки:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0

- Файлы Management Information Base (MIB), содержащие описание счетчиков и ловушек, публикуемых Kaspersky Industrial CyberSecurity for Nodes по протоколу SNMP:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0\mibs

- Служебные файлы Kaspersky Industrial CyberSecurity for Nodes:
  - %ProgramData%\Kaspersky Lab\KICS.5.0\Data
  - %ProgramData%\Kaspersky Lab\KICS.5.0\Settings
  - %ProgramData%\Kaspersky Lab\KICS.5.0\Dskm
- Файлы с параметрами источников обновлений:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Data

- Обновления баз и программных модулей, загруженные с помощью задачи *Обновление* (папка создается при первой загрузке обновлений с помощью задачи *Обновление*):

  %ProgramData%\Kaspersky Lab\KICS.5.0\Update distribution

- Журналы выполнения задач и журнал системного аудита:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Reports

- Набор используемых баз данных:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Bases

- Резервные копии баз; перезаписываются при каждом обновлении баз:

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB

- Временные файлы, создаваемые при выполнении задач обновления:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Data\temp\temporaryFolder

- Объекты на карантине (папка по умолчанию):

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB

- Объекты в резервном хранилище (папка по умолчанию):

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB

- Объекты, восстановленные из резервного хранилища и карантина (папка по умолчанию для восстановленных объектов):

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB\Restored

Папка, создаваемая при установке Консоли приложения

Заданная по умолчанию папка установки Консоли приложения зависит от разрядности операционной системы. По умолчанию используется следующая папка установки:

%ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console 5.0.0

Службы Kaspersky Industrial CyberSecurity for Nodes

Следующие службы Kaspersky Industrial CyberSecurity for Nodes запускаются под системной учетной записью (SYSTEM):

- Kaspersky Industrial CyberSecurity for Nodes Service (AVP.KICS.5.0). Основная системная служба Kaspersky Industrial CyberSecurity for Nodes, обеспечивающая защиту устройства от вирусов и прочих угроз.

- Kaspersky Industrial CyberSecurity for Nodes Side-by-Side Service (AVP.KICS.5.0.SbS). Системная служба, обеспечивающая защиту устройства во время обновления, восстановления или изменения состава компонентов Kaspersky Industrial CyberSecurity for Nodes.

- Kaspersky Seamless Update Service (avpsus.KICS.5.0). Системная служба, обеспечивающая установку и отзыв критических и одобренных обновлений модулей приложения.

- Kaspersky Industrial CyberSecurity for Nodes Remote Control Service (avpcos.KICS.5.0). Системная служба, обеспечивающая возможность удаленного запуска и остановки службы Kaspersky Industrial CyberSecurity for Nodes Service из Консоли приложения.

Группа Kaspersky Industrial CyberSecurity for Nodes

KICS Administrators – это группа на защищаемом устройстве, пользователи которой имеют полный доступ ко всем функциям Kaspersky Industrial CyberSecurity for Nodes.

Ключи системного реестра

При установке Kaspersky Industrial CyberSecurity for Nodes создаются следующие ключи системного реестра:

- Свойства Kaspersky Industrial CyberSecurity for Nodes:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.KICS.5.0]
- Параметры журнала событий Kaspersky Industrial CyberSecurity for Nodes (Kaspersky Event Log):
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Industrial CyberSecurity for Nodes]
- Настройки файла трассировки:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\Trace]
- Настройки задач и функций приложения:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\environment]

Системная задача Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect

Служба установщика Windows создает задачу Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect во время установки приложения. Задача запускается сразу после ее создания и далее при каждой загрузке ОС. Задача проверяет версию используемых приложением драйверов: если выполнено обновление версии операционной системы, приложение обновляет драйверы для соответствующей версии операционной системы.

Задача не влияет на работу приложения и может быть удалена. Рекомендуем помнить о сценарии обновления операционной системы.

Правила брандмауэра Windows

В зависимости от заданных параметров установки на защищаемом устройстве могут быть созданы разрешающие правила брандмауэра Windows для входящих соединений, описанные в таблице ниже.

Правила брандмауэра Windows

Название правила	Описание правила	Условие создания правила
AVP.KICS.5.0	Разрешающее правило для исполняемого файла avp.exe.	Создается всегда.
AVP.KICS.5.0 Remote UI Connection	Разрешающее правило для TCP-порта 13032.	Установка приложения с параметром `ADDWFEXCLUSION=1`.

Название правила	Описание правила	Условие создания правила
AVP.KICS.5.0 Remote UI Connection	Разрешающее правило для TCP-порта 13031. Данный номер порта используется по умолчанию. Вы можете изменить номер порта с помощью параметра `UIKLPORT=<port>`. В таком случае приложение создаст правило для указанного вами номера порта.	Установка приложения с параметрами `ADDWFEXCLUSION=1` и `UIKLPORT=13031`. Правило не создается, если передан параметр `ENABLEUIKLPORT=0`.
DHCP Discover In	Разрешающее правило для UDP-порта 67.	Установка приложения с компонентом Интеграция с KICS for Networks.
SSDP Discover In	Разрешающее правило для UDP-порта 1900.	

Процессы Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes запускает процессы, описанные в таблице ниже.

Процессы Kaspersky Industrial CyberSecurity for Nodes

Имя файла	Назначение
avp.exe	Рабочий процесс Kaspersky Industrial CyberSecurity for Nodes.
avpsus.exe	Процесс позволяет устанавливать и откатывать критические и одобренные обновления модулей приложения.

Проверка функций Kaspersky Industrial CyberSecurity for Nodes. Использование тестового вируса EICAR

В этом разделе описан тестовый вирус EICAR и его использование для проверки функций постоянной защиты файлов и проверки по требованию Kaspersky Industrial CyberSecurity for Nodes.

О тестовом вирусе EICAR

Тестовый вирус предназначен для проверки работы антивирусных приложений. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый вирус не является вредоносным объектом и не содержит исполняемого кода, который может нанести вред вашему устройству, но антивирусные приложения большинства производителей идентифицируют его как угрозу.

Файл, который содержит тестовый вирус, называется eicar.com. Его можно загрузить на веб-сайте EICAR.

Перед сохранением файла в папку на жестком диске устройства убедитесь, что для этого жесткого диска выключена Постоянная защита файлов.

Файл eicar.com содержит текстовую строку. При проверке файла Kaspersky Industrial CyberSecurity for Nodes обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Заражен** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли приложения и в журнале выполнения задачи.

Вы также можете использовать файл eicar.com, чтобы проверять, как Kaspersky Industrial CyberSecurity for Nodes выполняет лечение зараженных объектов и как обнаруживает возможно зараженные объекты. Для этого откройте файл с помощью текстового редактора, добавьте к началу текстовой строки в файле один из префиксов, перечисленных в таблице ниже, и сохраните файл с новым именем, например, eicar_cure.com.

Чтобы убедиться, что Kaspersky Industrial CyberSecurity for Nodes обрабатывает файл eicar.com с префиксом, в разделе параметров безопасности **Защита объектов** установите значение **Все объекты** для задач постоянной защиты компьютера и проверки по требованию в Kaspersky Industrial CyberSecurity for Nodes.

Префиксы в файлах EICAR

Префикс	Статус файла после проверки и действие Kaspersky Industrial CyberSecurity for Nodes
Без префикса	**Kaspersky Industrial CyberSecurity for Nodes присваивает объекту статус Заражен и удаляет его.**
SUSP–	Kaspersky Industrial CyberSecurity for Nodes присваивает статус **Возможно зараженный** объекту, обнаруженному с помощью эвристического анализатора, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению.
WARN–	Kaspersky Industrial CyberSecurity for Nodes присваивает статус **Возможно зараженный** объекту, если код объекта частично совпадает с кодом известной угрозы, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению.
CURE–	Kaspersky Industrial CyberSecurity for Nodes присваивает объекту статус **Заражен** и лечит его. Если лечение успешно, весь текст в файле заменяется словом "CURE".

Проверка функций постоянной защиты файлов и проверки по требованию

После установки Kaspersky Industrial CyberSecurity for Nodes вы можете убедиться, что Kaspersky Industrial CyberSecurity for Nodes обнаруживает объекты, содержащие вредоносный код. Для этого можно использовать тестовый вирус EICAR.

Чтобы проверить функцию постоянной защиты файлов:

1. Загрузите файл eicar.com с веб-сайта EICAR. Сохраните его в папку общего доступа на локальном диске любого устройства сети.

   Перед сохранением файла в папку убедитесь, что функция постоянной защиты файлов отключена для этой папки.

2. Если вы хотите проверить работу уведомлений пользователей сети, убедитесь, что Служба сообщений Microsoft Windows включена на защищаемом устройстве и на устройстве, на котором сохранен файл eicar.com.

3. Откройте Консоль приложения на защищаемом устройстве.

4. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого устройства одним из следующих способов:

   - Чтобы проверить работу уведомлений через окно Службы терминалов, скопируйте файл eicar.com на защищаемое устройство, подключившись к защищаемому устройству с помощью приложения "Подключение к удаленному рабочему столу" (Remote Desktop Connection).

   - Чтобы проверить работу уведомлений через Службу сообщений Microsoft Windows, скопируйте файл eicar.com с устройства, на котором вы его сохранили, через сетевое окружение этого устройства.

Постоянная защита файлов работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с защищаемого устройства.

- В Консоли приложения журналу выполнения задачи присвоен статус *Критический*. В журнале появилась строка с информацией об угрозе в файле eicar.com.

- На устройстве, с которого вы скопировали файл, появилось следующее сообщение Службы сообщений Microsoft Windows: Программа Kaspersky Industrial CyberSecurity for Nodes заблокировала доступ к <путь к файлу eicar.com на устройстве>\eicar.com на компьютере <сетевое имя устройства> в <время возникновения события>. Причина: обнаружена угроза. Вирус: EICAR-Test-File. Имя пользователя: <имя пользователя>. Имя компьютера: <сетевое имя устройства, с которого вы скопировали файл>.

  Убедитесь, что Служба сообщений Microsoft Windows работает на устройстве, с которого вы скопировали файл eicar.com.

Чтобы просмотреть журнал выполнения задачи:

1. В дереве Консоли приложения разверните узел **Проверка по требованию**.

2. Выберите созданную задачу проверки по требованию.

3. В панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.

Чтобы проверить функцию проверки по требованию:

1. Загрузите файл eicar.com с веб-сайта EICAR. Сохраните его в папку общего доступа на локальном диске любого устройства сети.

   Перед сохранением файла в папку убедитесь, что функция постоянной защиты файлов отключена для этой папки.

2. Откройте Консоль приложения и разверните узел **Проверка по требованию**.

3. Выберите вложенный узел **Проверка важных областей**.

4. На вкладке **Настройка** области проверки откройте контекстное меню на узле **Сетевое окружение**.

5. Выберите **Добавить сетевой файл**.

6. Введите сетевой путь к файлу eicar.com на удаленном компьютере в формате UNC (Universal Naming Convention).

7. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.

8. Запустите задачу Проверка важных областей.

Проверка по требованию работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с жесткого диска устройства.
- В Консоли приложения журналу выполнения задачи присвоен статус *Критический*. В журнале выполнения задачи проверки по требованию появилась строка с информацией об угрозе в файле eicar.com.

Обновление Kaspersky Industrial CyberSecurity for Nodes предыдущих версий до версии 5.0

При обновлении Kaspersky Industrial CyberSecurity for Nodes одной из предыдущих версий до версии 5.0 воспользуйтесь следующими рекомендациями:

- Запланируйте время обновления. Выберите время, когда серверы наименее загружены, например, в выходные дни.
- После обновления включайте компоненты приложения постепенно. То есть, например, сначала включите только компонент Постоянная защита файлов, затем включите другие компоненты защиты, затем включите компоненты контроля и так далее. На каждом шаге рекомендуем проверять работу приложения.
- Выполняйте обновление постепенно. Сначала выполните обновление на одном компьютере, затем на нескольких компьютерах, и далее выполните обновление на всех компьютерах организации.

Этапы обновления

Выполняйте обновление до Kaspersky Industrial CyberSecurity for Nodes версии 5.0 в следующем порядке:

1. **Обновите Kaspersky Security Center**

   Обновите все компоненты Kaspersky Security Center до версии 14.2 или выше, включая Агент администрирования на компьютерах пользователей и Kaspersky Security Center Web Console.

2. **Обновите Веб-плагин Kaspersky Industrial CyberSecurity for Nodes**

   В Kaspersky Security Center Web Console обновите Веб-плагин Kaspersky Industrial CyberSecurity for Nodes до версии 5.0.

3. **Выполните миграцию политик и задач Kaspersky Industrial CyberSecurity for Nodes**

   После миграции политик и задач необходимо настроить параметры, которые мастер миграции не может перенести, и которые отсутствовали в предыдущих версиях приложения. Также рекомендуем проверить, что мастер миграции перенес настройки корректно.

4. **Установите Kaspersky Industrial CyberSecurity for Nodes 5.0**

   В Kaspersky Industrial CyberSecurity for Nodes версии 5.0 вместо протокола DCOM используется протокол HTTPS. В связи с этим необходимо до установки новой версии Kaspersky Industrial CyberSecurity for Nodes выполнить настройку устройства, на котором будет обновляться приложение, для обеспечения возможности удаленного запуска сервиса KICS. Без выполнения данной настройки удаленный запуск будет недоступен.

   Вы можете установить Kaspersky Industrial CyberSecurity for Nodes версии 5.0 после удаления или поверх более ранней версии приложения.

   В случае установки поверх предыдущей версии приложения, устанавливаются те же компоненты приложения с учетом изменений названий и состава некоторых компонентов.

При удаленной установке инсталлятор устанавливает компоненты, которые вы выбрали в свойствах инсталляционного пакета.

5. **Если необходимо, активируйте Kaspersky Industrial CyberSecurity for Nodes 5.0**

   При установке Kaspersky Industrial CyberSecurity for Nodes 5.0 поверх более ранней версии приложения действующая лицензия автоматически применяется к приложению, и использование новых компонентов и задач приложения доступно в полном объеме. Срок действия лицензии остается без изменений.

6. **Проверьте работу приложения**

   После обновления Kaspersky Industrial CyberSecurity for Nodes убедитесь, что приложение работает корректно. Убедитесь в отсутствии ошибок в работе приложения, также проверьте время последнего соединения с Сервером администрирования, время последнего обновления и статус защиты компьютера.

   Обратите внимание на миграцию списков исключений, доверенных приложений, правил Контроля устройств и Контроля запуска программ.

Об обновлении Kaspersky Industrial CyberSecurity for Nodes

Обновление до Kaspersky Industrial CyberSecurity for Nodes 5.0 доступно для приложения версий 3.2 и выше. Для обновления более ранних версий приложения требуется удалить установленную версию приложения и установить приложение версии 5.0.

Обновление выполняется путем установки новой версии приложения поверх установленной версии приложения и не требует перезагрузки компьютера.

По умолчанию приложение создает новую папку установки с именем новой версии приложения на основе пути к существующей папке установки приложения. Вы можете вручную задать новый путь для папки установки приложения.

В процессе обновления Kaspersky Industrial CyberSecurity for Nodes до версии 5.0 установленная раннее версия приложения автоматически удаляется.

При обновлении Kaspersky Industrial CyberSecurity for Nodes, защищенной паролем, необходимо передать установщику этот пароль одним из следующих способов:

- При установке локально через интерфейс Мастера установки или в интерактивном режиме через командную строку указать пароль на соответствующем шаге.
- При установке локально через командную строку в неинтерактивном режиме указать пароль в качестве значения ключа `UNLOCK_PASSWORD`.
- При установке через групповые политики Active Directory с помощью значения ключа `UNLOCK_PASSWORD` в конфигурационном файле install_props.json.

Для обновлении приложения, защищенного паролем, удаленно через Kaspersky Security Center требуется предварительно выключить защиту паролем с помощью политики Kaspersky Security Center.

При обновлении приложения действующая лицензия автоматически применяется к Kaspersky Industrial CyberSecurity for Nodes 5.0, и использование новых компонентов и задач приложения доступно в полном объеме. Срок действия лицензии остается без изменений.

При обновлении приложения с истекшим сроком действия лицензии новая версия приложения после установки работает в режиме ограниченной функциональности (например, недоступно обновление баз приложения).

Об обновлении средств администрирования Kaspersky Industrial CyberSecurity for Nodes

Обновление Плагина управления приложением через Kaspersky Security Center до версии 5.0 доступно для Плагина управления версии 3.2, 4.0 и выше. Для обновления Плагина управления более ранних версий и Консоли приложения требуется удалить установленную версию и установить версию 5.0.

Обновление выполняется путем установки новой версии Плагина управления рядом с установленной версией и не требует перезагрузки компьютера.

О миграции настроек Плагина управления читайте в статье.

Миграция политик и задач

Вы можете перенести настройки политик и задач предыдущих версий приложения в версию 5.0 следующими способами:

- С помощью мастера массовой конвертации политик и задач (доступен только в Консоли администрирования Kaspersky Security Center).
- С помощью мастера миграции на Kaspersky Industrial CyberSecurity for Nodes 5.0 (доступен только в Kaspersky Security Center Web Console).

Рекомендуем сначала выполнить миграцию политик и задач Kaspersky Industrial CyberSecurity for Nodes на одном компьютере, затем на группе компьютеров и далее выполнить миграцию на всех компьютерах организации.

Как перенести настройки политик и задач с помощью мастера массовой конвертации политик и задач

1. В Консоли администрирования Kaspersky Security Center выберите Сервер администрирования и откройте контекстное меню.
2. Выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

Запустится мастер массовой конвертации политик и задач. Следуйте его указаниям.

Шаг 1. Выбор приложения, для которого нужно конвертировать политики и задачи

Выберите приложение Kaspersky Industrial CyberSecurity for Nodes 5.0. Перейдите к следующему шагу.

Шаг 2. Конвертация политик

Выберите политики обновляемой версии приложения, которые вы хотите создать для Kaspersky Industrial CyberSecurity for Nodes 5.0.

Шаг 3. Миграция с Kaspersky Endpoint Agent

Если необходимо, последовательно для каждой выбранной на предыдущем шаге мастера политики Kaspersky Industrial CyberSecurity for Nodes выберите политику Kaspersky Endpoint Agent, параметры которой будут добавлены в новую политику Kaspersky Industrial CyberSecurity for Nodes 5.0. Перейдите к следующему шагу.

Шаг 4. Конвертация задач

Выберите групповые задачи обновляемой версии приложения, которые вы хотите конвертировать для Kaspersky Industrial CyberSecurity for Nodes 5.0.

Негрупповые задачи (задачи, назначенные отдельным устройствам) не отображаются на текущем шаге.

Чтобы конвертировать негрупповые задачи обновляемой версии приложения для Kaspersky Industrial CyberSecurity for Nodes 5.0:

1. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительно мигрировать расписания и негрупповые задачи**.

2. Установите флажок **Мигрировать негрупповые задачи**.

3. Укажите значения настроек для подключения к Серверу администрирования Kaspersky Security Center.

4. Нажмите на кнопку **ОК**.

Шаг 5. Завершение работы мастера

Завершите работу мастера. В результате работы мастера будут выполнены следующие действия:

- Созданы новые политики для Kaspersky Industrial CyberSecurity for Nodes 5.0.

  В новые политики перенесены настройки из выбранных политик Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Endpoint Agent и добавлены новые настройки, которые появились в Kaspersky Industrial CyberSecurity for Nodes 5.0. Названия новых политик повторяют названия политик Kaspersky Industrial CyberSecurity for Nodes до конвертации с добавлением уточнения "(конвертированная)". Новые политики имеют статус *Неактивная политика*.

- Созданы новые задачи для Kaspersky Industrial CyberSecurity for Nodes 5.0.

  В новых задачах перенесены настройки из выбранных задач Kaspersky Industrial CyberSecurity for Nodes и добавлены новые настройки, которые появились в Kaspersky Industrial CyberSecurity for Nodes 5.0. Названия новых задач повторяют названия задач Kaspersky Industrial CyberSecurity for Nodes до конвертации с добавлением уточнения "(конвертированная)".

- Выбранные для конвертации политики и задачи остаются без изменений.

Как перенести настройки политик и задач с помощью мастера миграции

В главном окне Web Console или Cloud Console выберите **Операции → Миграция на Kaspersky Industrial CyberSecurity for Nodes 5.0.0**.

Запустится мастер миграции политик и задач. Следуйте его указаниям.

Шаг 1. Миграция политик

Выберите политики Kaspersky Industrial CyberSecurity for Nodes и, если необходимо, политики Kaspersky Endpoint Agent, параметры которых вы хотите объединить.

Убедитесь, что политики выбраны верно, и перейдите к следующем шагу.

Шаг 2. Миграция задач

Выберите задачи Kaspersky Industrial CyberSecurity for Nodes, которые вы хотите создать для Kaspersky Industrial CyberSecurity for Nodes 5.0.

Перейдите к следующему шагу.

Шаг 3. Завершение работы мастера

Завершите работу мастера. В результате работы мастера будут выполнены следующие действия:

- Созданы новые политики для Kaspersky Industrial CyberSecurity for Nodes 5.0.

  В новые политики перенесены настройки из мигрированных политик Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Endpoint Agent и добавлены новые настройки, которые появились в Kaspersky Industrial CyberSecurity for Nodes 5.0. Названия новых политик повторяют названия политик Kaspersky Industrial CyberSecurity for Nodes до объединения с добавлением фразы "скопирована из KICS". Новые политики имеют статус *Неактивная политика*.

- Созданы новые задачи для Kaspersky Industrial CyberSecurity for Nodes 5.0.

  В новых задачах перенесены настройки из мигрированных задач Kaspersky Industrial CyberSecurity for Nodes и добавлены новые настройки, которые появились в Kaspersky Industrial CyberSecurity for Nodes 5.0. Названия новых задач повторяют названия задач Kaspersky Industrial CyberSecurity for Nodes до миграции с добавлением фразы "скопирована из KICS".

Миграция настроек обновляемой версии приложения

После обновления приложения и плагинов управления приложением через Kaspersky Security Center до версии 5.0 переносятся без изменений:

- настройки компонентов и задач, за исключением тех, что изменяются до значений по умолчанию, и перечисленных в списке "Ограничения миграции настроек и компонентов";
- журналы выполнения задач и системного аудита, а также записи в Журнале событий Windows;
- параметры уведомлений о работе задач;
- учетные записи, с правами которых запускаются задачи;
- права на управление приложением;
- пароль для подключения к прокси-серверу;
- состояние атрибута в политиках Kaspersky Security Center.

После обновления приложения и плагинов управления приложением через Kaspersky Security Center до версии 5.0 сбрасываются или изменяются до значений по умолчанию для новой версии приложения:

- все счетчики, в том числе статусы состояния антивирусных баз;
- данные об установленных обновлениях программных модулей и антивирусных баз;
- статусы выполнения задач;
- права на управление службой Kaspersky Industrial CyberSecurity for Nodes Service;
- настройки приложения и задач, заданные через реестр;
- настройки приложения и задач, измененные в процессе установки критических исправлений;
- настройки событий;
- настройки передачи данных на Сервер администрирования Kaspersky Security Center – по умолчанию передача всех данных включена;
- настройки трассировки работы приложения и записи дампов памяти;
- настройки локальных задач приложения, которые размещены на вкладке **Уведомления**.

Настройки, которых не было в обновляемой версии приложения, будут иметь значения по умолчанию.

Ограничения миграции настроек и компонентов

- Содержимое карантина обновляемой версии приложения переносится в резервное хранилище приложения версии 5.0. После обновления максимальный размер резервного хранилища равен сумме максимальных размеров резервного хранилища и карантина обновляемого приложения, так же меняется и порог доступного пространства. При этом максимальный размер по умолчанию резервного хранилища увеличивается до 400 МБ, а порог доступного пространства – до 100 МБ.

- Параметры Kaspersky Industrial CyberSecurity for Nodes версии 4.0 **Папка карантина**, **Папка резервного хранилища** и **Папка, в которую восстанавливаются объекты** отсутствуют в Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и выше, поэтому они не переносятся при миграции. Аналогично не переносятся другие параметры, которые есть в обновляемой версии приложения, но отсутствуют в версии приложения, до которой выполняется обновление.

- В случае миграции конфигурации [KICS+KEA] на [KICS+встроенный агент] содержимое карантина Kaspersky Endpoint Agent переносится в карантин Kaspersky Industrial CyberSecurity for Nodes 5.0.

- Не переносится список заблокированных сетевых сессий клиентских компьютеров. При этом настройки автоматической разблокировки доступа к заблокированным сетевым файловым ресурсам остаются неизмененными после обновления приложения.

- Настройки Защиты паролем не мигрируют. В Kaspersky Industrial CyberSecurity for Nodes 4.5 Защита паролем значительно изменена. Если требуется, включите Защиту паролем и задайте пароль.

- Доверенная зона:

  - Способ выбора объектов доверенной зоны в Kaspersky Industrial CyberSecurity for Nodes 5.0 изменен. Поддерживается миграция исключений, заданных в виде отдельного файла или пути к файлу / папке. Исключения, заданные в виде предопределенной области (например, жесткие диски) или веб-адреса скрипта, не мигрируют. После миграции вам нужно добавить эти исключения вручную.

  - В доверенную зону добавлены предустановленные исключения из проверки и доверенные приложения, предназначенные для быстрой настройки работы приложения на серверах и с промышленными программами.

- Компоненты Контроль запуска программ и Контроль устройств значительно переработаны. Настройки компонентов обновляемой версии приложения мигрируют с учетом новой структуры настроек компонентов в Kaspersky Industrial CyberSecurity for Nodes 5.0. В связи с этим вам может потребоваться больше места на Сервере администрирования для хранения настроек приложения.

- Настройки компонентов Мониторинг файловых операций и Мониторинг доступа к реестру обновляемой версии приложения мигрируют в настройки компонента Контроль целостности системы.

- Компонент Управление сетевым экраном преобразован в Сетевой экран, который теперь не только взаимодействует с брандмауэром Windows, но и выполняет функции сетевого экрана. После миграции необходимо заново настроить режим работы компонента.

- Для использования KSN необходимо заново прочитать и принять условия Положения о KSN.

- Приложение версии 4.5 и выше не поддерживает настройку расписания работы отдельных компонентов. Если компоненты включены, то они работают постоянно, пока работает приложение.

- При миграции задач настройка времени запуска задачи переносится со сдвигом на количество часов, равное номеру часового пояса, установленному в настройках операционной системы компьютера, на котором выполняется миграция. Например, время запуск задачи более ранней версии приложения 7:00 и в настройках операционной системы указан часовой пояс UTC +3:00. Тогда после миграции задачи время запуска задачи изменится на 10:00.

- В настройках компонента Постоянная защита файлов и задач проверки по требованию убран блок для определения действий над возможно зараженными объектами. Эти настройки не переносятся из обновляемой версии приложения.

- При использовании приложения версии 4.5 и выше в составе решения Kaspersky Industrial CyberSecurity Endpoint Detection and Response, для работы с деталями алертов необходимо обновить Веб-плагин Endpoint Detection and Response до версии 15.1 или выше. В противном случае, если установлен Веб-плагин Kaspersky Endpoint Agent, цепочки развития угроз в карточках инцидентов, открытые этим Веб-плагином, могут содержать ограниченные данные или ошибки.

- Невозможно в Консоли администрирования и Web Console отправить для анализа в "Лабораторию Касперского" объекты карантина и резервного хранилища, если они мигрировали после обновления приложения версии 4.0 и ниже до версии 4.5 и выше или были помещены в хранилища по сценариям Kaspersky Anti Targeted Attack Platform или Kaspersky Industrial CyberSecurity for Networks.

- При миграции задач проверки по требованию уровень безопасности, установленный по умолчанию для предустановленных областей проверки, меняется с *Информировать* на *Другой*.

- Формат даты и времени в событиях, отправляемых в SIEM, изменился. В предыдущих версиях Kaspersky Industrial CyberSecurity for Nodes формирует события с меткой времени. Теперь приложение формирует события с датой и временем в формате `<DATE-TIME>`. Если требуется, перенастройте взаимодействие приложения с SIEM для конвертации даты и времени в метку времени.

- Если при локальном обновлении Kaspersky Industrial CyberSecurity for Nodes не был установлен компонент, который ранее входил в состав приложения, то настройки данного компонента не сохраняются. В дальнейшем при установке данного компонента для него будут применены настройки по умолчанию.

Соответствие компонентов и задач Kaspersky Industrial CyberSecurity for Nodes версии 4.0 и 5.0

При обновлении Kaspersky Industrial CyberSecurity for Nodes версии 4.0 до версии 5.0 набор компонентов и задач переносится только при локальной установке приложения.

Соответствие компонентов Kaspersky Industrial CyberSecurity for Nodes версии 4.0 и 5.0

Компонент Kaspersky Industrial CyberSecurity for Nodes 4.0	Компонент Kaspersky Industrial CyberSecurity for Nodes 5.0
Доверенная зона	Доверенная зона
Постоянная защита файлов	Постоянная защита файлов
Использование KSN	Использование KSN
Защита от эксплойтов	Защита от эксплойтов
Защита от сетевых угроз	Защита от сетевых угроз
AMSI-защита	AMSI-защита
Контроль запуска программ	Контроль запуска программ

Компонент Kaspersky Industrial CyberSecurity for Nodes 4.0	Компонент Kaspersky Industrial CyberSecurity for Nodes 5.0
Контроль устройств	Контроль устройств
Контроль Wi-Fi	Контроль устройств Функциональность компонента Контроль Wi-Fi включена в компонент Контроль устройств.
Управление сетевым экраном	Сетевой экран Функции сетевого экрана Kaspersky Industrial CyberSecurity for Nodes 4.0 выполняет Брандмауэр Windows, а приложение управляет Брандмауэром Windows. В Kaspersky Industrial CyberSecurity for Nodes 5.0 функции сетевого экрана выполняет отдельный компонент.
Защита от шифрования	Защита от шифрования
Мониторинг файловых операций	Контроль целостности системы Функциональность компонентов Мониторинг файловых операций и Мониторинг доступа к реестру объединена в компоненте Контроль целостности системы.
Анализ журналов	Анализ журналов
Мониторинг доступа к реестру	Контроль целостности системы Функциональность компонентов Мониторинг файловых операций и Мониторинг доступа к реестру объединена в компоненте Контроль целостности системы.
Портативный сканер	Portable Auditor
(отсутствует)	Откат вредоносных действий
(отсутствует)	Интеграция с KICS for Networks Компонент, выполняющий функцию Kaspersky Endpoint Agent.
(отсутствует)	Интеграция с SIEM Компонент, выполняющий функцию Kaspersky Endpoint Agent.
(отсутствует)	Managed Detection and Response (Industrial CyberSecurity) Компонент, выполняющий функцию Kaspersky Endpoint Agent.
(отсутствует)	Endpoint Detection and Response Expert (on-premises) Компонент, выполняющий функцию Kaspersky Endpoint Agent.
(отсутствует)	Endpoint Detection and Response (Industrial CyberSecurity)
(отсутствует)	Обнаружение аномалий с помощью Sigma-правил Компонент, выполняющий функцию Kaspersky Endpoint Agent.
Задача Kaspersky Industrial CyberSecurity for Nodes 4.0	**Задача Kaspersky Industrial CyberSecurity for Nodes 5.0**
Активация программы	Активация приложения
Копирование обновления	Обновление Функциональность задачи Копирование обновления включена в задачу Обновление.
Мониторинг целостности файлов на основе эталона	Мониторинг целостности системы на основе эталона
Обновление баз программы	Обновление Функциональность задачи Обновление баз программы включена в задачу Обновление.
Обновление модулей программы	Обновление Функциональность задачи Обновление модулей программы включена в задачу Обновление.
Откат обновления баз программы	Откат обновления
Проверка по требованию	Проверка по требованию
Проверка целостности программы	Проверка целостности приложения
Формирование правил контроля запуска программ	Формирование правил контроля запуска программ
Формирование правил контроля устройств	Формирование правил контроля устройств

Компонент Kaspersky Industrial CyberSecurity for Nodes 4.0	Компонент Kaspersky Industrial CyberSecurity for Nodes 5.0
(отсутствует)	Защита подключения к Серверу администрирования
(отсутствует)	Изменение состава компонентов Kaspersky Industrial CyberSecurity for Nodes
(отсутствует)	Аудит безопасности Задача, выполняющая функцию Kaspersky Endpoint Agent.
(отсутствует)	Завершение процесса Задача, выполняющая функцию Kaspersky Endpoint Agent.
(отсутствует)	Запуск процесса Задача, выполняющая функцию Kaspersky Endpoint Agent.
(отсутствует)	Поиск IOC Задача, выполняющая функцию Kaspersky Endpoint Agent.
(отсутствует)	Получение файла Задача, выполняющая функцию Kaspersky Endpoint Agent.
(отсутствует)	Помещение файла на карантин Задача, выполняющая функцию Kaspersky Endpoint Agent.
(отсутствует)	Удаление файла Задача, выполняющая функцию Kaspersky Endpoint Agent.

Установка и удаление Kaspersky Security Gateway

В этом разделе приведены инструкции по установке и удалению Kaspersky Security Gateway.

Об обновлении Kaspersky Security Gateway

Обновление Kaspersky Security Gateway выполняется путем установки новой версии программы поверх установленной версии программы и не требует перезагрузки компьютера.

В процессе обновления Kaspersky Security Gateway до версии 5.0 установленная раннее версия программы автоматически удаляется.

Значения параметров обновляемой версии Kaspersky Security Gateway передаются без изменения в Kaspersky Security Gateway 5.0.

При обновлении Kaspersky Security Gateway версии 4.5 и ниже до версии 5.0 запись файлов трассировки отключается. При необходимости настройте запись файлов трассировки заново.

Установка Kaspersky Security Gateway с помощью мастера установки

Чтобы установить Kaspersky Security Gateway,

запустите файл security_gateway.msi, входящий в комплект поставки.

Соответствующий мастер проведет вас по всем шагам установки. Следуйте инструкциям мастера.

Интерфейс мастера установки Kaspersky Security Gateway состоит из последовательных окон (шагов). Для перемещения между окнами мастера установки используйте кнопки **< Назад** и **Далее >**. Чтобы закрыть мастер установки после завершения, нажмите на кнопку **Готово**. Чтобы выйти из мастера установки на любом этапе процесса установки, нажмите на кнопку **Отмена**.

Шаг 1. Проверка требований к установке

Если среди обнаруженных программ есть предыдущая версия Kaspersky Security Gateway, мастер установки автоматически удаляет ее и устанавливает новую версию Kaspersky Security Gateway.

Если установлен Kaspersky Security Gateway 2.0 или более ранняя версия, мастер установки не сможет удалить ее и отменит установку. Перед установкой Kaspersky Security Gateway 5.0 вручную удалите Kaspersky Security Gateway 2.0 или более ранней версии.

Перед установкой или обновлением Kaspersky Security Gateway мастер установки проверяет выполнение следующих требований:

- Компьютер и установленные программы соответствуют аппаратным и программным требованиям.
- Учетная запись пользователя обладает необходимыми для установки приложений правами.

Если не выполнено какое-либо из предыдущих требований, на экране отображается соответствующее уведомление и процесс установки прерывается.

Шаг 2. Страница приветствия в начале установки

Если компьютер, на котором выполняется установка Kaspersky Security Gateway, полностью соответствует аппаратным и программным требованиям, откроется страница приветствия. На странице приветствия сообщается о начале установки Kaspersky Security Gateway на компьютере.

Перейдите к следующему шагу мастера.

Шаг 3. Ознакомление с текстом Лицензионного соглашения и Политики конфиденциальности

На этом этапе рекомендуется ознакомиться с Лицензионным соглашением и Политикой конфиденциальности "Лаборатории Касперского".

Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я принимаю условия 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 «Политику конфиденциальности»**.

Если вы не примите Лицензионное соглашение и (или) Политику конфиденциальности, установка будет прервана.

Перейдите к следующему шагу мастера.

Шаг 4. Выбор папки назначения

На этом шаге вам необходимо указать путь к папке назначения, в которую будет установлен Kaspersky Security Gateway. Чтобы выбрать папку назначения, нажмите на кнопку **Обзор**.

Перейдите к следующему шагу мастера.

Шаг 5. Выбор компонентов

На этом шаге вы можете выбрать устанавливаемые компоненты Kaspersky Security Gateway. По умолчанию выбрана установка всех компонентов.

Чтобы выбрать устанавливаемый компонент, нажмите на значок рядом с названием компонента, чтобы открыть его контекстное меню. Затем выберите **Компонент будет установлен на локальный жесткий диск** или **Компонент и его подкомпоненты будут установлены полностью**. Более подробная информация о задачах, выполняемых выбранным компонентом, и свободном месте на диске, требуемом для установки компонента, приведена в нижней части страницы мастера установки.

Чтобы просмотреть подробную информацию о доступном пространстве на локальных жестких дисках, нажмите на кнопку **Диск**. Информация отображается в открывшемся окне **Доступное дисковое пространство**.

Чтобы отменить установку компонента, в контекстном меню выберите пункт **Компонент будет недоступен**.

Чтобы вернуться к списку компонентов, установленных по умолчанию, нажмите на кнопку **Сброс**.

Перейдите к следующему шагу мастера.

Шаг 6. Настройка подключения к системе SCADA

На этом шаге вам нужно указать параметры для подключения к системе SCADA:

- Для подключения по протоколу IEC 60870-5-104: адрес (число от 1 до 65535) и TCP-порт (число от 1 до 65535) компьютера, на котором будет установлен Kaspersky Security Gateway.
- Для подключения по протоколу OPC UA: TCP-порт (число от 1 до 65535) компьютера, на котором будет установлен Kaspersky Security Gateway.

Чтобы запустить установку, нажмите на кнопку **Установить**.

Во время установки Kaspersky Security Gateway на компьютер могут быть разорваны текущие сетевые соединения. Большинство разорванных соединений восстанавливаются через непродолжительное время.

Шаг 7. Установка Kaspersky Security Gateway

Мастер установки копирует файлы Kaspersky Security Gateway на компьютер. Дождитесь завершения установки.

Завершите работу мастера.

Установка Kaspersky Security Gateway из командной строки

Чтобы установить Kaspersky Security Gateway из командной строки, выполните следующую команду:

```
msiexec /i security_gateway.msi EULA=1 PRIVACYPOLICY=1 /qn
```

где `EULA=1 PRIVACYPOLICY=1` соответствует тому, что вы принимаете условия Лицензионного соглашения для Kaspersky Security Gateway между вами и "Лабораторией Касперского" и Политики конфиденциальности, описывающей обработку и передачу данных.

Устанавливая значение 1 для параметров, вы подтверждаете следующее:

- Вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.
- Вы полностью прочитали и понимаете Политику конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности.

Для установки Kaspersky Security Gateway необходимо принять условия Лицензионного соглашения и Политики конфиденциальности.

Текст Лицензионного соглашения и Политики конфиденциальности включен в комплект поставки.

Удаление Kaspersky Security Gateway

Для удаления Kaspersky Security Gateway необходимы права администратора.

Чтобы удалить Kaspersky Security Gateway, выполните следующие действия:

1. Откройте Панель управления Microsoft Windows.
2. В Панели управления Microsoft Windows нажмите на значок **Программы и компоненты**.

   В Microsoft Windows откроется окно **Изменить или удалить программу**.

3. В окне **Удаление или изменение программы** выберите **Kaspersky Security Gateway** и нажмите на кнопку **Изменить**.

   Запустится Мастер установки.

4. В окне **Изменение, восстановление или удаление приложения** мастера установки нажмите на кнопку **Удаление**.

Мастер установки предложит настроить параметры удаления. Следуйте инструкциям мастера.

Шаг 1. Сохранение данных Kaspersky Security Gateway для дальнейшего использования

На этом шаге мастер установки предлагает сохранить конфигурационный файл Kaspersky Security Gateway для дальнейшего использования при последующей установке Kaspersky Security Gateway (например, при установке новой версии).

Чтобы сохранить конфигурационный файл Kaspersky Security Gateway,

установите флажок **Сохранить конфигурационный файл приложения**.

Флажок **Сохранить конфигурационный файл приложения** доступен, только если мастер установки запущен по нажатию кнопки **Изменить** в разделе **Программы и компоненты** Панели управления.

Перейдите к следующему шагу мастера.

Шаг 2. Удаление Kaspersky Security Gateway

На этом шаге мастер установки удаляет Kaspersky Security Gateway с компьютера. Дождитесь завершения удаления.

Завершите работу мастера.

При удалении Kaspersky Security Gateway может потребоваться перезагрузка операционной системы. Если немедленная перезагрузка компьютера не выполнена, удаление Kaspersky Security Gateway не завершится до перезапуска операционной системы или до выключения и повторного включения компьютера.

Установка OPC Core Components Redistributables

Начиная с Kaspersky Industrial CyberSecurity for Nodes версии 5.0 пакет OPC Core Components Redistributables не входит в пакет установки Kaspersky Security Gateway.

Если вы планируете использовать передачу данных по протоколу OPC DA, при установке Kaspersky Security Gateway версии 5.0 и выше или при обновлении приложения вам необходимо самостоятельно установить пакет OPC Core Components Redistributables, если данный пакет не был установлен другим приложением. Вы можете использовать файл opc_redist.msi, входящий в комплект поставки.

Если вы установили OPC Core Components Redistributables после установки Kaspersky Security Gateway, вам необходимо выполнить перезапуск службы Kaspersky Security Gateway OPC.

Интерфейс приложения

Приложением Kaspersky Industrial CyberSecurity for Nodes можно управлять с помощью следующих интерфейсов:

- Консоль приложения.
- Консоль администрирования Kaspersky Security Center.
- Kaspersky Security Center Web Console.

Консоль администрирования Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Industrial CyberSecurity for Nodes, а также настраивать параметры приложения, изменять набор доступных компонентов приложения, добавлять ключи, запускать и останавливать задачи.

Приложением можно управлять из Kaspersky Security Center с помощью плагина управления Kaspersky Industrial CyberSecurity for Nodes. Подробная информация об интерфейсе Kaspersky Security Center приведена в справке Kaspersky Security Center.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console – это веб-приложение, предназначенное для централизованного выполнения основных задач по управлению и поддержке системы безопасности сети организации. Kaspersky Security Center Web Console – это компонент Kaspersky Security Center, обеспечивающий пользовательский интерфейс. Подробная информация о Web Console приведена в справке Kaspersky Security Center.

Web Console позволяет выполнять следующие действия:

- Контролировать состояние системы безопасности организации.
- Устанавливать программы "Лаборатории Касперского" на устройства в сети.
- Управлять установленными приложениями.
- Просматривать отчеты о состоянии системы безопасности.

Работа с Плагином управления

Этот раздел содержит информацию о Плагине управления Kaspersky Industrial CyberSecurity for Nodes и об управлении приложением, установленном на защищаемом устройстве или группе защищаемых устройств.

Управление Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленным приложением Kaspersky Industrial CyberSecurity for Nodes, объединенными в группу администрирования, с помощью Плагина управления Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Security Center также позволяет отдельно настраивать параметры каждого защищаемого устройства, входящего в группу администрирования.

Группа администрирования формируется вручную на стороне Kaspersky Security Center. Группа администрирования включает устройства с установленным приложением Kaspersky Industrial CyberSecurity for Nodes, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в справке Kaspersky Security Center.

Параметры приложения для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Industrial CyberSecurity for Nodes на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Для запуска Плагина управления Kaspersky Industrial CyberSecurity for Nodes в Kaspersky Security Center дополнительных действий не требуется. После установки Плагина управления на защищаемое устройство администратора, он запускается вместе с любой из консолей администрирования Kaspersky Security Center.

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Настройки задачи, указанные в активной политике, имеют приоритет над настройками задачи, настроенными локально в Консоли приложения или удаленно в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center.

  С помощью политик можно настроить общие параметры приложения, параметры задач постоянной защиты компьютера, задач контроля активности на устройствах, задач защиты сетевых хранилищ и параметры запуска локальных системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств.

  С помощью групповых задач вы можете активировать приложение, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи Формирование правил контроля запуска программ.

- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.

- **С помощью окна свойств отдельного устройства**. В окне **Свойства: <Имя защищаемого устройства>** можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры приложения, так и параметры всех задач Kaspersky Industrial CyberSecurity for Nodes, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Управление параметрами приложения

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Industrial CyberSecurity for Nodes в Консоли администрирования Kaspersky Security Center.

Настройка общих параметров приложения в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Industrial CyberSecurity for Nodes из Kaspersky Security Center для группы защищаемых устройств или для отдельного защищаемого устройства.

Настройка параметров интерфейса и проверки в Kaspersky Security Center

Чтобы настроить параметры масштабируемости и интерфейс приложения, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры приложения.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры приложения для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам приложения.

4. В разделе **Настройки приложения** в блоке **Настройки интерфейса** нажмите на кнопку **Настройка**.

5. В окне **Настройки интерфейса** на закладке **Общие** настройте следующие параметры:

   - В разделе **Взаимодействие с пользователем** настройте отображение значка области уведомлений в панели задач при каждом запуске приложения.

     - **Отображать пользовательский интерфейс**. На клиентском компьютере доступен значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Industrial CyberSecurity for Nodes. Также Kaspersky Industrial CyberSecurity for Nodes показывает уведомления над значком приложения. Из контекстного меню значка в области уведомлений Windows открывается Диагностическое окно. А по ссылке в Диагностическом окне открывается Консоль программы.

     - **Не отображать пользовательский интерфейс**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Industrial CyberSecurity for Nodes. Также недоступны значок в области уведомлений Windows и уведомления.

   - В разделе **Статусы** можно указать какие предупреждения вы хотите видеть на значке Kaspersky Industrial CyberSecurity for Nodes в области уведомлений.

6. Нажмите на кнопку **ОК**.

Настроенные параметры приложения будут сохранены.

Настройка параметров безопасности в Kaspersky Security Center

Чтобы настроить параметры безопасности вручную, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры приложения.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры приложения для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам приложения.

4. В разделе **Настройки приложения** в подразделе **Безопасность и надежность** нажмите на кнопку **Настройка**.

5. В окне **Настройки безопасности** на вкладке **Безопасность** настройте следующие параметры:

   - В разделе **Общие** рекомендовано оставить включенной по умолчанию функцию **Запускать приложение при включении компьютера (рекомендуется)**.

   - В разделе **Самозащита** включите или отключите функцию **Защищать процессы приложения от внешних угроз**.

- В разделе **Действия при переходе на источник бесперебойного питания** задайте ограничение нагрузки на защищаемое устройство со стороны Kaspersky Industrial CyberSecurity for Nodes при переходе на источник бесперебойного питания:
  - **Не запускать задачи проверки по расписанию**
  - **Остановить выполняемые задачи проверки**
- В разделе **Статус компьютера при применении настроек** настройте отображение статусов клиентских компьютеров с установленным приложением при появлении ошибок применения политики или выполнения задачи.
- В разделе **Настройки совместимости** настройте параметр **Совместимость с приложениями для удаленного администрирования**.

6. На закладке **Настройки проверки** настройте следующие параметры:
   - **Ограничить потребление ресурсов процессора для задач проверки**. Kaspersky Industrial CyberSecurity for Nodes ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Максимальное значение**. Включение этой опции может негативно сказаться на производительности Kaspersky Industrial CyberSecurity for Nodes.
   - **Уступать ресурсы другим приложениям**. Потребление ресурсов компьютера Kaspersky Industrial CyberSecurity for Nodes при проверке компьютера может увеличить нагрузку на центральный процессор и дисковые подсистемы. Это может замедлить работу других приложений. Для оптимизации производительности в Kaspersky Industrial CyberSecurity for Nodes предусмотрен режим передачи ресурсов другим приложениям. В этом режиме операционная система может понизить приоритет потоков задач проверки Kaspersky Industrial CyberSecurity for Nodes при высокой нагрузке на центральный процессор. Это позволит перераспределить ресурсы операционной системы для других приложений. То есть задачи проверки получат меньше процессорного времени. В результате Kaspersky Industrial CyberSecurity for Nodes будет проверять компьютер дольше. По умолчанию режим передачи ресурсов другим приложениям включен.
7. Нажмите на кнопку **OK**.

Настроенные параметры безопасности и надежности будут сохранены.

Настройка параметров соединения в Kaspersky Security Center

Настроенные параметры соединения используются для подключения Kaspersky Industrial CyberSecurity for Nodes к серверам обновлений и активации, а также при интеграции программ со службами Kaspersky Security Network.

Чтобы настроить параметры соединения, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры приложения.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры приложения для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам приложения.

4. В разделе **Настройки приложения** в подразделе **Настройки соединения** нажмите на кнопку **Настройка**.

   Откроется окно **Настройки соединения**.

5. В разделе **Прокси-сервер** нажмите на кнопку **Настройка**.

6. В открывшемся окне в разделе **Настройки прокси-сервера** выберите один из вариантов определения настроек прокси-сервера:

   - **Не использовать прокси-сервер**. Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes не использует прокси-сервер.

   - **Автоматически определять настройки прокси-сервера.** Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует настройки прокси-сервера, заданные в параметрах операционной системы.

   - **Использовать указанный прокси-сервер**. Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует параметры прокси-сервера, указанные вручную. Введите IP-адрес или символьное имя прокси-сервера и номер порта.

     При необходимости снимите флажок **Не использовать прокси-сервер для локальных адресов**. Если функция включена, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленным приложением Kaspersky Industrial CyberSecurity for Nodes, происходит напрямую, прокси-сервер не используется. По умолчанию функция включена.

7. В разделе **Настройки аутентификации на прокси-сервере** выберите в раскрывающемся списке метод аутентификации на прокси-сервере:

   a. Если вы выбрали вариант **Автоматически определять настройки прокси-сервера**:

      - **Не использовать аутентификацию**.

      - **NTLM-аутентификация**. NTLM-аутентификация с помощью учетной записи текущего пользователя (значение по умолчанию).

      - **Kerberos-аутентификация**. Kerberos-аутентификация с помощью учетной записи текущего пользователя.

   b. Если вы выбрали вариант **Использовать указанный прокси-сервер**:

      - **Не использовать аутентификацию**.

      - **NTLM-аутентификация**. NTLM-аутентификация с помощью учетной записи текущего пользователя (значение по умолчанию).

      - **NTLM-аутентификация с именем пользователя и паролем.** NTLM-аутентификация с помощью учетных данных, заданных вручную.

- **Kerberos-аутентификация**. Kerberos-аутентификация с помощью учетной записи текущего пользователя.

  Для обеспечения корректной работы Kerberos-аутентификации при использовании CNAME-записей для адреса прокси-сервера вам необходимо зарегистрировать имя субъекта-службы (SPN) для каждой CNAME-записи.

- **Kerberos-аутентификация с именем пользователя и паролем**. Kerberos-аутентификация с использованием учетных данных, заданных вручную.

- **Имя пользователя и пароль**. Аутентификация с использованием учетных данных, заданных вручную.

При необходимости введите имя пользователя и пароль.

Если выбрана Kerberos-аутентификация, Kaspersky Industrial CyberSecurity for Nodes может в зависимости от настроек прокси-сервера осуществлять аутентификацию как по протоколу Kerberos, так и по протоколу NTLM.

8. В разделе **Лицензирование** установите или снимите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения**.

9. Нажмите на кнопку **OK**.

10. В разделе **Контролируемые порты** укажите вариант контроля сетевых портов:

    - **Контролировать все сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты контролируют потоки данных, передаваемые через любые открытые сетевые порты компьютера.

    - **Контролировать только выбранные сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты контролируют выбранные сетевые порты компьютера и сетевую активность выбранных приложений. Список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика, настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского". При необходимости вы можете редактировать список сетевых портов.

11. Нажмите на кнопку **Настройка** и настройте следующие параметры:

    - **Контролировать все порты для приложений из списка, рекомендованного "Лабораторией Касперского"**. Kaspersky Industrial CyberSecurity for Nodes контролирует сетевые порты приложений из предустановленного списка. В список включены, например, Google Chrome, Adobe Reader, Java и другие приложения.

    - **Контролировать все порты для указанных приложений**. Kaspersky Industrial CyberSecurity for Nodes контролирует сетевые порты приложений, добавленных в список.

12. Нажмите на кнопку **OK**.

Настроенные параметры соединения будут сохранены.

Настройка режима запуска локальных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления. Запуск осуществляется по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.

- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Industrial CyberSecurity for Nodes будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: *Проверка важных областей*, *Проверка при старте операционной системы*, *Проверка целостности приложения*, *Мониторинг целостности системы на основе эталона*.

- Задачи обновления: *Обновление баз и модулей приложения*, *Обновление приложения*.

Если защищаемое устройство исключено из группы администрирования, расписание локальных системных задач будет автоматически включено.

Чтобы разрешить или запретить в политике настройку режима запуска локальных задач приложения:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**, разверните нужную группу и в панели результатов выберите закладку **Политики**.

2. На закладке **Политики** в контекстном меню политики, для которой вы хотите настроить запуск по расписанию локальных системных задач Kaspersky Industrial CyberSecurity for Nodes для группы защищаемых устройств, выберите пункт **Свойства**.

3. В окне свойств политики выберите раздел **Настройки приложения**.

4. Нажмите на кнопку **Настройка** в подразделе **Запуск локальных системных задач**.

5. Установите флажок **Разрешить использование локальных задач**.

6. Используйте флажок **Разрешить управление расписанием**, чтобы разрешить или запретить настройку режима запуска локальных задач приложения.

Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

Чтобы настроить общие параметры карантина и резервного хранилища в Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры приложения.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры приложения для группы защищаемых устройств, выберите вкладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры задачи или программы для отдельного защищаемого устройства, выберите вкладку **Устройства** и перейдите к параметрам локальной задачи или параметрам приложения.

4. Перейдите в раздел **Дополнительные возможности**.

5. В подразделе **Хранилища** нажмите на кнопку **Настройка**.

6. Настройте параметры, которые приведены в следующей таблице.

Настройки хранилища

Параметр	Описание
На вкладке **Отчеты** укажите настройки отчетов:	
Хранить отчеты не более	Если флажок установлен, то максимальный срок хранения отчетов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения отчетов составляет 30 дней. По истечении этого времени Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые записи из файла отчета.
Ограничить размер файла отчетов до	Если флажок установлен, то максимальный размер файла отчетов ограничен заданным значением. По умолчанию максимальный размер файла составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые записи из файла отчетов таким образом, чтобы размер файла отчетов не превышал максимального значения.
На вкладке **Резервное хранилище** укажите настройки резервного хранилища:	
Хранить объекты не более	Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения файлов составляет 30 дней. По истечении максимального срока хранения Kaspersky Industrial CyberSecurity for Nodes удаляет наиболее старые файлы из резервного хранилища.
Ограничить размер хранилища до	Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 400 МБ. После достижения максимального размера резервного хранилища приложение Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.

Параметр	Описание
Порог доступного пространства	Флажок включает или выключает отслеживание минимального объема свободного места в резервном хранилище (по умолчанию 100 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен порог свободного места в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отслеживает размер свободного места в резервном хранилище. Флажок **Порог доступного пространства** активен, если установлен флажок **Ограничить размер хранилища до**.
На вкладке **Карантин** укажите настройки карантина:	
Ограничить размер карантина до	Если функция включена, Kaspersky Industrial CyberSecurity for Nodes отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 1024 МБ) Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен максимальный размер карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа. При этом приложение прекращает помещать новые объекты на карантин. Вам нужно вручную очистить карантин. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes не отслеживает суммарный размер объектов в карантине. По умолчанию функция выключена.
Порог доступного пространства	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отслеживает минимальный объем свободного места в папке карантина (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен порог свободного места в карантине* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа. Флажок **Порог доступного пространства** активен, если установлен флажок **Ограничить размер карантина до**. По умолчанию функция включена.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Industrial CyberSecurity for Nodes на нескольких защищаемых устройствах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлено приложение Kaspersky Industrial CyberSecurity for Nodes.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Industrial CyberSecurity for Nodes на всех защищаемых устройствах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, имеет статус *Активная* в Консоли администрирования.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Industrial CyberSecurity for Nodes. Вы можете просмотреть эту информацию в Консоли приложения в узле **Анализ журналов**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых устройствах: *Запретить редактирование параметров*. После применения политики Kaspersky Industrial CyberSecurity for Nodes использует на защищаемых устройствах значения параметров, для которых в свойствах политики вы указали, что **Редактирование запрещено** . В этом случае Kaspersky Industrial CyberSecurity for Nodes не использует значения параметров, действовавшие до применения политики. Kaspersky Industrial CyberSecurity for Nodes не применяет значения параметров активной политики, для которых в свойствах политики выбран вариант **Редактирование разрешено** .

Если политика активна, то значения параметров, отмеченные в политике значком , отображаются в Консоли приложения, но недоступны для редактирования. Значения остальных параметров доступны для редактирования в Консоли приложения.

Параметры, настроенные в активной политике и отмеченные значком , также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемое устройство с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры задачи Постоянная защита компьютера или Защита сетевых хранилищ, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

Создание политики

Перед созданием политики необходимо установить плагин администрирования klcfginst.exe.

Чтобы создать политику для группы защищаемых устройств, на которых установлено и запущено приложение:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для защищаемых устройств которой вы хотите создать политику.
2. В панели результатов выбранной группы администрирования выберите вкладку **Политики** и запустите мастер создания политик по кнопке **Новая политика**.

   Откроется окно **Мастер создания политики**.
3. В окне **Выбор приложения для создания групповой политики** выберите Kaspersky Industrial CyberSecurity for Nodes.
4. Нажмите на кнопку **Далее**.
5. В поле **Имя** укажите название групповой политики.

   Имя политики не должно содержать следующие символы: `" * < : > ? \ | .`
6. Чтобы применить параметры политики, используемые в предыдущей версии программы, выполните следующие действия:

   a. Установите флажок **Использовать параметры политики для предыдущей версии приложения**.

   b. Нажмите на кнопку **Обзор**.

   c. Выберите политику, которую требуется применить.

   d. Нажмите на кнопку **Далее**.

7. В окне **Выбор типа операции** в блоке **Настройки Постоянной защиты файлов** установите флажок **Включить Постоянную защиту файлов** и укажите уровень безопасности.

   Если режим работы задачи не выбран, вы не можете перейти на следующий шаг Мастера создания политики.

8. Укажите настройки Постоянной защиты компьютера.

9. Настройте исключения из проверки и доверенные приложения.

10. В окне **Создание групповой политики для приложения** выберите одно из следующих состояний политики:

    - **Активная политика**, если требуется, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, то она станет неактивной и будет применена новая созданная политика.
    - **Неактивная политика**, если сразу применять созданную политику не требуется. Вы сможете активировать эту политику позже.
    - **Политика для автономных пользователей** активируется, когда компьютер покидает периметр сети организации.
    - Установите флажок **Открыть свойства политики сразу после создания**, чтобы автоматически закрыть **Мастер создания политики** и настроить новую политику после нажатия на кнопку **Далее**.

11. Нажмите на кнопку **Готово**.

    Созданная политика отобразится в списке политик на вкладке **Политики** выбранной группы администрирования. В окне **Свойства: <Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Industrial CyberSecurity for Nodes.

После создания новой политики создается набор разрешающих правил для предотвращения блокировки программ и обеспечения их непрерывной работы.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes создает набор правил для входящего сетевого трафика при создании новой политики:

- Два разрешающих правила для процесса совместного доступа к рабочему столу Windows с помощью Агента администрирования Kaspersky Security Center, расположенных в папках %Program Files% и %Program Files (x86)%. Статус: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.
- Два разрешающих правила для локального порта 15000. Состояние: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes создает набор правил для исходящего сетевого трафика при создании новой политики:

- Два разрешающих правила для службы Kaspersky Industrial CyberSecurity for Nodes, расположенных в папках %Program Files% и %Program Files (x86)%. Статус: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.
- Два разрешающих правила для рабочего процесса Kaspersky Industrial CyberSecurity for Nodes, расположенных в папках %Program Files% и %Program Files (x86)%. Статус: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.
- Два разрешающих правила для локального порта 13000. Состояние: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.

Настройка политики

Чтобы настроить параметры политики, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Разверните группу администрирования, параметры политики которой вы хотите настроить, и выберите в панели результатов закладку **Политики**.
3. Выберите политику, параметры которой вы хотите настроить.

   Откройте окно **Свойства: <Имя политики>** одним из следующих способов:

   - Выберите параметр **Свойства** в контекстном меню политики.
   - Дважды щелкните мышью по нужной политике.
4. На закладке **Общие** в разделе **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:

   - **Активная политика**, если вы хотите, чтобы политика применялась на всех защищаемых устройствах, входящих в выбранную группу администрирования.
   - **Политика для автономных пользователей** – активируется, когда компьютер покидает периметр сети организации.
   - **Неактивная политика**, если вы хотите активировать политику позже на всех защищаемых устройствах, входящих в выбранную группу администрирования.
5. Настройте параметры приложения в остальных разделах политики.

Вы можете включать и выключать выполнение любой задачи на всех защищаемых устройствах, входящих в группу администрирования, с помощью политики Kaspersky Security Center.

Вы можете настроить применение параметров политики на всех защищаемых устройствах сети для каждого отдельного компонента программы.

6. Нажмите на кнопку **OK**.

Настроенные параметры будут применены в политике.

Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Industrial CyberSecurity for Nodes, их создании, настройке параметров выполнения, запуске и остановке.

О создании задач в Kaspersky Security Center

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых устройств. Вы можете создавать задачи следующих типов в Kaspersky Security Center:

- *Активация приложения*;
- *Аудит безопасности*;
- *Завершение процесса*;
- *Запуск процесса*;
- *Защита подключения к Серверу администрирования*;
- *Изменение состава компонентов Kaspersky Industrial CyberSecurity for Nodes*;
- *Мониторинг целостности системы на основе эталона*;
- *Обновление*;
- *Откат обновления*;
- *Поиск IOC*;
- *Получение файла*;
- *Помещение файла на карантин*;
- *Проверка по требованию*;
- *Проверка целостности приложения*;
- *Удаление ключа*;

- *Удаление файла*;
- *Формирование правил контроля запуска программ*;
- *Формирование правил контроля устройств*.

Вы можете создать локальные и групповые задачи следующими способами:

- Для отдельного защищаемого устройства в разделе **Задачи**.
- Для группы администрирования: в панели результатов узла выбранной группы защищаемых устройств на закладке **Задачи**.
- Для набора защищаемых устройств: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач *Обновление* и *Проверка по требованию* на всех защищаемых устройствах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center приведена в справке Kaspersky Security Center.

Создание задачи в Kaspersky Security Center

Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center:

1. Запустите мастер создания задачи одним из следующих способов:
   - Для создания локальной задачи:
     a. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый сервер.
     b. В панели результатов на вкладке **Устройства** откройте контекстное меню защищаемого устройства и выберите пункт **Свойства**.
     c. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.
   - Для создания групповой задачи:
     a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
     b. Выберите группу администрирования, для которой требуется создать задачу.
     c. В панели результатов перейдите на вкладку **Задачи** и выберите пункт **Новая задача**.

   Откроется окно мастера создания задачи.
2. В окне **Выбор типа задачи** под заголовком **Kaspersky Industrial CyberSecurity for Nodes** выберите тип создаваемой задачи.

3. В зависимости от типа задачи параметры могут различаться.

   - Создайте задачу проверки по требованию.

   - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:

     a. В блоке **Источник обновлений** можно указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

        Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

     b. Настройте параметры функции, снижающей нагрузку на дисковую подсистему:

     c. Вы можете указать действия, которые Kaspersky Industrial CyberSecurity for Nodes будет совершать при наличии критических обновлений модулей программы, а также по завершении установки критических обновлений. Кроме того, можно указать, будет ли Kaspersky Industrial CyberSecurity for Nodes получать информацию о доступных плановых обновлениях.

     d. Укажите состав обновлений для копирования и путь к папке, в которой Kaspersky Industrial CyberSecurity for Nodes будет сохранять скопированные обновления.

   - Для создания задачи *Активация приложения*:

     a. В окне **Настройки активации** укажите файл ключа или код активации, с помощью которого вы хотите активировать программу.

     b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.

   - Создайте задачу Формирование правил контроля запуска программ.

   - Создайте задачу Формирование правил контроля устройств.

4. Настройте расписание задачи.

5. Нажмите на кнопку **OK**.

6. Если задача создана для набора защищаемых устройств, выберите сеть (группу) защищаемых устройств, на которых она будет выполняться.

7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, которую вы хотите использовать для запуска задачи.

8. В окне **Определение названия задачи** введите название задачи (не более 100 символов, не должно содержать символы `" * < > ? \ | :`).

   Рекомендуется включить в название задачи ее тип (например, Проверка по требованию общих папок).

9. В окне **Завершение создания задачи** выполните следующие действия:

    a. Установите флажок **Запустить задачу после завершения работы мастера**, если вы хотите запустить задачу сразу после создания.

    b. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

Переход к параметрам локальной задачи и общим параметрам приложения для отдельного компьютера

Если приложение работает под управлением политики Kaspersky Security Center и в этой политике запрещено изменять параметры программы, эти параметры недоступны для изменения для отдельного компьютера.

Чтобы перейти к параметрам локальной задачи для отдельного компьютера:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите вкладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:

    - двойным щелчком мыши на имени защищаемого устройства;
    - в контекстном меню на имени защищаемого устройства выберите пункт **Свойства**.

    Откроется окно **Свойства: <Имя защищаемого устройства>**.

5. Перейдите в раздел **Задачи**.
6. В списке задач выберите локальную задачу, параметры которой требуется настроить, одним из следующих способов:

    - двойным щелчком мыши на названии задачи;
    - выберите задачу в списке и нажмите на кнопку **Свойства**;
    - в контекстном меню на имени задачи выберите пункт **Свойства**.

    Откроется окно **Свойства: <Название задачи>**.

Чтобы перейти к общим параметрам приложения для отдельного компьютера:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемое устройство.
2. В панели результатов выберите закладку **Устройства**.

3. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:

   - двойным щелчком мыши на имени защищаемого устройства;
   - в контекстном меню на имени защищаемого устройства выберите пункт **Свойства**.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.

4. Перейдите в раздел **Программы**.

5. В списке установленных программ выберите Kaspersky Industrial CyberSecurity for Nodes одним из следующих способов:

   - двойным щелчком мыши на имени Kaspersky Industrial CyberSecurity for Nodes;
   - выберите Kaspersky Industrial CyberSecurity for Nodes в списке и нажмите на кнопку **Свойства**;
   - в контекстном меню на имени Kaspersky Industrial CyberSecurity for Nodes выберите пункт **Свойства**.

   Откроется окно **Параметры Kaspersky Industrial CyberSecurity for Nodes**.

Настройка групповых задач в Kaspersky Security Center

Чтобы настроить групповую задачу для нескольких защищаемых устройств, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.

2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.

3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.

4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:

   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить параметры задачи**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

5. В разделе **Уведомление** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в справке Kaspersky Security Center.

6. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:

   - Если вы настраиваете задачу *Проверка по требованию*:
     - В разделе **Область проверки** настройте область проверки.
     - В разделе **Настройки** настройте приоритет задачи и интеграцию с другими компонентами программы.

- Чтобы настроить параметры задачи *Обновление*, выполните следующие действия:
  - Перейдите в раздел **Настройки** и укажите **Настройки обновления баз и модулей приложения**.
  - Выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
- Чтобы настроить задачу *Активация приложения*, выполните следующие действия:
  - В разделе **Настройки** укажите файл ключа или код активации, с помощью которого вы хотите активировать программу.
  - Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
- Чтобы настроить задачу *Формирование правил контроля устройств*, в разделе **Настройки** укажите параметры, на основе которых будет сформирован список правил контроля устройств.

7. Настройте расписание задачи в разделе **Расписание**.
8. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе приведена в справке Kaspersky Security Center.
9. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи. Подробная информация о настройке параметров в этом разделе приведена в справке Kaspersky Security Center.
10. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Настраиваемые параметры групповых задач приведены далее:

- Формирование правил контроля запуска программ

  При настройке параметров задачи *Формирование правил контроля запуска программ* вы можете выбрать способ создания разрешающих правил на закладке **Правила**:

  - **Создавать разрешающие правила на основе запущенных приложений**
  - **Создавать разрешающие правила для приложений из папок**

  Вы можете указать следующие действия при формировании разрешающих правил контроля запуска программ на закладке **Настройки**:

  - **Использовать цифровой сертификат**
  - **Использовать заголовок и отпечаток цифрового сертификата**
  - **Если сертификат отсутствует, использовать**
  - **Использовать хеш SHA256**
  - **Формировать правила для пользователей и / или групп пользователей**

Вы можете настроить параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Industrial CyberSecurity for Nodes создает по завершении задачи.

Вы можете настроить расписание запуска задачи.

- Формирование правил контроля устройств
  - Выберите режим работы: учитывать данные системы обо всех когда-либо подключавшихся внешних устройствах или только о подключенных в настоящий момент внешних устройствах.
  - Настройте параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Industrial CyberSecurity for Nodes создает по завершении задачи.
  - Вы можете настроить расписание запуска задачи.
- Активация приложения
  - Вы можете применить код активации или файл ключа для активации программы или продления срока действия лицензии.
  - Вы можете настроить расписание запуска задачи.
- Обновление баз и модулей приложения
  - В блоке параметров **Источник обновлений** можно указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

    Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
  - Вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему:
    - **Снизить нагрузку на дисковую подсистему**
    - **Объем оперативной памяти, используемой для оптимизации (МБ)**
  - Вы можете указать действия, которые Kaspersky Industrial CyberSecurity for Nodes будет совершать при наличии критических обновлений модулей приложения, а также по завершении установки критических обновлений. Кроме того, можно указать, будет ли Kaspersky Industrial CyberSecurity for Nodes получать информацию о доступных плановых обновлениях.
  - Вы можете указать состав обновлений для копирования и путь к папке, в которой Kaspersky Industrial CyberSecurity for Nodes будет сохранять скопированные обновления.
  - Вы можете настроить расписание запуска задачи.
- Проверка по требованию
  - Вы можете сформировать область проверки для задачи проверки по требованию и настроить параметры уровня безопасности.
  - В блоке параметров **Эвристический анализатор** вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка.

- В блоке **Интеграция с другими компонентами** можно настроить следующие параметры:
  - запуск задачи проверки в фоновом режиме;
  - считать выполнение задачи проверкой важных областей;
  - не запускать несколько задач проверки одновременно.
- Вы можете настроить расписание запуска задачи.

- Проверка целостности приложения
  - Вы можете настроить расписание запуска задачи.

- Мониторинг целостности системы на основе эталона
  - Вы можете настроить режим мониторинга и настроить правила действия с файлами, реестром и устройствами.
  - Вы можете настроить расписание запуска задачи.

Задача Активация приложения

Чтобы настроить задачу Активация приложения, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомление** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в справке Kaspersky Security Center.
5. В разделе **Настройки активации** укажите файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить ключ для продления срока действия лицензии.
6. В разделе **Расписание** настройте параметры расписания задачи.

7. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в справке Kaspersky Security Center.

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповой задачи будут сохранены.

Задача обновления

Чтобы настроить задачу Обновление, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.

2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.

3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.

4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:

   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

5. В разделе **Уведомление** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в справке Kaspersky Security Center.

6. В разделе **Настройки** выполните следующие действия:

   a. Выберите источник обновлений по кнопке **Настройка** в разделе **Настройки обновления баз и модулей приложения**:

      - Сервер администрирования Kaspersky Security Center.
      - Серверы обновлений "Лаборатории Касперского".
      - Другие HTTP-, FTP-серверы и сетевые ресурсы.

      Чтобы использовать в качестве источника обновлений общую папку SMB, необходимо указать учетную запись, с правами которой запускается задача.

      Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

   b. Настройте параметры функции, снижающей нагрузку на дисковую подсистему:

      - **Снизить нагрузку на дисковую подсистему**. Флажок включает или выключает процесс оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти. По умолчанию флажок снят.
      - **Объем оперативной памяти, используемой для оптимизации (МБ)**.

c. Укажите действия, которые Kaspersky Industrial CyberSecurity for Nodes будет совершать при наличии критических обновлений модулей приложения или при наличии информации о плановых обновлениях.

d. Укажите настройки копирования обновлений.

7. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления).

8. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

> Подробная информация о настройке параметров в этих разделах приведена в справке Kaspersky Security Center.

9. В окне **Свойства: <Имя задачи>** нажмите кнопку **ОК**.

Для задачи *Откат обновления* можно настроить только стандартные параметры задачи, контролируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этих разделах приведена в справке Kaspersky Security Center.

Проверка целостности приложения

Чтобы настроить групповую задачу Проверка целостности приложения, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.

2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.

3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить.

4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:

   - Выберите название задачи в списке созданных задач двойным щелчком мыши.

   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

5. В разделе **Уведомление** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в справке Kaspersky Security Center.

6. В разделе **Устройства** выберите устройства, для которых требуется настроить задачу *Проверка целостности приложения*.

7. В разделе **Расписание** настройте параметры расписания задачи.

8. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

9. Если требуется, в разделе **Исключения из области действия задачи** укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этих разделах приведена в справке Kaspersky Security Center.

10. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

Настройка расписания задач

Чтобы настроить расписание задач с помощью Плагина управления, выполните следующие действия:

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный компьютер.
2. В рабочей области выберите вкладку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. Перейдите в раздел **Задачи**.
5. Двойным щелчком мыши откройте окно свойств задачи, для которой вы хотите настроить расписание.
6. Выберите раздел **Расписание**.
7. Настройте параметры расписания (см. таблицу ниже) в соответствии с вашими требованиями.

   Поля с параметрами расписания задач проверки по требованию и обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

8. Нажмите на кнопку **Применить**, чтобы сохранить параметры запуска задачи.

Если вы хотите настроить Параметры приложения для отдельной задачи с помощью Kaspersky Security Center, см. раздел "Настройка локальных задач в окне Параметры приложения в Kaspersky Security Center".

Параметры расписания задач

Параметр	Описание
Запуск по расписанию	Выберите режим запуска задачи: • **Каждый N час**. Задача будет запускаться с периодичностью в заданное количество часов. Укажите время запуска задачи и период в часах. • **Каждые N дней**. Задача будет запускаться с периодичностью в заданное количество дней. Укажите время запуска задачи и период в днях. • **Каждые N минут**. Задача будет запускаться с периодичностью в заданное количество минут. Укажите время запуска задачи и период в минутах. • **Еженедельно**. Задача будет запускаться в определенный день недели. Укажите день недели и время запуска. • **Ежемесячно**. Задача будет запускаться в определенный день месяца. Укажите число и время запуска. • **Один раз**. Задача будет запускаться однократно в указанный день и время. • **Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. • **При загрузке обновлений в хранилище**. Задача будет запускаться после каждой загрузки обновлений в хранилище. • **По завершении другой задачи**. Задача будет запускаться после завершения другой задачи. Выберите задачу и статус ее выполнения. Kaspersky Industrial CyberSecurity for Nodes не поддерживает режим **По завершении другой задачи** для настройки расписания локальных задач. • **При обнаружении вирусной атаки**. Задача будет запускаться в случае обнаружения вирусной атаки. • **При запуске приложения**. Задача будет запускаться при каждом запуске Kaspersky Industrial CyberSecurity for Nodes.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.
Использовать автоматическое определение случайного интервала между запусками задачи	Если флажок установлен, задача запускается на компьютерах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Использовать случайную задержку запуска задачи в интервале (мин)	Если флажок установлен, задача запускается на компьютерах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Включать устройства перед запуском задачи функцией Wake-on-LAN	Если флажок установлен, операционная система на компьютере будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут. Установите флажок, если вы хотите запустить выполнение задачи на всех компьютерах, включая компьютеры, которые выключены.
Выключать устройства после выполнения задачи	Если флажок установлен, компьютер будет выключен после выполнения задачи. Например, вы можете включить эту функцию для проверки компьютера в пятницу после рабочего дня. После завершения работы задачи приложение выключает компьютер на выходные.
Остановить, если задача выполняется дольше	Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Industrial CyberSecurity for Nodes останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Industrial CyberSecurity for Nodes выполнит сначала и по расписанию.

Параметр	Описание
Приостановить задачу	Вы можете задавать временной интервал, в течение которого выполнение ранее запущенной по расписанию задачи будет приостановлено. По окончании заданного периода времени выполнение задачи будет возобновлено. Это может понадобиться, например, для снижения влияния Kaspersky Industrial CyberSecurity for Nodes на производительность компьютера в период наиболее активного его использования. Данная функция доступна только для задач проверки по требованию.
Выключить расписание с	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes прекратит выполнение задачи по расписанию начиная с указанной даты. Для задачи будет установлен режим запуска **Вручную**. Данная функция доступна только для задач проверки по требованию.

Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Industrial CyberSecurity for Nodes доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о работе с отчетами Kaspersky Security Center см. в справке Kaspersky Security Center.

Отчет о статусе компонентов Kaspersky Industrial CyberSecurity for Nodes

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Выполняется*, *Приостановлено*, *Остановлено*, *Не поддерживается лицензией*.

Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в справке Kaspersky Security Center.

Чтобы просмотреть статусы компонентов в параметрах программы, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить Параметры приложения.
2. Выберите закладку **Устройства** и откройте окно **Параметры приложения**.
3. Выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

Чтобы просмотреть стандартный отчет Kaspersky Security Center, выполните следующие действия:

1. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
2. Выберите закладку **Отчеты**.
3. Откройте **Отчет о статусе компонентов программы** двойным щелчком мыши.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
   - детальная таблица, показывающая статус, версию, устройство и группу компонента.

Отчеты о запрещенных программах в активном и в тестовом режимах

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Информировать). В этих отчетах приведена информация о заблокированных программах на защищаемых устройствах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

Чтобы просмотреть отчет о запрещенных программах в режиме Информировать, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме Информировать.
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.

3. Выберите закладку **Отчеты**.

4. Откройте **Отчет о запрещенных программах в тестовом режиме** двойным щелчком мыши.

   Будет сформирован отчет.

5. Ознакомьтесь со следующими элементами отчета:

   - диаграмма, показывающая 10 программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

Чтобы просмотреть отчет о запрещенных программах в Активном режиме, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме Активный.

2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.

3. Выберите закладку **Отчеты**.

4. Откройте **Отчет о запрещенных программах** двойным щелчком мыши.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

Статус постоянной защиты

Kaspersky Industrial CyberSecurity for Nodes передает на Сервер администрирования Kaspersky Security Center параметр **Статус постоянной защиты**, значение которого зависит от текущего состояния компонентов защиты приложения на защищаемом устройстве (см. таблицу ниже).

Kaspersky Industrial CyberSecurity for Nodes определяет статус постоянной защиты на основе состояния следующих компонентов приложения:

- Постоянная защита файлов;
- Контроль устройств;
- Сетевой экран;
- Защита от сетевых угроз;
- AMSI-защита;
- Защита от шифрования;
- Защита от атак BadUSB;

- Откат вредоносных действий;
- Защита от эксплойтов.

Вы можете узнать статус постоянной защиты приложения в консоли Kaspersky Security Center.

Как узнать статус постоянной защиты в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Управляемые устройства**.

   В списке устройств в графе **Статус постоянной защиты** отображается текущее значение статуса постоянной защиты. Если графа **Статус постоянной защиты** отсутствует, настройте параметры столбцов, нажав на ссылку **Добавить или удалить столбцы**.

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Управляемые устройства**.

   В списке устройств в графе **Статус постоянной защиты** отображается текущее значение статуса постоянной защиты. Если графа **Статус постоянной защиты** отсутствует, настройте параметры столбцов, нажав на ссылку **Добавить или удалить столбцы**.

Как узнать статус постоянной защиты в Web Console

В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

В списке устройств в графе **Статус постоянной защиты** отображается текущее значение статуса постоянной защиты. Если графа **Статус постоянной защиты** отсутствует, настройте параметры столбцов (⚙).

Возможные значения параметра Статус постоянной защиты

Значение	Описание
Нет данных	На Сервере администрирования отсутствует информация о статусе постоянной защиты для данного устройства.
Не установлен	Ни один из компонентов не установлен.
Не поддерживается лицензией	Приложение не активировано или лицензия не допускает работу установленных компонентов.
Сбой	В работе одного или нескольких компонентов произошел сбой.
Остановлен	Один или несколько компонентов выключены.
Приостановлена	Работа одного или нескольких компонентов приостановлена.
Запускается	Выполняется включение одного или нескольких компонентов.
Выполняется	Компоненты приложения включены и работают.

Если в Kaspersky Security Center значение параметра **Статус постоянной защиты** отлично от *Выполняется*, проверьте, что установленные компоненты Kaspersky Industrial CyberSecurity for Nodes из списка включены и приложение активировано.

Работа с Консолью Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит информацию о Консоли Kaspersky Industrial CyberSecurity for Nodes и об управлении программой через Консоль Kaspersky Industrial CyberSecurity for Nodes, установленную на защищаемом устройстве или другом устройстве.

Запуск Консоли приложения

Чтобы запустить Консоль приложения:

1. Откройте Диагностическое окно одним из следующих способов:

   - Запустите файл avpui.exe, расположенный в папке установки приложения на защищаемом устройстве. По умолчанию файл расположен в папке C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.

   - Нажмите на значок приложения в области уведомлений панели задач.

2. В открывшемся Диагностическом окне нажмите на ссылку **Консоль Kaspersky Industrial CyberSecurity for Nodes**.

   Если вы уже настраивали подключение к защищаемому устройству, откроется Консоль приложения.

   Если вы запускаете Консоль приложения впервые, откроется окно **Выбор защищаемого устройства**, в котором необходимо указать настройки для подключения Консоли приложения к защищаемому компьютеру.

   > Консоль приложения версии 4.5 несовместима с Kaspersky Industrial CyberSecurity for Nodes версии 5.0 и выше. При попытке подключения вам будет предложено установить пакет совместимости для Консоли приложения. Пакет совместимости будет загружен с устройства, к которому выполняется подключение.

Интерфейс Консоли Kaspersky Industrial CyberSecurity for Nodes

В этом разделе описаны основные элементы интерфейса приложения.

Окно Консоли Kaspersky Industrial CyberSecurity for Nodes

После подключения к приложению Kaspersky Industrial CyberSecurity for Nodes, установленной на другом защищаемом устройстве, в название узла добавляется имя защищаемого устройства, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Industrial CyberSecurity for Nodes <Имя защищаемого устройства> как <имя учетной записи>**. При подключении к программе Kaspersky Industrial CyberSecurity for Nodes, установленной на том же защищаемом устройстве, что и Консоль Kaspersky Industrial CyberSecurity for Nodes, название узла имеет вид Kaspersky Industrial CyberSecurity for Nodes.

Дерево Консоли

В дереве Консоли приложения отображается узел Kaspersky Industrial CyberSecurity for Nodes и вложенные узлы функциональных компонентов программы.

Узел **Kaspersky Industrial CyberSecurity for Nodes** содержит следующие вложенные узлы:

- **Постоянная защита компьютера** позволяет управлять следующими задачами:
  - **Постоянная защита файлов**
  - **Kaspersky Security Network**
  - **Защита от эксплойтов**
  - **Защита от сетевых угроз**
  - **Защита от шифрования**
  - **Откат вредоносных действий**
  - **AMSI-защита**
- **Настройки телеметрии**: настройка параметров телеметрии, отправляемой приложением в адрес совместимых решений Detection and Response и SIEM-систем.
- **Контроль компьютера**: контроль приложений, запускаемых на защищаемом устройстве, и подключаемых устройств.
  - **Контроль запуска программ**
  - **Контроль устройств**
  - **Сетевой экран**
- **Автоматическое формирование правил**: настройка автоматического формирования групповых и системных правил для компонентов Контроль запуска программ и Контроль устройств.
  - **Формирование правил контроля запуска программ**
  - **Формирование правил контроля устройств**

- Групповые задачи формирования правил **<Имена задач>** (если есть)

  Групповые задачи создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль Kaspersky Industrial CyberSecurity for Nodes.

- **Мониторинг целостности системы**: настройка параметров контроля целостности системы и анализа журнала событий Windows.
  - **Анализ журналов**
  - **Контроль целостности системы**
- **Защита промышленной сети**, получение информации о защищаемых ПЛК и проверка их целостности.
  - **Проверка целостности проектов ПЛК**
  - **Получение данных о проектах ПЛК**
- **Проверка по требованию**: управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы**
  - **Проверка важных областей**
  - **Проверка целостности приложения**
  - **Проверка съемных дисков**
  - **Полная проверка**
  - Пользовательские задачи **<Имена задач>** (если есть)

  В узле отображаются системные задачи, созданные при установке программы, пользовательские задачи и групповые задачи проверки по требованию, сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Обновление**: управление обновлением баз и модулей Kaspersky Industrial CyberSecurity for Nodes, а также возможность отката последнего обновления:
  - **Обновление баз и модулей приложения**
  - **Откат последнего обновления**
  - **Обновление приложения**

  В узле отображаются все пользовательские и групповые задачи обновлений, сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Хранилища**: управление параметрами резервного копирования и списка заблокированных сетевых сеансов.
  - **Резервное хранилище**
  - **Заблокированные сетевые сессии**

- **Журналы и уведомления**: управление журналами выполнения локальных задач и журналом системного аудита Kaspersky Industrial CyberSecurity for Nodes.
  - **Системный аудит**
  - **Защита промышленной сети**
  - **Контроль запуска программ**
  - **Контроль устройств**
  - **Проверка целостности приложения**
  - **Анализ журналов**
  - **Контроль целостности системы**
  - **Защита от сетевых угроз**
  - **Проверка по требованию**
  - **Сетевой экран**
  - **Защита от эксплойтов**
  - **Защита от шифрования**
  - **AMSI-защита**
  - **Обновление**
  - **Постоянная защита файлов**
  - **Резервное хранилище**
  - **Endpoint Detection and Response (Industrial CyberSecurity)**
- **Лицензирование**: добавление и удаление ключей Kaspersky Industrial CyberSecurity for Nodes, просмотр информации о лицензиях.

Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Industrial CyberSecurity for Nodes**, в панели результатов отобразится информация о текущем состоянии защиты устройства, информация о Kaspersky Industrial CyberSecurity for Nodes, состоянии защиты функциональных компонентов программы и статусе ключа.

Контекстное меню узла Kaspersky Industrial CyberSecurity for Nodes

С помощью пунктов контекстного меню узла **Kaspersky Industrial CyberSecurity for Nodes** можно выполнять следующие операции:

- **Приостановить защиту**.
- **Доверенная зона**. Просмотреть и настроить параметры доверенной зоны.
- **Настройки телеметрии Интеграции с KATA / Интеграции с KICS for Networks**.
- **Проверка съемных дисков**. Настроить проверку съемных дисков, подключенных к защищаемому устройству по USB.
- **Права пользователей на управление приложением**. Просмотреть и настроить права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes.
- **Права пользователей на управление службой KICS for Nodes Service**. Просмотреть и настроить права пользователя на управление службой Kaspersky Industrial CyberSecurity for Nodes Service.
- **Хранилища**.
- **Экспортировать настройки**. Сохранить настройки программы в конфигурационный файл в формате XML. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Импортировать настройки**. Импортировать настройки программы из конфигурационного файла в формате XML. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Обновить**. Обновить содержимое окна Консоли Kaspersky Industrial CyberSecurity for Nodes. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Свойства приложения**. Просмотреть и настроить параметры работы Kaspersky Industrial CyberSecurity for Nodes или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

  Для выполнения этой операции также можно воспользоваться ссылкой **Свойства приложения** в панели результатов узла Kaspersky Industrial CyberSecurity for Nodes.

- **Справка**. Перейти к просмотру справки Kaspersky Industrial CyberSecurity for Nodes. Выполнение этой операции также доступно в контекстных меню задач программы.

Панель инструментов и контекстное меню задач Kaspersky Industrial CyberSecurity for Nodes

Вы можете управлять задачами программы с помощью элементов контекстного меню каждой задачи в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes.

С помощью пунктов контекстного меню выбранной задачи вы можете выполнять следующие операции:

- **Возобновить/Приостановить**. Возобновить или приостановить выполнение задачи. Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты и задач проверки по требованию.
- **Создать задачу**. Создать новую пользовательскую задачу.
- **Удалить задачу**. Удалить пользовательскую задачу.
- **Экспортировать настройки** / **Импортировать настройки**. Экспортировать или импортировать настройки задачи.
- **Свойства**. Открыть окно свойств задачи.
- **Справка**. Открыть соответствующую страницу онлайн-справки.

Значок области уведомлений в панели задач

Сразу после установки Kaspersky Industrial CyberSecurity for Nodes значок приложения появляется в области уведомлений панели задач Microsoft Windows.

Если значок приложения в области уведомлений скрыт, администратор выключил отображение интерфейса приложения в политике.

Значок приложения выполняет следующие функции:

- служит индикатором работы приложения;
- обеспечивает доступ к контекстному меню значка приложения и главному окну приложения.

Для отображения информации о работе приложения предназначены следующие статусы значка приложения:

- Значок означает, что работа критически важных компонентов защиты приложения включена. Kaspersky Industrial CyberSecurity for Nodes покажет предупреждение , если от пользователя требуется выполнить действие, например, перезагрузить компьютер после обновления приложения.
- Значок означает, что работа критически важных компонентов защиты приложения выключена или нарушена. Работа компонентов защиты может быть нарушена, например, если срок действия лицензии истек или произошел сбой в работе приложения. Kaspersky Industrial CyberSecurity for Nodes покажет предупреждение с описанием проблемы в защите компьютера.

Вы можете открыть контекстное меню значка области уведомлений нажатием на правую кнопку мыши.

Контекстное меню включает несколько команд, предназначенных для отображения окон приложения (см. таблицу ниже).

Команды контекстного меню, отображаемые с помощью значка области уведомлений

Команда	Описание
Открыть Консоль приложения	Открывает Консоль Kaspersky Industrial CyberSecurity for Nodes (если она установлена).
Открыть диагностическое окно	Открывает Диагностическое окно программы.
О приложении	Открывает окно **О приложении** с информацией о Kaspersky Industrial CyberSecurity for Nodes. Для зарегистрированных пользователей Kaspersky Industrial CyberSecurity for Nodes окно **О приложении** содержит информацию об установленных срочных обновлениях.
Скрыть	Скрывает значок области уведомлений в панели задач.

Скрытый значок области уведомлений можно отобразить в любое время.

Чтобы снова отобразить значок области уведомлений,

в Microsoft Windows в меню **Пуск** выберите **Все программы** > **Kaspersky Industrial CyberSecurity for Nodes**. Значок появится в области уведомлений панели задач Microsoft Windows.

Названия параметров могут отличаться в зависимости от версии установленной операционной системы.

Настройка общих параметров в Консоли приложения

Общие параметры и параметры диагностики сбоев Kaspersky Industrial CyberSecurity for Nodes определяют общие условия работы приложения. Эти параметры позволяют контролировать количество рабочих процессов, используемых Kaspersky Industrial CyberSecurity for Nodes, включать восстановление задач Kaspersky Industrial CyberSecurity for Nodes после их аварийного завершения, вести журнал, включать создание файлов дампов для процессов Kaspersky Industrial CyberSecurity for Nodes при их аварийном завершении и настраивать другие общие параметры.

Настройка параметров приложения недоступна из Консоли Kaspersky Industrial CyberSecurity for Nodes, если изменение данных параметров запрещено активной политикой Kaspersky Security Center.

Чтобы настроить общие параметры работы Kaspersky Industrial CyberSecurity for Nodes:

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:

   - В панели результатов узла перейдите по ссылке **Свойства приложения**.
   - В контекстном меню узла выберите пункт **Свойства приложения**.

   Откроется окно **Свойства приложения**.

2. На вкладке **Интерфейс** укажите, какие предупреждения вы хотите видеть на значке Kaspersky Industrial CyberSecurity for Nodes в области уведомлений.

3. На вкладке **Настройки безопасности** настройте следующие параметры:

   - В блоке **Общие** настройте функцию **Запускать приложение при включении компьютера (рекомендуется)**.
   - В блоке **Самозащита** настройте защиту процессов приложения и защиту сервисов операционной системы.
   - В блоке **Действия при переходе на источник бесперебойного питания** задайте ограничение нагрузки на защищаемое устройство со стороны Kaspersky Industrial CyberSecurity for Nodes при переходе на источник бесперебойного питания:
     - **Не запускать задачи проверки по расписанию**.
     - **Остановить выполняемые задачи проверки**.
   - В блоке **Настройки совместимости** настройте параметр **Совместимость с приложениями для удаленного администрирования**.
   - В блоке **Настройки проверки** настройте ограничение потребления ресурсов процессора для задач проверки и включите возможность уступать ресурсы другим приложениям.

4. На вкладке **Настройки сети** настройте следующие параметры:

   - В блоке **Прокси-сервер** укажите настройки прокси-сервера: тип аутентификации и данные, необходимые для аутентификации на прокси-сервере.
   - В блоке **Контролируемые порты** укажите вариант контроля сетевых портов:
     - **Контролировать все сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты контролируют потоки данных, передаваемые через любые открытые сетевые порты компьютера.
     - **Контролировать только выбранные сетевые порты**. Режим контроля сетевых портов, при котором компоненты защиты контролируют выбранные сетевые порты компьютера и сетевую активность выбранных приложений. Список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика, настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского". При необходимости вы можете редактировать список сетевых портов.
   - В блоке **Порт для удаленного подключения**, если необходимо, измените порты для подключения Консоли приложения к компьютеру с установленным приложением.

     Номер порта по умолчанию для подключения с учетными данными Windows – 13032, для подключения с учетными данными вручную созданных пользователей – 13031. Диапазон возможных номеров портов: 1 – 65535.

     > До перезапуска приложения используются прежние сохраненные значения портов.

5. На вкладке **Диагностика сбоев** нажмите на кнопку **Настройка** и настройте трассировку работы приложения и запись дампов памяти.

6. Нажмите на кнопку **OK**.

Параметры работы Kaspersky Industrial CyberSecurity for Nodes будут сохранены.

Управление задачами Kaspersky Industrial CyberSecurity for Nodes

В этом разделе приведена информация о создании, настройке, запуске и остановке задач Kaspersky Industrial CyberSecurity for Nodes.

Категории задач Kaspersky Industrial CyberSecurity for Nodes

Функции постоянной защиты компьютера, контроля компьютера, автоматического формирования правил, мониторинга целостности системы, проверки по требованию, защиты промышленной сети, работы с хранилищем и обновления Kaspersky Industrial CyberSecurity for Nodes реализованы в виде задач.

Вы можете управлять задачами с помощью контекстного меню задачи в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes и панели результатов. Вы можете просматривать информацию о состоянии задачи в панели результатов. Операции по управлению задачами регистрируются в журнале системного аудита.

Существует два типа задач Kaspersky Industrial CyberSecurity for Nodes: *локальные* и *групповые*.

Локальные задачи

Локальные задачи могут выполняться только на том защищаемом устройстве, для которого они созданы. В зависимости от способа запуска существуют следующие типы локальных задач:

- **Локальные системные задачи**. Эти задачи создаются автоматически при установке Kaspersky Industrial CyberSecurity for Nodes. Вы можете изменять параметры всех локальных системных задач, кроме задачи *Откат обновления*. Локальные системные задачи нельзя переименовывать или удалять. Вы можете запускать локальные системные и пользовательские задачи проверки по требованию одновременно.

- **Локальные пользовательские задачи**. В Консоли приложения вы можете создавать задачи проверки по требованию, обновления, мониторинга целостности системы на основе эталона. В Kaspersky Security Center можно создавать задачи проверки по требованию, обновления, и т. д. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

Групповые задачи

Групповыми задачами и задачами для наборов защищаемых устройств можно управлять из Kaspersky Security Center. Все групповые задачи являются пользовательскими. Групповые задачи также отображаются в Консоли приложения. В Консоли приложения можно только просматривать состояние групповых задач. С помощью Консоли приложения нельзя управлять или настраивать групповые задачи.

Запуск, приостановка, возобновление, остановка задач вручную

Вы можете запустить, приостановить, возобновить или остановить задачи вручную. Данные функции доступны не для всех задач Kaspersky Industrial CyberSecurity for Nodes.

Чтобы запустить, приостановить, возобновить или остановить задачу, выполните следующие действия:

1. В дереве Консоли приложения откройте контекстное меню задачи.
2. Выберите одну из следующих команд: **Запуск** или **Приостановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита.

Настройка расписания задач

В Консоли Kaspersky Industrial CyberSecurity for Nodes вы можете настроить расписание запуска локальных системных и пользовательских задач. Настроить расписание запуска групповых задач нельзя.

Чтобы настроить расписание запуска задачи, выполните следующие действия:

1. Выберите задачу в дереве Консоли, для которой требуется настроить расписание.
2. В панели результатов нажмите на ссылку **Свойства**.
3. В открывшемся окне в блоке **Режим запуска** выполните одно из следующих действий:
   - Установите флажок **Вручную**, чтобы выполнять запуск задачи вручную в удобное для вас время.
   - Установите флажок **По расписанию**, чтобы включить запуск задачи по расписанию.
4. Если выбран вариант **По расписанию**, настройте параметры расписания запуска задачи (см. таблицу ниже).
5. При необходимости установите флажок **Запускать задачу с правами пользователя** и укажите данные учетной записи, с правами которой будет выполняться запуск задачи.
6. Нажмите на кнопку **OK**.

Параметры расписания задачи будут сохранены.

Параметр	Описание
Режим запуска	Выберите режим запуска задачи: • **Минуты**. Задача будет запускаться с периодичностью в заданное количество минут. Укажите время запуска задачи и период в минутах. • **Часы**. Задача будет запускаться с периодичностью в заданное количество часов. Укажите время запуска задачи и период в часах. • **Дни**. Задача будет запускаться с периодичностью в заданное количество дней. Укажите время запуска задачи и период в днях. • **Недели**. Задача будет запускаться в указанные дни недели с периодичностью в заданное количество недель. Укажите период запуска, выберите с помощью флажков дни недели, в которые будет выполняться запуск, и укажите время запуска задачи. • **Каждый месяц**. Задача будет запускаться в определенный день месяца. Укажите число и время запуска. • **В указанное время**. Задача будет запускаться однократно в указанный день и время. • **После каждого обновления**. Задача будет запускаться после каждой загрузки обновлений в хранилище. • **После запуска приложения**. Задача будет запускаться при каждом запуске Kaspersky Industrial CyberSecurity for Nodes.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.
Использовать автоматическое определение случайного интервала между запусками задачи	Если флажок установлен, задача запускается на компьютерах не точно по расписанию, а случайным образом в течение определенного интервала времени, то есть происходит распределенный запуск задачи. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества компьютеров, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако, когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Использовать случайную задержку запуска задачи в интервале (мин)	Если флажок установлен, задача запускается на компьютерах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Приостановить задачу	Вы можете задавать временной интервал, в течение которого выполнение ранее запущенной по расписанию задачи будет приостановлено. По окончании заданного периода времени выполнение задачи будет возобновлено. Это может понадобиться, например, для снижения влияния Kaspersky Industrial CyberSecurity for Nodes на производительность компьютера в период наиболее активного его использования. Данная функция доступна только для задач проверки по требованию.
Выключить расписание с	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes прекратит выполнение задачи по расписанию начиная с указанной даты. Для задачи будет установлен режим запуска **Вручную**. Данная функция доступна только для задач проверки по требованию.

Использование учетных записей для запуска задач

Вы можете запускать задачи, используя системную учетную запись пользователя или указать другую учетную запись.

Об использовании учетных записей для запуска задач

Вы можете указать учетную запись для запуска следующих задач Kaspersky Industrial CyberSecurity for Nodes:

- *Формирование правил контроля запуска программ*;
- *Формирование правил контроля устройств*;
- *Анализ журналов*;
- *Проверка целостности приложения*;
- *Обновление*.

По умолчанию указанные задачи выполняются с правами системной учетной записи.

Рекомендуется указать другую учетную запись с достаточными правами доступа в следующих случаях:

- Для задачи *Обновление*:
  - если в качестве источника обновления указана папка общего доступа на другом устройстве в сети;
  - если для доступа к источнику обновлений используется прокси-сервер с NTLM- или Kerberos-аутентификацией.
- Для задачи *Формирование правил контроля запуска программ*: если сформированные правила экспортируются в конфигурационный файл, недоступный для системной учетной записи (например, находящийся в папке общего доступа на защищаемом устройстве).

Вы можете запускать перечисленные задачи с правами системной учетной записи. В ходе выполнения этих задач Kaspersky Industrial CyberSecurity for Nodes обращается к папкам общего доступа на другом устройстве в сети, если это устройство зарегистрировано в то же домене, что и защищаемое устройство. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Industrial CyberSecurity for Nodes обращается к устройству с правами учетной записи **<имя домена \ имя устройства>**.

Указание учетной записи для запуска задачи

Возможность указать учетную запись в Консоли приложения доступна не для всех задач.

Чтобы указать учетную запись для запуска задачи, выполните следующие действия:

1. В дереве Консоли приложения выберите задачу, которую вы хотите запустить с правами определенной учетной записи.
2. В панели результатов нажмите на ссылку **Свойства**.

   Откроется окно **Свойства: <Название задачи>**.

3. Перейдите на вкладку **Режим запуска** и выполните следующие действия:

   a. Установите флажок **Запускать задачу с правами пользователя**.

   b. Укажите имя и пароль пользователя, учетную запись которого вы хотите использовать.

   Выбранный вами пользователь должен быть зарегистрирован на защищаемом устройстве или в одном домене с ним.

4. Нажмите на кнопку **OK**.

Импорт и экспорт настроек

В этом разделе приведена информация об экспорте настроек Kaspersky Industrial CyberSecurity for Nodes. Также описан экспорт настроек определенных компонентов приложения в конфигурационный файл в формате XML и импорт этих настроек из конфигурационного файла в приложение.

Об импорте и экспорте настроек

Вы можете экспортировать настройки Kaspersky Industrial CyberSecurity for Nodes в конфигурационный файл в формате XML и импортировать настройки в Kaspersky Industrial CyberSecurity for Nodes из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все настройки приложения, так и настройки его отдельных компонентов.

Когда вы экспортируете все настройки Kaspersky Industrial CyberSecurity for Nodes, в файл сохраняются общие настройки приложения и настройки следующих компонентов и функций Kaspersky Industrial CyberSecurity for Nodes:

- Постоянная защита файлов;
- Защита от эксплойтов;
- Защита от сетевых угроз;
- Защита от шифрования;
- Откат вредоносных действий;
- AMSI-защита;
- Контроль запуска программ;
- Контроль устройств;
- Сетевой экран;
- Формирование правил контроля запуска программ;
- Формирование правил контроля устройств;

- Анализ журналов;
- Контроль целостности системы;
- Проверка целостности проектов ПЛК;
- Получение данных о проектах ПЛК;
- Проверка при старте операционной системы;
- Проверка важных областей;
- Проверка целостности приложения;
- Проверка съемных дисков;
- Полная проверка;
- Обновление баз и модулей приложения;
- Откат последнего обновления;
- Обновление.

Также вы можете сохранять в файле общие настройки Kaspersky Industrial CyberSecurity for Nodes и права учетных записей пользователей.

Если в момент экспорта настроек действует политика Kaspersky Security Center, приложение экспортирует значения, применяемые политикой.

Вы не можете экспортировать настройки групповых задач.

Kaspersky Industrial CyberSecurity for Nodes экспортирует все пароли, используемые в приложении, например, настройки учетных записей для запуска задач или соединения с прокси-сервером. Экспортированные пароли хранятся в конфигурационном файле в зашифрованном виде. Пароли можно импортировать только с помощью приложения Kaspersky Industrial CyberSecurity for Nodes, установленного на этом же защищаемом устройстве, если оно не было переустановлено или обновлено.

Нельзя импортировать ранее сохраненные пароли с помощью приложения Kaspersky Industrial CyberSecurity for Nodes, установленной на другом защищаемом устройстве. После импорта настроек на другом защищаемом устройстве нужно ввести все пароли вручную.

Если в момент экспорта настроек включена функция **Запрашивать пароль для подтверждения критических действий**, установленный на устройстве пароль будет экспортирован и в дальнейшем автоматически применен на другом устройстве при импорте настроек.

Можно импортировать настройки из конфигурационного файла, содержащего настройки только отдельных компонентов Kaspersky Industrial CyberSecurity for Nodes (например, созданного в приложении Kaspersky Industrial CyberSecurity for Nodes, установленном с неполным набором компонентов). После импорта настроек в Kaspersky Industrial CyberSecurity for Nodes изменяются только те настройки, которые содержались в конфигурационном файле. Остальные настройки не изменяются.

Заблокированные настройки активной политики Kaspersky Security Center при импорте настроек не изменяются.

Экспорт настроек

Чтобы экспортировать настройки в конфигурационный файл, выполните следующие действия:

1. Для экспорта всех настроек Kaspersky Industrial CyberSecurity for Nodes, в контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes** выберите пункт **Экспортировать настройки**.

   Для экспорта настроек отдельного функционального компонента, нажмите **Экспортировать настройки** в панели результатов.

   > Экспортировать настройки Kaspersky Security Network невозможно. Kaspersky Security Network нужно настраивать вручную.

2. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список настроек, а также выберите папку, в которой вы хотите сохранить этот файл.

   При указании пути можно использовать системные переменные окружения; пользовательские переменные окружения использовать нельзя.

   > Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует параметры, используемые в политике.

3. Сохраните файл.

4. В окне **Экспорт успешно завершен** нажмите на кнопку **OK**.

   Kaspersky Industrial CyberSecurity for Nodes экспортирует список настроек в XML-файл.

Чтобы экспортировать список Доверенных приложений, выполните следующие действия:

1. В дереве Консоли приложения откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.

2. Выберите пункт **Настроить доверенную зону**.

3. Откроется окно **Настроить доверенную зону**.

4. Перейдите в раздел **Доверенные приложения** и нажмите кнопку **Настройка**.

   Откроется окно со списком доверенных приложений.

5. Выберите доверенные приложения, которые вы хотите экспортировать.

   Если вы не выбрали ни одного доверенного приложения, Kaspersky Industrial CyberSecurity for Nodes экспортирует все доверенные приложения.

6. Нажмите на стрелку и выберите из выпадающего списка вариант **Экспортировать**.

7. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список доверенных приложений, а также выберите папку, в которой вы хотите сохранить этот файл.

8. Сохраните файл.

   Kaspersky Industrial CyberSecurity for Nodes экспортирует список доверенных приложений в XML-файл.

Также вы можете экспортировать настройки Kaspersky Industrial CyberSecurity for Nodes из командной строки.

Импорт настроек

Чтобы импортировать настройки из сохраненного конфигурационного файла, выполните следующие действия:

1. Для импорта всех настроек Kaspersky Industrial CyberSecurity for Nodes, в контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes** выберите пункт **Импортировать настройки**.

   Для импорта настроек отдельного функционального компонента, нажмите **Импортировать настройки** в панели результатов.

   После импорта общих параметров или параметров функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes на защищаемое устройство, восстановить их прежние значения невозможно.

   Импортировать настройки Kaspersky Security Network невозможно. Kaspersky Security Network нужно настраивать вручную.

2. В открывшемся окне выберите конфигурационный файл в формате XML, из которого вы хотите импортировать настройки, и нажмите **Открыть**.

3. В окне **Импорт успешно завершен** нажмите на кнопку **ОК**.

4. В панели инструментов Консоли приложения нажмите на кнопку **Обновить**.

Импортированные настройки отобразятся в окне Консоли приложения.

Kaspersky Industrial CyberSecurity for Nodes не импортирует пароли (учетные данные для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом защищаемом устройстве или на этом же защищаемом устройстве, после того как на нем было переустановлено или обновлено приложение Kaspersky Industrial CyberSecurity for Nodes. После завершения импорта пароли необходимо ввести вручную.

Чтобы импортировать список Доверенных приложений, выполните следующие действия:

1. В дереве Консоли приложения откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.

2. Выберите пункт **Настроить доверенную зону**.

3. Откроется окно **Настроить доверенную зону**.

4. Перейдите в раздел **Доверенные приложения** и нажмите кнопку **Настройка**.

5. Нажмите на стрелку и выберите из выпадающего списка вариант **Импортировать**.

6. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных приложений.

7. Откройте файл.

   Если на компьютере уже есть список доверенных приложений, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

8. Список появится на закладке **Доверенные приложения**. Нажмите **ОК**.

Просмотр состояния защиты и информации о Kaspersky Industrial CyberSecurity for Nodes

Чтобы просмотреть информацию о состоянии защиты устройства в Kaspersky Industrial CyberSecurity for Nodes,

выберите узел **Kaspersky Industrial CyberSecurity for Nodes** в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes.

По умолчанию информация в панели результатов Консоли Kaspersky Industrial CyberSecurity for Nodes обновляется автоматически:

- каждые 10 секунд при локальном подключении;
- каждые 15 секунд при удаленном подключении.

Вы можете обновлять информацию вручную.

*Чтобы вручную обновить информацию в узле **Kaspersky Industrial CyberSecurity for Nodes**,*

в контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes** выберите пункт **Обновить**.

В панели результатов Консоли Kaspersky Industrial CyberSecurity for Nodes отображается следующая информация о приложении:

- статус использования Kaspersky Security Network;
- состояние защиты устройства;
- данные об обновлении баз и модулей приложения;
- актуальные данные диагностики;
- данные о задачах контроля защищаемого устройства;
- данные о лицензии;
- статус защиты промышленной сети;
- статус интеграции с Kaspersky Security Center: данные сервера с установленной программой Kaspersky Security Center, к которому подключена программа; данные о контроле задач программы активной политикой.

Для отображения состояния защиты используется цветовая индикация:

- *Зеленый цвет*. Задача выполняется в соответствии с настроенными параметрами. Защита обеспечивается.
- *Желтый цвет*. Задача не запущена, приостановлена или остановлена. Возможно возникновение угрозы безопасности. Рекомендуется настроить и запустить задачу.
- *Красный цвет*. Задача завершена с ошибкой или при работе задачи была обнаружена угроза безопасности. Рекомендуется запустить задачу или принять меры по устранению обнаруженной угрозы безопасности.

Часть информации в блоке (например, названия задач или количество обнаруженных угроз) являются ссылками, по которым вы можете перейти в узел соответствующей задачи или открыть журнал ее выполнения.

В разделе **Использование Kaspersky Security Network** отображается текущий статус задачи, например, *Выполняется*, *Остановлено* или *Не выполнялось*. Индикатор может принимать следующие значения:

- Зеленый цвет панели означает, что задача **Использование KSN** выполняется и запросы статусов отправляются в KSN.
- Желтый цвет панели означает, что принято одно из Положений, но задача не выполняется, или задача выполняется, но файловые запросы не отправляются в KSN.
- Красный цвет панели означает, что задача завершена с ошибкой.

Защита компьютера

В разделе **Защита компьютера** (см. таблицу ниже) отображается информация о текущем состоянии защиты устройства.

Информация о состоянии защиты устройства

Раздел Защита	Информация
Индикатор состояния защиты устройства	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый цвет панели отображается по умолчанию и означает, что компонент Постоянная защита файлов установлен и задача выполняется. • Желтый цвет панели означает, что компонент Постоянная защита файлов не установлен и задача *Проверка важных областей* давно не выполнялась. • Красный цвет панели – задачи постоянной защиты файлов не выполняются.
Постоянная защита файлов	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*.
Проверка важных областей	**Дата последней проверки** – дата и время последней проверки важных областей на наличие вирусов и других угроз компьютерной безопасности. *Не выполнялось* – событие, которое возникает, если задача *Проверка важных областей* выполнялась 30 и более дней назад (по умолчанию). Вы можете изменять порог формирования этого события.
Защита от сетевых угроз	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*.
Защита от эксплойтов	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*. **Режим работы** – один из двух доступных режимов работы компонента Защита от эксплойтов: **Блокировать** или **Информировать**.
Защита от шифрования	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*. **Режим работы** – один из трех доступных режимов работы компонента Защита от шифрования: **Удалять**, **Блокировать** или **Информировать**.

Обновление

В разделе **Обновление** (см. таблицу ниже) отображается информация об актуальности баз и модулей приложения.

Информация о состоянии баз и модулей Kaspersky Industrial CyberSecurity for Nodes

Раздел Обновление	Информация
Индикатор состояния баз и модулей приложения	Цвет панели с названием раздела является индикатором состояния баз и модулей приложения. Индикатор может принимать следующие значения: • Зеленый цвет панели отображается по умолчанию и означает, что базы приложения актуальны и последняя задача обновления баз и модулей приложения завершена успешно. • Желтый цвет панели – означает, что базы устарели или последняя задача обновления баз приложения завершена с ошибкой. • Красный цвет панели показывает, что возникло событие *Базы сильно устарели* или *Базы актуальны*.
Актуальность баз приложения	Параметр может принимать следующие значения: • **Базы актуальны** – базы приложения были обновлены не более чем 7 дней назад (по умолчанию). • **Базы устарели** – базы приложения были обновлены от 7 до 14 дней назад (по умолчанию). • **Базы сильно устарели** – базы приложения обновлены более чем 14 дней назад (по умолчанию). Вы можете изменять пороги формирования событий *Базы устарели* и *Базы сильно устарели*.
Дата выпуска баз приложения	Дата и время выпуска последнего обновления баз приложения. Дата и время указаны в UTC-формате.
Статус последней запущенной задачи обновления баз приложения	Дата и время последнего обновления базы приложения. Дата и время указаны по местному времени защищаемого устройства. Значение в поле окрашивается в красный цвет, если возникло событие *Завершено с ошибкой*.

Контроль

В разделе **Контроль** (см. таблицу ниже) отображается информация о задачах Контроль запуска программ, Контроль устройств и Сетевой экран.

Информация о состоянии контроля защищаемого устройства

Раздел Контроль	Информация
Индикатор состояния контроля защищаемого устройства	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый цвет панели отображается по умолчанию и означает, что компонент Контроль запуска программ установлен и задача выполняется в активном режиме; компонент Защита от эксплойтов установлен и активен. • Желтый цвет панели отображается при наличии одного или нескольких из следующих условий: Защита от эксплойтов не запущена; Задача Контроль запуска программ запущена в режиме Информировать; Защита от эксплойтов работает в активном режиме, а задача Контроль запуска программ не выполняется или завершена с ошибкой. • Красный цвет панели отображается, если задача Контроль запуска программ не выполняется или завершена с ошибкой, и Защита от эксплойтов не работает или работает в режиме **Информировать**.
Контроль запуска программ	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*. **Режим работы** – один из доступных режимов работы задачи Контроль запуска программ: **Информировать** или **Блокировать**.
Контроль устройств	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*. **Режим работы** – один из двух доступных режимов работы задачи Контроль устройств: **По правилам** или **Информировать**.
Сетевой экран	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*.

Диагностика

В разделе **Диагностика** (см. таблицу ниже) отображается информация о задачах Контроль целостности системы и Анализ журналов.

Информация о состоянии диагностики системы

Раздел Диагностика	Информация
Индикатор статуса диагностики	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что один или оба компонента диагностики системы установлены и задача выполняется. • Желтый – оба компонента установлены, но одна из задач диагностики системы не выполняется; возникает событие *Не выполняется*. • Красный – одна из задач завершена с ошибкой.
Контроль целостности системы	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*.
Анализ журналов	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*.

Закладка **Защита промышленной сети**

В разделе **Получение данных о проектах ПЛК** отображается информация о списке ПЛК, включенных в область защиты.

Информация о получении данных о ПЛК

Раздел Получение данных о проектах ПЛК	Информация
Индикатор статуса области защиты ПЛК	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый цвет означает, что задача была успешно завершена минимум один раз. • Желтый цвет означает, что проверка ни разу не выполнялась. • Красный цвет означает, что задача завершена с ошибкой.
Получение данных о проектах ПЛК	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*.

В разделе **Проверка целостности проектов ПЛК** отображается информация о количестве защищаемых ПЛК и событиях нарушения целостности.

Информация о проверке целостности проектов ПЛК

Раздел Проверка целостности проектов ПЛК	Информация
Индикатор статуса целостности ПЛК	Цвет панели с названием раздела является индикатором состояния задач, выполняемых в разделе. Индикатор может принимать следующие значения: • Зеленый цвет означает, что задача была успешно завершена минимум один раз. • Желтый цвет означает, что проверка целостности ни разу не выполнялась. • Красный цвет означает, что задача завершена с ошибкой.
Проверка целостности проектов ПЛК	**Статус** – текущее состояние компонента, например, *Выполняется* или *Отключено*.

Информация о лицензии Kaspersky Industrial CyberSecurity for Nodes отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes**.

Вы можете настроить свойства Kaspersky Industrial CyberSecurity for Nodes, перейдя по ссылке Свойства приложения.

Вы можете подключиться к другому защищаемому устройству, перейдя по ссылке Подключиться к удаленному компьютеру.

Настройка параметров резервного хранилища в Консоли приложения

Чтобы настроить общие параметры резервного хранилища, выполните следующие действия:

1. В дереве Консоли приложения откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes** и выберите пункт **Хранилища**.

2. Настройте параметры, которые приведены в таблице ниже.

Настройки хранилища

Параметр	Описание
На вкладке **Отчеты** укажите настройки отчетов:	
Хранить отчеты не более	Если флажок установлен, то максимальный срок хранения отчетов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения отчетов составляет 30 дней. По истечении этого времени Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые записи из файла отчета.
Ограничить размер файла отчетов до	Если флажок установлен, то максимальный размер файла отчетов ограничен заданным значением. По умолчанию максимальный размер файла составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые записи из файла отчетов таким образом, чтобы размер файла отчетов не превышал максимального значения.
На вкладке **Резервное хранилище** укажите настройки резервного хранилища:	
Хранить объекты не более	Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения файлов составляет 30 дней. По истечении максимального срока хранения Kaspersky Industrial CyberSecurity for Nodes удаляет наиболее старые файлы из резервного хранилища.
Ограничить размер хранилища до	Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 400 МБ. После достижения максимального размера резервного хранилища приложение Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.
Порог доступного пространства	Флажок включает или выключает отслеживание минимального объема свободного места в резервном хранилище (по умолчанию 100 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен порог свободного места в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отслеживает размер свободного места в резервном хранилище. Флажок **Порог доступного пространства** активен, если установлен флажок **Ограничить размер хранилища до**.

Работа с Веб-плагином из Web Console

Этот раздел содержит информацию о Плагине управления Kaspersky Industrial CyberSecurity for Nodes для Web Console и об управлении приложением, установленным на защищаемом устройстве или группе защищаемых устройств.

Управление Kaspersky Industrial CyberSecurity for Nodes из Web Console

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленным приложением Kaspersky Industrial CyberSecurity for Nodes, объединенными в группу администрирования, с помощью Веб-плагина Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Security Center Web Console также позволяет отдельно настраивать параметры каждого защищаемого устройства, входящего в группу администрирования.

Группа администрирования формируется вручную на стороне Kaspersky Security Center Web Console. Группа администрирования включает устройства с установленной программой Kaspersky Industrial CyberSecurity for Nodes, для которых требуется настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в справке Kaspersky Security Center.

Параметры приложения для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Industrial CyberSecurity for Nodes на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes из Web Console следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли приложения или удаленно в окне свойств устройства в Web Console. С помощью политик можно настроить общие параметры приложения, параметры задач постоянной защиты компьютера, задач контроля активности на устройствах, задач защиты сетевых хранилищ и параметры запуска локальных системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств. С помощью групповых задач вы можете активировать приложение, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи Формирование правил контроля запуска программ.

- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.

- **С помощью окна свойств отдельного устройства**. В окне свойств устройства можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры приложения, так и параметры всех задач Kaspersky Industrial CyberSecurity for Nodes, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center Web Console позволяет настроить параметры приложения, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы защищаемых устройств, так и для отдельного защищаемого устройства.

Ограничения Веб-плагина

Веб-плагин Kaspersky Industrial CyberSecurity for Nodes имеет следующие ограничения по сравнению с Плагином управления Kaspersky Industrial CyberSecurity for Nodes:

- Для компонента Контроль запуска программ нельзя сформировать правила на основе цифрового сертификата или событий Kaspersky Security Center.
- Для компонента Контроль устройств нельзя сформировать правила на основе подключенных устройств или данных системы.

Управление параметрами приложения

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Industrial CyberSecurity for Nodes в Web Console.

Настройка общих параметров приложения с помощью Веб-плагина

С помощью Веб-плагина можно настроить общие параметры Kaspersky Industrial CyberSecurity for Nodes для группы защищаемых устройств или для отдельного защищаемого устройства.

Настройка параметров интерфейса и проверки с помощью Веб-плагина

Чтобы настроить параметры интерфейса приложения, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите вкладку **Параметры приложения**.
4. Выберите раздел **Настройки приложения**.
5. Нажмите на кнопку **Настроить** в подразделе **Настройки интерфейса**.
6. Настройте параметры, которые приведены в следующей таблице.

Настройки взаимодействия с пользователем и настройки проверки

Параметр	Описание
Взаимодействие с пользователем	**Не отображать пользовательский интерфейс**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Industrial CyberSecurity for Nodes. Также недоступны значок в области уведомлений Windows и уведомления. **Отображать пользовательский интерфейс.** На клиентском компьютере доступен значок в области уведомлений Windows. В контекстном меню значка пользователь может выполнять операции с Kaspersky Industrial CyberSecurity for Nodes. Также Kaspersky Industrial CyberSecurity for Nodes показывает уведомления над значком приложения. Из контекстного меню значка в области уведомлений Windows открывается Диагностическое окно. А по ссылке в Диагностическом окне открывается Консоль программы.
Отображать состояние приложения в области уведомлений	Установите флажки напротив тех категорий событий, уведомления о которых вы хотите видеть в области уведомлений Microsoft Windows.

Настройка параметров безопасности и надежности с помощью Веб-плагина

Чтобы вручную настроить параметры безопасности, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите вкладку **Параметры приложения**.
4. Выберите раздел **Настройки приложения**.
5. Нажмите на кнопку **Настроить** в подразделе **Безопасность и надежность**.
6. Настройте параметры, которые приведены в следующей таблице.

Настройки безопасности и надежности

Параметр	Описание
Запускать приложение при включении компьютера (рекомендуется)	Если флажок установлен, то приложение Kaspersky Industrial CyberSecurity for Nodes запускается после загрузки операционной системы и защищает компьютер пользователя в течение всего сеанса работы. Если флажок не установлен, то приложение Kaspersky Industrial CyberSecurity for Nodes не запускается после загрузки операционной системы до того момента, как пользователь запустит приложение вручную. Защита компьютера выключена и данные пользователя могут находиться под угрозой.
Защищать процессы приложения от внешних угроз	Если флажок установлен, то Kaspersky Industrial CyberSecurity for Nodes предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти и записей в системном реестре.
Защищать сервисы операционной системы	Если защита сервисов операционной системы включена, сторонние приложения не могут совершать действия в отношении процессов операционной системы. Если защита сервисов операционной системы выключена, сторонние приложения могут совершать действия в отношении процессов операционной системы.

Параметр	Описание
Откладывать задачи по расписанию при работе от аккумулятора	Если флажок установлен, то режим экономии питания аккумулятора включен. Приложение Kaspersky Industrial CyberSecurity for Nodes откладывает выполнение задач, для которых задан запуск по расписанию. По мере необходимости вы можете самостоятельно запускать задачи проверки и обновления. Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию: • *Обновление баз и модулей приложения*; • *Полная проверка*; • *Проверка важных областей*; • *Выборочная проверка*; • *Проверка целостности приложения*; • *Поиск IOC*.
Статус компьютера при применении настроек	Параметры отображения статусов клиентских компьютеров с установленным приложением Kaspersky Industrial CyberSecurity for Nodes в Web Console при появлении ошибок применения политики или выполнения задачи. Доступны статусы *OK*, *Предупреждение* и *Критический*.
Совместимость с приложениями для удаленного администрирования	При появлении сбоев в работе Kaspersky Industrial CyberSecurity for Nodes с инструментами для удаленного администрирования (англ. Remote Administration Tool, RAT) вы можете включить режим совместимости. Сбои могут быть связаны с проблемами совместимости RAT и функции безопасного рабочего стола (англ. Secure Desktop) приложения. Эта функция предназначена для подтверждения действий, которые могут снизить безопасность компьютера. Функция позволяет приложению показывать диалоговое окно подтверждения, изолированное от других процессов. Функция обеспечивает безопасность запроса за счет повышенных прав. Таким образом, подтвердить действие может только пользователь, а не вредоносное ПО. Если флажок установлен, режим совместимости с RAT включен. Приложение показывает диалоговое окно подтверждения без этой функции. Это может снизить уровень безопасности компьютера. Рекомендуется не включать режим совместимости, если Kaspersky Industrial CyberSecurity for Nodes с RAT работает корректно. Если флажок снят, режим совместимости с RAT выключен. По умолчанию флажок снят. Пример. При работе с браузером в режиме RemoteApp Kaspersky Industrial CyberSecurity for Nodes может не показывать диалоговое окно подтверждения при переходе на сайт с недоверенным сертификатом, так как RemoteApp не поддерживает функцию безопасного рабочего стола приложения. Это может привести к тому, что браузер перестает отвечать. Для корректной работы браузера в режиме RemoteApp нужно включить режим совместимости. Вы также можете попробовать включить режим совместимости при появлении сбоев в работе функции безопасного рабочего стола с другим сторонним ПО.
Ограничить потребление ресурсов процессора для задач проверки	Kaspersky Industrial CyberSecurity for Nodes ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в поле **Максимальное значение**. При этом приложение может потреблять существенно больше процессорного времени за счет работы других компонентов. Включение этой функции может негативно сказаться на производительности Kaspersky Industrial CyberSecurity for Nodes. По умолчанию эта функция выключена.
Уступать ресурсы другим приложениям	Потребление ресурсов компьютера Kaspersky Industrial CyberSecurity for Nodes при проверке компьютера может увеличить нагрузку на центральный процессор и дисковые подсистемы. Это может замедлить работу других приложений. Для оптимизации производительности в Kaspersky Industrial CyberSecurity for Nodes предусмотрен режим передачи ресурсов другим приложениям. В этом режиме операционная система может понизить приоритет потоков задач проверки Kaspersky Industrial CyberSecurity for Nodes при высокой нагрузке на центральный процессор. Это позволит перераспределить ресурсы операционной системы для других приложений. То есть задачи проверки получат меньше процессорного времени. В результате Kaspersky Industrial CyberSecurity for Nodes будет проверять компьютер дольше. По умолчанию режим передачи ресурсов другим приложениям включен.

Настройка параметров соединения с помощью Веб-плагина

Настроенные параметры соединения используются для подключения Kaspersky Industrial CyberSecurity for Nodes к серверам обновлений и активации, а также при интеграции программ со службами Kaspersky Security Network.

Чтобы настроить параметры соединения, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите вкладку **Параметры приложения**.
4. Выберите раздел **Настройки приложения**.
5. Нажмите на кнопку **Настроить** в подразделе **Настройки соединения**.
6. Настройте параметры, которые приведены в следующей таблице.

Настройки соединения

Параметр	Описание
Ограничивать трафик при лимитном подключении	Если флажок установлен, приложение ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным. Приложение Kaspersky Industrial CyberSecurity for Nodes определяет высокоскоростное мобильное подключение к интернету как лимитное, а подключение по Wi-Fi – как безлимитное. Учет стоимости подключения работает на компьютерах под управлением Windows 8 и выше.
Не использовать прокси-сервер	Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes не использует прокси-сервер.
Автоматически определять настройки прокси-сервера	Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует настройки прокси-сервера, заданные в параметрах операционной системы.
Использовать указанный прокси-сервер	Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes использует параметры прокси-сервера, указанные вручную. Введите IP-адрес или символьное имя прокси-сервера и номер порта.
Не использовать прокси-сервер для локальных адресов	Если функция включена, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленным приложением Kaspersky Industrial CyberSecurity for Nodes, происходит напрямую, прокси-сервер не используется. По умолчанию функция включена.

Параметр	Описание
Настройки аутентификации на прокси-сервере	Для аутентификации приложения на прокси-сервере для доступа в интернет нужно ввести учетные данные пользователя. Kaspersky Industrial CyberSecurity for Nodes поддерживает автоматическую аутентификацию на прокси-сервере. Если выполнить аутентификацию автоматически не удалось, приложение предлагает ввести учетные данные вручную. **Не использовать аутентификацию** **NTLM-аутентификация**. NTLM-аутентификация с помощью учетной записи текущего пользователя (значение по умолчанию). **NTLM-аутентификация с именем пользователя и паролем**. NTLM-аутентификация с помощью учетных данных, заданных вручную. **Имя пользователя и пароль**. Аутентификация с использованием учетных данных, заданных вручную. **Kerberos-аутентификация**. Kerberos-аутентификация с помощью учетной записи текущего пользователя. Для обеспечения корректной работы Kerberos-аутентификации при использовании CNAME-записей для адреса прокси-сервера вам необходимо зарегистрировать имя субъекта-службы (SPN) для каждой CNAME-записи. **Kerberos-аутентификация с именем пользователя и паролем**. Kerberos-аутентификация с использованием учетных данных, заданных вручную. Если выбрана Kerberos-аутентификация, Kaspersky Industrial CyberSecurity for Nodes может в зависимости от настроек прокси-сервера осуществлять аутентификацию как по протоколу Kerberos, так и по протоколу NTLM.
Контролировать все сетевые порты	Режим контроля сетевых портов, при котором компоненты защиты контролируют потоки данных, передаваемые через любые открытые сетевые порты компьютера.
Контролировать только выбранные сетевые порты	Режим контроля сетевых портов, при котором компоненты защиты контролируют выбранные сетевые порты компьютера и сетевую активность выбранных приложений. Список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика, настроен в соответствии с рекомендациями специалистов "Лаборатории Касперского".
Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения	Укажите, будет ли Kaspersky Security Center использоваться в качестве прокси-сервера для активации приложения.

Настройка запуска по расписанию локальных задач с помощью Веб-плагина

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления. Запуск осуществляется по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Industrial CyberSecurity for Nodes будет выполнять обновления баз и модулей приложения, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: *Проверка важных областей*, *Проверка при старте операционной системы*, *Проверка целостности приложения*, *Мониторинг целостности системы на основе эталона*.
- Задача *Обновление*.

Если защищаемое устройство исключено из группы администрирования, расписание локальных системных задач будет автоматически включено.

Чтобы разрешить или запретить в политике запуск по расписанию локальных системных задач Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите вкладку **Параметры приложения**.
4. Выберите раздел **Настройки приложения**.
5. Нажмите на кнопку **Настроить** в подразделе **Запуск локальных системных задач**.
6. Настройте параметры, которые приведены в следующей таблице.

Настройки запуска локальных задач

Параметр	Описание
Разрешить использование локальных задач	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Industrial CyberSecurity for Nodes. Пользователь, при отсутствии дополнительных ограничений политики, может настраивать и запускать задачи. При этом параметры расписания запуска задачи остаются недоступными для пользователя. Пользователь может запускать задачи только вручную. Если флажок снят, то использование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в локальном интерфейсе Kaspersky Industrial CyberSecurity for Nodes, а также при работе с командной строкой.
Разрешить управление расписанием	Флажок доступен, если установлен флажок **Разрешить использование локальных задач**. Если флажок установлен, в Консоли приложения в свойствах локальных задач становится доступной настройка режима запуска. По умолчанию флажок снят.
Разрешить отображение групповых задач	Если флажок установлен, то групповые задачи отображаются в локальном интерфейсе Kaspersky Industrial CyberSecurity for Nodes. Пользователь может просмотреть полный список задач в Консоли приложения. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes показывает пустой список задач.
Разрешить управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в Консоли приложения или в упрощенном интерфейсе приложения. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в Kaspersky Security Center.

Настройка параметров карантина и резервного хранилища с помощью Веб-плагина

Чтобы настроить общие параметры карантина и резервного хранилища в Kaspersky Security Center, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите вкладку **Параметры приложения**.
4. Выберите раздел **Дополнительные возможности**.
5. В подразделе **Хранилища** нажмите на кнопку **Настройка**.
6. Настройте параметры, которые приведены в следующей таблице.

Настройки хранилища

Параметр	Описание
На вкладке **Отчеты** укажите настройки отчетов:	
Хранить отчеты не более	Если флажок установлен, то максимальный срок хранения отчетов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения отчетов составляет 30 дней. По истечении этого времени Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые записи из файла отчета.
Ограничить размер файла отчетов до	Если флажок установлен, то максимальный размер файла отчетов ограничен заданным значением. По умолчанию максимальный размер файла составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые записи из файла отчетов таким образом, чтобы размер файла отчетов не превышал максимального значения.
На вкладке **Резервное хранилище** укажите настройки резервного хранилища:	
Хранить объекты не более	Если флажок установлен, то максимальный срок хранения файлов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения файлов составляет 30 дней. По истечении максимального срока хранения Kaspersky Industrial CyberSecurity for Nodes удаляет наиболее старые файлы из резервного хранилища.
Ограничить размер хранилища до	Если флажок установлен, то максимальный размер резервного хранилища ограничен заданным значением. По умолчанию максимальный размер составляет 400 МБ. После достижения максимального размера резервного хранилища приложение Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет наиболее старые файлы таким образом, чтобы размер резервного хранилища не превышал максимального значения.
Порог доступного пространства	Флажок включает или выключает отслеживание минимального объема свободного места в резервном хранилище (по умолчанию 100 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие Превышен порог свободного места в резервном хранилище и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа. Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отслеживает размер свободного места в резервном хранилище. Флажок **Порог доступного пространства** активен, если установлен флажок **Ограничить размер хранилища до**. По умолчанию флажок установлен.
На вкладке **Карантин** укажите настройки карантина:	
Ограничить размер карантина до	Если функция включена, Kaspersky Industrial CyberSecurity for Nodes отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 1024 МБ) Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен максимальный размер карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа. При этом приложение прекращает помещать новые объекты на карантин. Вам нужно вручную очистить карантин. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes не отслеживает суммарный размер объектов в карантине. По умолчанию функция выключена.

Параметр	Описание
Порог доступного пространства	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отслеживает минимальный объем свободного места в папке карантина (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен порог свободного места в карантине* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа. Флажок **Порог доступного пространства** активен, если установлен флажок **Ограничить размер карантина до**. По умолчанию функция включена.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Industrial CyberSecurity for Nodes на нескольких защищаемых устройствах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлено приложение Kaspersky Industrial CyberSecurity for Nodes.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Industrial CyberSecurity for Nodes на всех защищаемых устройствах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, имеет статус *Активная* в Web Console.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Industrial CyberSecurity for Nodes. Вы можете просмотреть эту информацию в Консоли приложения в узле **Журналы и уведомления**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых устройствах: *Запретить изменение параметров*. После применения политики Kaspersky Industrial CyberSecurity for Nodes использует на защищаемых устройствах параметры, для которых в свойствах политики вы установили значок . В этом случае выбранные параметры используются вместо параметров, действовавших до применения политики. Kaspersky Industrial CyberSecurity for Nodes не применяет параметры активной политики, для которых в свойствах политики установлен значок .

Если политика активна, то значения параметров, отмеченные в политике значком , отображаются в Консоли приложения, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком) доступны для редактирования в Консоли приложения.

Параметры, настроенные в активной политике и отмеченные значком , также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемое устройство с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры для любой задачи постоянной защиты компьютера или защиты сетевых хранилищ, которая выполняется в текущий момент, то параметры, задаваемые политикой, изменятся сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

Как создать политику с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на кнопку **Добавить**.
3. Откроется окно **Новая политика**.
4. В разделе **Выберите приложение** выберите Kaspersky Industrial CyberSecurity for Nodes.
5. Укажите в каких режимах используется Kaspersky Industrial CyberSecurity for Nodes на защищенных устройствах.
6. Если необходимо, укажите файлы или папки, а также имена объектов (согласно Вирусной энциклопедии), которые будут исключены из проверки всеми или некоторыми компонентами приложения.
7. На закладке **Общие** вы можете выполнить следующие действия:
   - Изменить имя политики.

     Имя политики не должно содержать следующие символы: `" * < : > ? \ | .`

   - Выбрать статус политики:
     - **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве активной политики.
     - **Неактивна**. Резервная политика. При необходимости можно перевести неактивную политику в активный статус.
     - **Для автономных пользователей**. Эта политика активируется, когда компьютер покидает периметр сети организации.
   - Настроить наследование параметров:
     - **Наследовать параметры родительской политики**. Если включен этот переключатель, значения параметров политики наследуются из политики верхнего уровня. Параметры политики недоступны для изменения, если для родительской политики установлен .
     - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики распространяются на дочерние политики. В параметрах дочерней политики автоматически устанавливается флажок **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из родительской политики, за исключением параметров, отмеченных . Параметры дочерней политики недоступны для изменения, если для родительской политики установлен .
8. На закладке **Параметры приложения** настройте параметры политики в соответствии с вашими требованиями.
9. Нажмите на кнопку **Сохранить**.

После создания новой политики создается набор разрешающих правил для предотвращения блокировки программ и обеспечения их непрерывной работы.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes создает набор правил для входящего сетевого трафика при создании новой политики:

- Два разрешающих правила для процесса совместного доступа к рабочему столу Windows с помощью Агента администрирования Kaspersky Security Center, расположенных в папках %Program Files% и %Program Files (x86)%. Статус: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.

- Два разрешающих правила для локального порта 15000. Состояние: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes создает набор правил для исходящего сетевого трафика при создании новой политики:

- Два разрешающих правила для службы Kaspersky Industrial CyberSecurity for Nodes, расположенных в папках %Program Files% и %Program Files (x86)%. Статус: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.

- Два разрешающих правила для рабочего процесса Kaspersky Industrial CyberSecurity for Nodes, расположенных в папках %Program Files% и %Program Files (x86)%. Статус: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.

- Два разрешающих правила для локального порта 13000. Состояние: включено. Разрешенные внешние адреса: все. Протоколы: TCP и UDP, по одному правилу на протокол.

Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Industrial CyberSecurity for Nodes, их создании, настройке параметров выполнения, запуске и остановке.

О создании задач с помощью Веб-плагина

Вы можете создавать локальные и групповые задачи следующими способами:

- Для отдельного защищаемого устройства: в окне **<Имя защищаемого устройства>** в разделе **Задачи**.

- Для группы администрирования: в панели результатов узла выбранной группы защищаемых устройств на закладке **Задачи**.

- Для набора защищаемых устройств: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач *Обновление* и *Проверка по требованию* на всех защищаемых устройствах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center приведена в справке Kaspersky Security Center.

Создание задачи с помощью Веб-плагина

Чтобы создать новую задачу в Web Console:

1. Запустите мастер создания задачи одним из следующих способов:

   - Для создания локальной задачи:

     a. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

     b. Выберите название защищаемого устройства.

     c. В открывшемся окне **<Имя устройства>** выберите вкладку **Задачи**.

     d. Нажмите на кнопку **Добавить**.

   - Для создания групповой задачи:

     a. В главном окне Web Console выберите **Управление активами** → **Задачи**.

     b. Нажмите на кнопку **Добавить**.

   Откроется окно мастера создания задачи.

2. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.

3. В раскрывающемся списке **Тип задачи** выберите тип создаваемой задачи.

4. В зависимости от выбранного типа задачи выполните одно из следующих действий:

   - Создайте задачу проверки по требованию.

   - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:

     a. В блоке **Источники обновлений** можно указать Сервер администрирования Kaspersky Security Center или Серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

     Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

     b. Настройте параметры функции, снижающей нагрузку на дисковую подсистему:

     c. Вы можете указать действия, которые Kaspersky Industrial CyberSecurity for Nodes будет совершать при наличии критических обновлений модулей программы, а также по завершении установки критических обновлений. Кроме того, можно указать, будет ли Kaspersky Industrial CyberSecurity for Nodes получать информацию о доступных плановых обновлениях.

     d. Укажите состав обновлений для копирования и путь к папке, в которой Kaspersky Industrial CyberSecurity for Nodes будет сохранять скопированные обновления.

- Для создания задачи Активация приложения:

  a. В окне **Выбор лицензионного ключа** укажите файл ключа или код активации, с помощью которого вы хотите активировать программу.

  b. Установите флажок **Использовать ключ в качестве резервного**, если вы хотите создать задачу для продления срока действия лицензии.

- Создайте задачу Формирование правил контроля запуска программ и настройте ее параметры.
- Создайте задачу Формирование правил контроля устройств и настройте ее параметры.

5. Нажмите на кнопку **Далее**.
6. Если задача создана для набора защищаемых устройств, выберите сеть (группу) защищаемых устройств, на которых она будет выполняться.
7. Нажмите на кнопку **Далее**.
8. В окне **Завершение создания задачи** установите флажок **Открыть окно свойств задачи после ее создания**, чтобы настроить параметры задачи.
9. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

Настройка групповых задач с помощью Веб-плагина

Чтобы настроить групповую задачу для нескольких защищаемых устройств, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. Перейдите на вкладку **Параметры приложения**.
4. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:

   - Если вы настраиваете задачу *Проверка по требованию*:

     a. В разделе **Область проверки** настройте область проверки.

     b. В разделе **Настройки** настройте уровень эвристического анализа и интеграцию с другими компонентами программы.

- Для настройки задачи *Обновление* укажите параметры задачи в соответствии с вашими требованиями:

  a. В разделе **Источники обновлений** настройте параметры источника обновлений.

  b. В секции **Настройки обновлений** настройте параметры оптимизации дисковой подсистемы, укажите действия, которые Kaspersky Industrial CyberSecurity for Nodes будет совершать при наличии критических обновлений модулей приложения или при наличии информации о плановых обновлениях, настройте параметры копирования обновлений.

- Чтобы настроить задачу *Активация приложения*, примените файл ключа или код активации, с помощью которого вы хотите активировать приложение. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.

- Чтобы настроить автоматическое формирование разрешающих правил контроля устройств, укажите параметры, на основе которых будет сформирован список разрешающих правил.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи *Откат обновления*).

6. На закладке **Параметры** в разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе приведена в справке Kaspersky Security Center.

7. Нажмите на кнопку **Сохранить**.

Настроенные параметры групповых задач будут сохранены.

Настройка задачи Активация приложения с помощью Веб-плагина

Чтобы настроить задачу Активация приложения, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.

3. В разделе **Параметры приложения** укажите файл ключа, с помощью которого вы хотите активировать приложение. Установите флажок **Использовать ключ в качестве резервного**, если вы хотите добавить ключ для продления срока действия лицензии.

4. Настройте расписание задачи в разделе **Расписание**.

5. В окне **<Название задачи>** нажмите на кнопку **Сохранить**.

Настройка задачи обновления с помощью Веб-плагина

Чтобы настроить задачу Обновление, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно <Название задачи>.
3. Выберите закладку **Параметры приложения**.
4. В разделе **Источники обновлений** настройте параметры источника обновлений:

   a. Укажите Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновлений: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

   Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

   b. Настройте параметры функции, снижающей нагрузку на дисковую подсистему:

   - **Снизить нагрузку на дисковую подсистему**
   - **Объем оперативной памяти, используемой для оптимизации (МБ)**

   c. Укажите действия, которые Kaspersky Industrial CyberSecurity for Nodes будет совершать при наличии критических обновлений модулей приложения или при наличии информации о плановых обновлениях.

   d. Укажите настройки копирования обновлений.
5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи *Откат обновления*).
6. В окне **<Название задачи>** нажмите на кнопку **ОК**.

Настройка расписания задач

В Web Console вы можете настроить расписание локальных системных и пользовательских задач.

Чтобы настроить расписание групповых задач с помощью Web Console, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.

3. Перейдите в раздел **Расписание** и настройте параметры расписания (см. таблицу ниже) в соответствии с вашими требованиями.

> Поля с параметрами расписания задач проверки по требованию и обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры запуска задачи.

Параметры расписания задач

Параметр	Описание
Запуск по расписанию	Выберите режим запуска задачи: • **Каждый N час**. Задача будет запускаться с периодичностью в заданное количество часов. Укажите время запуска задачи и период в часах. • **Каждые N дней**. Задача будет запускаться с периодичностью в заданное количество дней. Укажите время запуска задачи и период в днях. • **Каждые N минут**. Задача будет запускаться с периодичностью в заданное количество минут. Укажите время запуска задачи и период в минутах. • **По дням недели**. Задача будет запускаться в указанные дни недели. Выберите дни недели и укажите время запуска. При необходимости запуска задачи с интервалом в несколько недель введите требуемое значение в поле **Период**. • **Ежемесячно**. Задача будет запускаться в определенный день месяца. Укажите число и время запуска. • **Один раз**. Задача будет запускаться однократно в указанный день и время. • **Вручную**. Режим запуска, при котором вы запускаете проверку вручную в удобное для вас время. • **При загрузке обновлений в хранилище**. Задача будет запускаться после каждой загрузки обновлений в хранилище. • **По завершении другой задачи**. Задача будет запускаться после завершения другой задачи. Выберите задачу и статус ее выполнения. Kaspersky Industrial CyberSecurity for Nodes не поддерживает режим **По завершении другой задачи** для настройки расписания локальных задач. • **При обнаружении вирусной атаки**. Задача будет запускаться в случае обнаружения вирусной атаки. • **Запустить через N (мин) после запуска приложения**. Задача будет запускаться при каждом запуске Kaspersky Industrial CyberSecurity for Nodes через указанное время. Укажите количество минут в поле **Задержка запуска задачи (мин)**.
Запускать пропущенные задачи	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes запускает пропущенную задачу, как только это станет возможным. Задача может быть пропущена, например, если в установленное время запуска задачи был выключен компьютер. Когда у приложения появляется возможность выполнить пропущенные задачи, для распределения нагрузки на компьютер приложение запускает задачи не одновременно, а случайным образом в течение определенного интервала времени. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.
Использовать автоматическое определение случайного интервала между запусками задачи	Если флажок установлен, задача запускается на компьютерах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Использовать автоматическую случайную задержку запуска задачи в интервале	Если флажок установлен, задача запускается на компьютерах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества компьютеров к Серверу администрирования при запуске задачи по расписанию. Если флажок снят, запуск задачи на компьютерах выполняется по расписанию.
Включать устройства перед запуском задачи функцией Wake-on-LAN	Если флажок установлен, операционная система на компьютере будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут. Установите флажок, если вы хотите запустить выполнение задачи на всех компьютерах, включая компьютеры, которые выключены.
Выключать устройства после выполнения задачи	Если флажок установлен, компьютер будет выключен после выполнения задачи. Например, вы можете включить эту функцию для проверки компьютера в пятницу после рабочего дня. После завершения работы задачи приложение выключает компьютер на выходные.

Параметр	Описание
Остановить, если задача выполняется дольше	Ограничение длительности выполнения задачи. По истечении заданного времени Kaspersky Industrial CyberSecurity for Nodes останавливает выполнение задачи. При этом задача не будет завершена. Следующий запуск задачи Kaspersky Industrial CyberSecurity for Nodes выполнит сначала и по расписанию.
Приостановка выполнения задачи	Вы можете задавать временной интервал, в течение которого выполнение ранее запущенной по расписанию задачи будет приостановлено. По окончании заданного периода времени выполнение задачи будет возобновлено. Это может понадобиться, например, для снижения влияния Kaspersky Industrial CyberSecurity for Nodes на производительность компьютера в период наиболее активного его использования. Данная функция доступна только для задач проверки по требованию.
Дата окончания	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes прекратит выполнение задачи по расписанию начиная с указанной даты. Для задачи будет установлен режим запуска **Вручную**. Данная функция доступна только для задач проверки по требованию.

Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Industrial CyberSecurity for Nodes доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в справке Kaspersky Security Center.

Отчет о статусе компонентов Kaspersky Industrial CyberSecurity for Nodes components

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Выполняется*, *Приостановлено*, *Остановлено*, *Не поддерживается лицензией*.

Состояние *Не установлен* относится к компонентам приложения, а не к самому приложению. Если приложение не установлено, Kaspersky Security Center Web Console присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в см. в справке Kaspersky Security Center.

Чтобы просмотреть статус компонентов в Web Console, выполните следующие действия:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. Щелкните по названию устройства и перейдите в раздел **Приложения**.
3. Щелкните по названию приложения Kaspersky Industrial CyberSecurity for Nodes.
4. В открывшемся окне на закладке **Общие** перейдите в раздел **Компоненты**.
5. Ознакомьтесь с таблицей состояния компонентов.

Чтобы просмотреть стандартный отчет в Web Console, выполните следующие действия:

1. Выберите **Мониторинг** → **Отчеты**.
2. В списке выберите **Отчет о статусе компонентов приложения** и нажмите на него.

   Будет сформирован отчет.
3. Ознакомьтесь со следующими элементами отчета:
   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
   - детальная таблица, показывающая статус, версию, устройство и группу компонента.

Отчеты о запрещенных программах в активном и в тестовом режимах

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Информировать). В этих отчетах приведена информация о заблокированных программах на защищаемых устройствах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

Чтобы просмотреть отчет о запрещенных программах в режиме Информировать, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме Информировать.
2. Выберите **Мониторинг** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных приложениях в тестовом режиме** и нажмите на него.

   Будет сформирован отчет.

4. Ознакомьтесь со следующими элементами отчета:

   - диаграмма, показывающая 10 программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме Активный.
2. Выберите **Мониторинг** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных приложениях** и нажмите на него.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения.

О Лицензионном соглашении

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

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения и Политики конфиденциальности, описывающих обработку и передачу данных, следующими способами:

- Во время установки Kaspersky Industrial CyberSecurity for Nodes.
- Во время установки Консоли Kaspersky Industrial CyberSecurity for Nodes.
- Во время установки Kaspersky Security Gateway.
- Ознакомившись с документом license.txt, входящим в комплект поставки.
- На сайте "Лаборатории Касперского" (https://www.kaspersky.ru/business/eula).

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

О лицензии

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

Действующая лицензия дает право на использование приложения в соответствии с условиями Лицензионного соглашения, а также на получение технической поддержки при необходимости.

Объем услуг и срок использования приложения зависит от типа лицензии, используемой для активации приложения.

Приложение можно активировать двумя способами:

- С помощью файла ключа, дающего право на использование приложения в рамках коммерческой лицензии.
- С помощью кода активации для приобретения коммерческой лицензии.

По истечении срока действия коммерческой лицензии из всех компонентов и задач приложения без обновлений баз будут доступны:

- Постоянная защита файлов;
- Контроль целостности системы;
- задачи проверки по требованию.

Чтобы продолжить использование Kaspersky Industrial CyberSecurity for Nodes в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии. Рекомендуем продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

Если удалить лицензионный ключ, приложение продолжит работать. Компонент Контроль целостности системы останется доступным, а остальные компоненты, задачи и обновление баз Kaspersky Industrial CyberSecurity for Nodes станут недоступны. То же самое произойдет, если "Лаборатория Касперского" добавит вашу лицензию в список запрещенных.

О Лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

О ключе

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

Вы можете добавить ключ в приложение с помощью файла ключа или кода активации. Ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Специалисты "Лаборатории Касперского" могут поместить ключ в список запрещенных ключей из-за нарушения Лицензионного соглашения. Если ключ заблокирован, для работы приложения требуется добавить другой ключ.

Ключ может быть активным и резервным.

Активный ключ – ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен ключ для коммерческой лицензии. В приложении не может быть больше одного активного ключа.

Резервный ключ – ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Резервный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Резервный ключ может быть добавлен только при наличии активного ключа.

О файле ключа

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

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Industrial CyberSecurity for Nodes.

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

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

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации.

О коде активации

Код активации – уникальная последовательность из 20 символов (букв и цифр). Вам нужно ввести код активации, чтобы добавить ключ для активации Kaspersky Industrial CyberSecurity for Nodes. Вы получаете код активации на адрес электронной почты, указанный при приобретении Kaspersky Industrial CyberSecurity for Nodes.

Чтобы активировать приложение помощью кода активации, необходим доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Можно восстановить утерянный после установки приложения код активации. Код активации может понадобиться, например, чтобы зарегистрировать Kaspersky CompanyAccount. Чтобы восстановить код активации, обратитесь к партнеру "Лаборатории Касперского", у которого вы приобрели лицензию.

Активация приложения с помощью файла ключа

Вы можете активировать Kaspersky Industrial CyberSecurity for Nodes с помощью файла ключа.

Чтобы активировать Kaspersky Industrial CyberSecurity for Nodes с помощью файла ключа:

1. В дереве Консоли приложения разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить ключ**.
3. В открывшемся окне нажмите на кнопку **Обзор**.
4. Выберите файл ключа с расширением key.

   Вы также можете добавить ключ в качестве резервного. Для этого установите флажок **Использовать в качестве дополнительного ключа**.

5. Нажмите на кнопку **OK**.

Будет применен выбранный файл ключа. При этом:

- Если для активации приложения уже добавлен активный ключ и вы добавите другой ключ в качестве активного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее ключ будет удален.
- Если для активации приложения уже добавлен резервный ключ и вы добавите другой ключ в качестве дополнительного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее резервный ключ будет удален.
- Если для активации приложения уже добавлены активный ключ и резервный ключ, а вы добавите новый ключ в качестве активного, то новый ключ заменит ранее добавленный активный ключ, а резервный ключ не будет удален.

Информация о добавленном ключе отобразится в панели результатов узла **Лицензирование**.

Активация приложения с помощью кода активации

Для активации приложения с помощью кода активации защищаемое устройство должно быть подключено к интернету.

Вы можете активировать Kaspersky Industrial CyberSecurity for Nodes с помощью кода активации.

При активации этим способом Kaspersky Industrial CyberSecurity for Nodes отправляет данные на сервер активации для проверки введенного кода:

- В случае успешной проверки кода активации приложение будет активировано.
- При сбое проверки кода активации отобразится соответствующее уведомление. В этом случае обратитесь к поставщику, у которого была приобретена лицензия на приложение Kaspersky Industrial CyberSecurity for Nodes.
- В случае превышения количества активаций с помощью указанного кода активации, отображается соответствующее уведомление. Процесс активации приложения будет прерван, и вам будет предложено обратиться в Службу технической поддержки.

Вы можете активировать Kaspersky Industrial CyberSecurity for Nodes, используя код активации в Консоли приложения или создав групповую задачу *Активация приложения* с помощью Плагина управления или Веб-плагина.

Чтобы активировать Kaspersky Industrial CyberSecurity for Nodes с помощью кода активации в Консоли приложения:

1. В дереве Консоли приложения разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить код активации**.
3. В открывшемся окне введите код активации в поле **Код активации**.
   - Чтобы применить код активации для добавления резервного ключа, установите флажок **Использовать в качестве дополнительного ключа**.
   - Чтобы просмотреть информацию о лицензии, нажмите на кнопку **Показать информацию о лицензии**. Информация отобразится в блоке **Информация о лицензии**.
4. Нажмите на кнопку **OK**.

   Kaspersky Industrial CyberSecurity for Nodes отправит информацию о примененном коде активации на сервер активации.

Просмотр информации о действующей лицензии

Просмотр статуса лицензии

Информация о статусе действующей лицензии отображается в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** Консоли приложения. Статус лицензии может принимать следующие значения:

- **Выполняется проверка статуса ключа** – Kaspersky Industrial CyberSecurity for Nodes проверяет добавленный файл ключа и ожидает ответа о текущем статусе.
- **Действующая лицензия до** – приложение Kaspersky Industrial CyberSecurity for Nodes активировано до указанной даты. Статус выделен желтым цветом в следующих случаях:
  - до истечения срока действия лицензии остается 30 дней и не добавлен резервный ключ;
  - Добавленный ключ помещен в список запрещенных и будет заблокирован.

- **Приложение не активировано** – приложение Kaspersky Industrial CyberSecurity for Nodes не активировано, поскольку не добавлен ключ. Статус выделен красным цветом.
- **Срок действия лицензии истек** – приложение Kaspersky Industrial CyberSecurity for Nodes не активировано, поскольку истек срок действия лицензии. Статус выделен красным цветом.
- **Нарушено Лицензионное соглашение** – приложение Kaspersky Industrial CyberSecurity for Nodes не активировано, поскольку нарушены условия Лицензионного соглашения. Статус выделен красным цветом.
- **Ключ добавлен в запрещенный список** – добавленный файл ключа заблокирован и помещен в список запрещенных ключей специалистами "Лаборатории Касперского", например, если ключ был использован сторонними лицами для незаконной активации приложения. Статус выделен красным цветом.

Просмотр информации о действующей лицензии

Чтобы просмотреть информацию о действующей лицензии,

в дереве Консоли приложения разверните узел **Лицензирование**.

В панели результатов узла **Лицензирование** отобразится общая информация о действующей лицензии (см. таблицу ниже).

Общая информация о лицензии в узле Лицензирование

Поле	Описание
Статус кода активации или ключа	Статус кода активации или ключа: *Активный ключ* или *Дополнительный*.
Дата окончания срока действия	Дата и время окончания срока действия лицензии, связанной с активным ключом.
Тип лицензии	Тип лицензии: *Коммерческая лицензия*.
Статус активации	Информация о статусе активации может принимать следующие значения: • **Применено** – если вы активировали приложение с помощью ключа. • **Активация приложения** – если вы применили код активации для активации приложения и процесс активации еще не закончен. Статус изменяется на **Применено** после завершения активации приложения и обновления содержимого панели результатов узла. • **Ошибка активации** – если не удалось активировать приложение. Вы можете посмотреть причину неудачного завершения активации в журнале выполнения задач.
Ключ	Номер ключа, с помощью которого вы активировали приложение.

Чтобы просмотреть подробную информацию о лицензии,

в панели результатов узла **Лицензирование** откройте контекстное меню требуемой лицензии и выберите пункт **Свойства**.

Подробная информация о лицензии в окне Свойства ключа

Поле	Описание
Ключ	Номер ключа, с помощью которого вы активировали программу.
Приложение	Название программы, которая была активирована с помощью добавленного ключа.
Тип лицензии	Тип лицензии: коммерческая или пробная.
Срок действия лицензии	Количество дней, начиная с даты активации приложения, в течение которых действует лицензия.
Дата активации	Дата добавления ключа в приложение.

Поле	Описание
Дата окончания срока действия	Дата окончания срока действия лицензии по активному ключу. Если вы активируете программу по неограниченной подписке, в поле указывается значение *Не ограничена*. Если программе Kaspersky Industrial CyberSecurity for Nodes не удается определить дату окончания действия лицензии, указывается значение *Неизвестна*.
Истекает через (сут)	Число суток, оставшихся до даты окончания срока действия лицензии по активному ключу.
Право на техническую поддержку	Информация о том, оказывает ли "Лаборатории Касперского" или ее партнеры техническую поддержку заказчику по условиям предоставления лицензии.
Информация о поддержке	Контактная информация "Лаборатории Касперского" или партнера, который осуществляет техническую поддержку. Поле может быть пустым, если техническая поддержка не осуществляется.
Информация о владельце	Информация о заказчике лицензии: имя заказчика и название организации, для которой приобретена лицензия.
Информация о лицензии	Номер и тип действующей лицензии.
Функциональность	Функции приложения, которые доступны по лицензии.

Продление срока действия лицензии

По умолчанию Kaspersky Industrial CyberSecurity for Nodes уведомляет вас о скором окончании срока действия лицензии за 30 дней до окончания срока действия лицензии.

Вы можете продлить срок действия лицензии, не дожидаясь его окончания, с помощью резервного ключа. Это позволяет не прерывать защиту устройства на период после окончания срока действия лицензии и до активации приложения по новой лицензии.

Чтобы обновить лицензию:

1. Получите новый файл ключа или код активации.
2. В дереве Консоли приложения выберите узел **Лицензирование**.
3. В панели результатов узла **Лицензирование** выполните одно из следующих действий:
   - Если вы хотите продлить срок действия лицензии с помощью файла ключа:
     a. Перейдите по ссылке **Добавление ключа**.
     b. В открывшемся окне нажмите на кнопку **Обзор**.
     c. Выберите новый файл ключа с расширением key.
     d. Установите флажок **Использовать в качестве дополнительного ключа**.
   - Если вы хотите продлить срок действия лицензии с помощью кода активации:
     a. Перейдите по ссылке **Добавить код активации**.
     b. В открывшемся окне введите приобретенный код активации.
     c. Установите флажок **Использовать в качестве дополнительного ключа**.

Для применения кода активации необходимо подключение к интернету.

4. Нажмите на кнопку **OK**.

Резервный ключ будет добавлен и автоматически станет активным по истечении срока действия текущей лицензии на Kaspersky Industrial CyberSecurity for Nodes.

Удаление ключа

Если вы удалите добавленный ключ, вы можете его восстановить, повторно применив файл ключа.

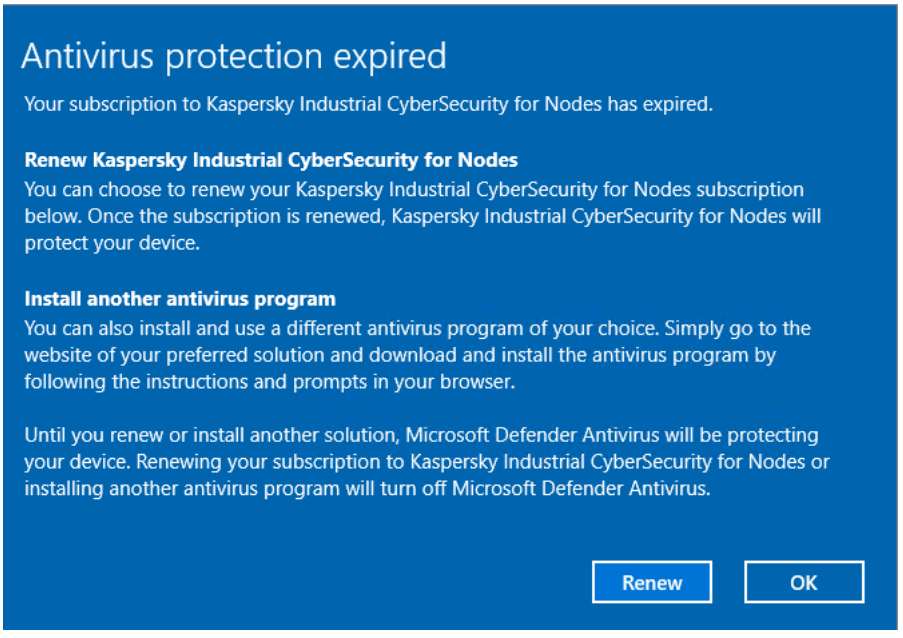
Чтобы удалить добавленный ключ:

1. В дереве Консоли приложения выберите узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** в таблице с информацией о добавленных ключах выберите ключ, который вы хотите удалить.
3. В контекстном меню строки с информацией о выбранном ключе выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить удаление ключа.

   Выбранный ключ будет удален.

После удаления ключа компьютер остается без защиты Kaspersky Industrial CyberSecurity for Nodes. Далее приложение отправляет команду о статусе защиты в Центр безопасности Windows (англ. Windows Security Center – WSC) для включения встроенных инструментов защиты. При этом приложение показывает окно с предложением продлить срок действия лицензии (см. рис. ниже). Если всплывающее окно мешает работе других приложений, и вы хотите выключить отображение этого окна, задайте значение для ключа реестра `NeedShowUPAOWindows=0`. Ключ расположен в ветке `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\environment\`.

При выключении отображения окна продления срока действия лицензии приложение Kaspersky Industrial CyberSecurity for Nodes не отправляет команду о статусе защиты в Центр безопасности Windows. Таким образом, Центр безопасности Windows не включает встроенные инструменты защиты. Учитывайте этот риск при выключении отображения окна.



Окно с предложением продлить срок действия лицензии

Запуск и остановка Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит информацию о запуске и остановке Kaspersky Industrial CyberSecurity for Nodes, а также о запуске Консоли Kaspersky Industrial CyberSecurity for Nodes и Плагина Kaspersky Security Center для управления приложением.

Запуск и остановка приложения

После установки Kaspersky Industrial CyberSecurity for Nodes на компьютер пользователя запуск приложения выполняется автоматически. Далее по умолчанию запуск Kaspersky Industrial CyberSecurity for Nodes выполняется сразу после операционной системы. Настроить автоматический запуск приложения в параметрах операционной системы невозможно.

Загрузка антивирусных баз Kaspersky Industrial CyberSecurity for Nodes после загрузки операционной системы занимает до двух минут, в зависимости от производительности (технических возможностей) компьютера. В течение этого времени уровень защиты компьютера снижен. Загрузка антивирусных баз при запуске приложения Kaspersky Industrial CyberSecurity for Nodes в уже запущенной операционной системе не вызывает снижения уровня защиты компьютера.

Как настроить автоматический запуск приложения в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Настройки приложения → Безопасность и надежность** и нажмите на кнопку **Настройка**.
4. На вкладке **Безопасность** используйте флажок **Запускать приложение при включении компьютера (рекомендуется)**, чтобы включить или выключить автоматический запуск приложения.
5. Сохраните внесенные изменения.

Как настроить автоматический запуск приложения в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Настройки приложения → Безопасность и надежность**.
5. Нажмите на кнопку **Настроить**.

   Откроется окно **Безопасность и надежность**.

6. Используйте флажок **Запускать приложение при включении компьютера (рекомендуется)**, чтобы включить или выключить автоматический запуск приложения.

7. Сохраните внесенные изменения.

Как настроить автоматический запуск приложения в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes**.

2. В контекстном меню узла выберите пункт **Свойства приложения**.

3. В открывшемся окне выберите вкладку **Настройки безопасности**.

4. Используйте флажок **Запускать приложение при включении компьютера (рекомендуется)**, чтобы включить или выключить автоматический запуск приложения.

5. Сохраните внесенные изменения.

Вы можете останавливать и запускать Kaspersky Industrial CyberSecurity for Nodes, если вы входите в группу "Администраторы" на защищаемом устройстве.

Как запустить или остановить приложение в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

2. В рабочей области выберите вкладку **Устройства**.

3. Откройте свойства компьютера двойным щелчком мыши.

4. В окне свойств компьютера выберите раздел **Приложения**.

5. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Industrial CyberSecurity for Nodes (5.0.0)**.

6. Выполните одно из следующих действий:

   - Если вы хотите запустить приложение, справа от списка приложений "Лаборатории Касперского" нажмите на кнопку .
   - Если вы хотите остановить работу приложения, справа от списка приложений "Лаборатории Касперского" нажмите на кнопку .

Как запустить или остановить приложение в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

2. Нажмите на имя компьютера, на котором вы хотите запустить или остановить Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств компьютера.

3. Выберите вкладку **Приложения**.

4. Установите флажок напротив приложения **Kaspersky Industrial CyberSecurity for Nodes (5.0.0)**.

5. Нажмите на кнопку **Запустить** или **Остановить**.

Как запустить или остановить приложение в Консоли приложения

1. Для остановки Kaspersky Industrial CyberSecurity for Nodes выполните следующие действия:

   a. Откройте Консоль приложения.

   > Учетная запись пользователя должна обладать правами на доступ к функции **Завершение работы приложения**.

   b. В дереве Консоли приложения откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.

   c. Выберите пункт **Остановить приложение**.

   d. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить остановку приложения.

   Приложение будет остановлено.

2. Для запуска **Kaspersky Industrial CyberSecurity for Nodes**, выполните следующие действия:

   a. Запустите файл avpui.exe, расположенный в папке установки Консоли приложения на защищаемом устройстве. По умолчанию файл расположен в папке C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console.

   Откроется окно **Выбор защищаемого устройства**.

   b. Если Kaspersky Industrial CyberSecurity for Nodes и Консоль приложения установлены на одном компьютере, выберите **Локальный компьютер (компьютер, на котором запущена Консоль приложения)**.

   c. Если Kaspersky Industrial CyberSecurity for Nodes и Консоль приложения установлены на разных компьютерах:

      1. Выберите **Другое устройство**.

      2. С помощью кнопки **Обзор** укажите имя компьютера с установленным приложением.

      3. Укажите порт для подключения к компьютеру с установленным приложением:

         - **С учетными данными Windows**. Порт для подключения с учетными данными Windows. Значение по умолчанию – 13032.

         - **С учетными данными вручную созданных пользователей**. Порт для подключения с учетными данными вручную созданных пользователей. Значение по умолчанию – 13031.

   d. При необходимости включите функцию **Использовать аутентификацию** и укажите учетные данные для подключения Консоли приложения к компьютеру с установленным приложением. Указанная учетная запись должна обладать правами на доступ к функциям **Чтение настроек** и **Удаленное подключение к приложению** на компьютере с установленным приложением.

   e. Нажмите на кнопку **Управление службой приложения**.

f. В открывшемся окне нажмите на кнопку **Запустить**.

Приложение будет запущено.

Окно **Выбор защищаемого устройства** открывается также в случае разрыва соединения с компьютером, на котором установлено приложение, или прекращения работы сервиса KICS в результате ошибки. Вы можете использовать кнопку **Запустить** для восстановления работы сервиса KICS.

Также вы можете выполнить запуск и остановку приложения из командной строки.

Приостановка и восстановление защиты и контроля компьютера

Приостановка защиты и контроля компьютера означает выключение на некоторое время всех компонентов защиты и всех компонентов контроля Kaspersky Industrial CyberSecurity for Nodes.

Состояние приложения отображается с помощью значка приложения в области уведомлений панели задач:

- значок свидетельствует о приостановке защиты и контроля компьютера;
- значок свидетельствует о том, что защита и контроль компьютера включены.

Приостановка и возобновление защиты и контроля компьютера не оказывает влияния на выполнение задач проверки и задачи обновления.

Если в момент приостановки и возобновления защиты и контроля компьютера были установлены сетевые соединения, на экран выводится уведомление о разрыве этих сетевых соединений.

Чтобы приостановить защиту и контроль компьютера:

1. В дереве Консоли приложения откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Приостановить защиту**.
3. Выберите один из следующих вариантов:
   - **Приостановить на указанное время <период времени>** – защита и контроль компьютера включатся через интервал времени, указанный в раскрывающемся списке ниже.
   - **Приостановить до перезагрузки** – защита и контроль компьютера включатся после перезапуска приложения или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск приложения.
   - **Приостановить** – защита и контроль компьютера включатся тогда, когда вы решите возобновить их.

Kaspersky Industrial CyberSecurity for Nodes приостановит работу всех компонентов защиты и контроля, не отмеченных в политике замком ().

Чтобы возобновить защиту и контроль компьютера:

1. Откройте контекстное меню значка приложения, который расположен в области уведомлений панели задач.

2. В контекстном меню выберите пункт **Возобновить защиту**.

Вы можете возобновить защиту и контроль компьютера в любой момент, независимо от того, какой вариант приостановки защиты и контроля компьютера вы выбрали ранее.

Диагностическое окно

В этом разделе описано использование диагностического окна.

О диагностическом окне

Компонент Диагностическое окно устанавливается и удаляется вместе с компонентом Значок области уведомлений независимо от Консоли приложения и может быть использован, даже если Консоль приложения не установлена на защищаемом устройстве. Диагностическое окно запускается через значок области уведомлений или путем запуска файла avpui.exe из папки программы на защищаемом устройстве.

В диагностическом окне можно выполнять следующие действия:

- открывать окно **О приложении** со списком установленных обновлений и доступных исправлений;
- просматривать информацию об общем статусе программы;
- просматривать произошедшие инциденты безопасности;
- просматривать текущую активность на защищаемом устройстве;
- запускать и останавливать запись файлов дампов и файлов трассировки;
- создавать Portable Auditor;
- открывать Консоль приложения.

Вы можете просматривать Диагностическое окно, даже если доступ к функциям Kaspersky Industrial CyberSecurity for Nodes защищен паролем. Введение пароля не требуется.

Диагностическое окно невозможно настроить через Kaspersky Security Center.

Просмотр состояния Kaspersky Industrial CyberSecurity for Nodes с помощью диагностического окна

Чтобы просмотреть состояние приложения с помощью Диагностического окна:

1. Откройте Диагностическое окно одним из следующих способов:

   - Запустите файл avpui.exe, расположенный в папке установки приложения на защищаемом устройстве. По умолчанию файл расположен в папке C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.

   - Нажмите на значок приложения в области уведомлений панели задач.

2. В разделе **Статус защиты** вы можете просмотреть текущий статус ключа, а также статус задач постоянной защиты компьютера и задач обновления. Для уведомления о состояниях защиты используется цветовая индикация (см. таблицу ниже).

Цветовая индикация в диагностическом окне

Раздел	Состояние
Статус постоянной защиты	Панель *зеленого* цвета отображается при выполнении следующих условий: • Компонент Постоянная защита файлов включен. • Компонент Контроль запуска программ включен в режиме **Блокировать**.
	Панель *желтого* цвета отображается, если выполнено одно или несколько из следующих условий: • Компонент Постоянная защита файлов выключен. • Компонент Контроль запуска программ включен в режиме **Информировать**.
	Панель *красного* цвета отображается, если выполнены оба условия: • Компонент Постоянная защита файлов не установлен или выключен. • Компонент Контроль запуска программ не установлен или включен в режиме **Информировать**.
Лицензирование	Панель *зеленого* цвета отображается при действующей лицензии.
	Панель *желтого* цвета отображается, если возникло одно из следующих событий: • *Выполняется проверка статуса лицензии.* • *До истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ или код активации.* • *Добавленный ключ помещен в список запрещенных и будет заблокирован.*
	Панель *красного* цвета отображается, если возникло одно из следующих событий: • *Приложение не активировано.* • *Срок действия лицензии истек.* • *Нарушено Лицензионное соглашение.* • *Ключ добавлен в запрещенный список.*
Обновление	Панель *зеленого* цвета отображается, если базы программы актуальны.
	Панель *желтого* цвета отображается, если базы программы устарели.
	Панель *красного* цвета отображается, если базы программы сильно устарели.

Просмотр статистики событий безопасности

В разделе **Статистика** отображаются все события безопасности. Статистика каждой задачи защиты отображается в отдельном блоке, где указано количество инцидентов, а также дата и время возникновения последнего инцидента. При регистрации инцидента цвет блока меняется на красный.

Чтобы просмотреть статистику:

1. Откройте Диагностическое окно одним из следующих способов:

   - Запустите файл avpui.exe, расположенный в папке установки приложения на защищаемом устройстве. По умолчанию файл расположен в папке C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.

   - Нажмите на значок приложения в области уведомлений панели задач.

2. Перейдите в раздел **Статистика**.

3. Просмотрите инциденты безопасности для задач защиты.

Просмотр текущей активности приложения

Чтобы просмотреть текущую активность приложения на защищаемом устройстве:

1. Откройте Диагностическое окно одним из следующих способов:

   - Запустите файл avpui.exe, расположенный в папке установки приложения на защищаемом устройстве. По умолчанию файл расположен в папке C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.

   - Нажмите на значок приложения в области уведомлений панели задач.

2. Перейдите в раздел **Текущая активность приложения**.

Для отображения статуса активности приложения используется цветовая индикация:

- В разделе **Задачи**:

  - *Зеленый цвет*. Не выполнены условия, при которых требовалась бы индикация красным цветом.

  - *Желтый цвет*. Проверка важных областей не проводилась давно.

  - *Красный цвет*. Выполнено как минимум одно из следующих условий:

    - Ни одна задача не запущена и расписание запуска не настроено ни для одной задачи.

    - Ошибки запуска программы зарегистрированы как критические события.

- В разделе **Kaspersky Security Network**:
  - *Зеленый цвет*. Задача **Использование Kaspersky Security Network** запущена.
  - *Желтый цвет*. Положение о KSN принято, но задача не запущена.

Настройка трассировки работы приложения и записи дампов памяти

Чтобы настроить трассировку работы приложения и запись дампов памяти:

1. Откройте Диагностическое окно одним из следующих способов:
   - Запустите файл avpui.exe, расположенный в папке установки приложения на защищаемом устройстве. По умолчанию файл расположен в папке C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0.
   - Нажмите на значок приложения в области уведомлений панели задач.
2. Перейдите в раздел **Диагностика сбоев**.
3. Используйте флажок **Включить защиту файлов дампов и файлов трассировки**, чтобы включить или выключить защиту файлов дампов и файлов трассировки.

   Если защита файлов дампов и файлов трассировки включена, доступ к файлам имеют следующие пользователи:
   - К файлам дампов имеют доступ системный и локальный администраторы, а также пользователь, включивший запись файлов дампов и файлов трассировки.
   - К файлам трассировки имеют доступ только системный и локальный администраторы.
4. Используйте флажок **Записывать отладочную информацию в файл трассировки**, чтобы включить или выключить трассировку работы приложения.

   По умолчанию трассировка работы приложения выключена.
5. Если необходимо, измените заданную по умолчанию папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки. Для этого нажмите на кнопку **Обзор** и выберите нужную папку.

   > Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

   Kaspersky Industrial CyberSecurity for Nodes создаст в выбранной папке подпапку для хранения файлов трассировки с названием logs-Kaspersky Industrial CyberSecurity for Nodes-<uid>, где <uid> – уникальный восьмизначный идентификатор.

6. Выберите уровень детализации отладочной информации:

   - **Обычный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждениях, а также информация о работе приложения в нормальном режиме (значение по умолчанию).
   - **Критический** – в файле трассировки сохраняются только сообщения о неустранимых ошибках.
   - **Диагностический** – в файле трассировки сохраняются сообщения обо всех ошибках, а также предупреждения.
   - **Важный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждения, а также дополнительная информация.
   - **Детальный** – в файле трассировки сохраняется вся информация о работе приложения.

   Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.

7. Для удаления старых файлов трассировки включите функцию **Заменять старые файлы трассировки более новыми**.

   Если функция включена, настройте максимальный размер и количество файлов трассировок:

   a. Укажите **Максимальный размер файла трассировки (МБ)**.

      Доступные значения: от 1 до 4095 МБ. Значение по умолчанию – 100 МБ.

   b. Укажите значение **Максимальное количество файлов трассировки**.

      Доступные значения: от 1 до 999. Значение по умолчанию – 5.

8. Используйте флажок **Создавать во время сбоя файл дампа в указанной папке**, чтобы включить или выключить трассировку работы приложения.

   По умолчанию запись дампов выключена.

9. Если необходимо, измените заданную по умолчанию папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки. Для этого нажмите на кнопку **Обзор** и выберите нужную папку.

   Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

10. Нажмите на кнопку **Применить**.

Механизмы самозащиты Kaspersky Industrial CyberSecurity for Nodes

Механизмы самозащиты предотвращают выполнение другими приложениями действий, которые могут нарушить работу Kaspersky Industrial CyberSecurity for Nodes. В приложении реализованы механизмы, обеспечивающие защиту от изменения или удаления папок приложения, процессов памяти и записей системного реестра. Также Kaspersky Industrial CyberSecurity for Nodes поддерживает технологию Antimalware Protected Process Light (AM-PPL) от Microsoft, которая защищает процессы приложения от вредоносных действий. Дополнительно приложение позволяет управлять правами доступа пользователей к функциям приложения и отдельно к службе приложения.

Включение и выключение механизмов самозащиты

Kaspersky Industrial CyberSecurity for Nodes предотвращает изменение и удаление файлов приложения на жестком диске, процессов в памяти и записей в системном реестре.

Технология блокирует доступ к следующим компонентам приложения:

- файлы в папке установки Kaspersky Industrial CyberSecurity for Nodes и другие файлы приложения;
- раздел реестра с ключами приложения;
- процессы, которые запускает приложение.

> Механизмы самозащиты не распространяются на процессы Kaspersky Industrial CyberSecurity for Nodes, инициированные недоверенными родительскими процессами.

По умолчанию механизмы самозащиты Kaspersky Industrial CyberSecurity for Nodes включены.

Как включить или выключить механизмы самозащиты в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Параметры приложения**.
4. В блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.
5. В открывшемся окне выберите вкладку **Безопасность**.
6. В блоке **Самозащита** используйте флажок **Защищать процессы приложения от внешних угроз**, чтобы включить или выключить механизмы самозащиты.
7. Закройте замок для применения политики на компьютерах.
8. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как включить или выключить механизмы самозащиты в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в панели результатов перейдите по ссылке **Свойства приложения**.
2. В открывшемся окне выберите вкладку **Настройки безопасности**.
3. В блоке **Самозащита** используйте флажок **Защищать процессы приложения от внешних угроз**, чтобы включить или выключить механизмы самозащиты.
4. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как включить или выключить механизмы самозащиты в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Настройки приложения**.
5. В блоке **Безопасность и надежность** нажмите на кнопку **Настроить**.

   Откроется окно **Безопасность и надежность**.
6. В блоке **Самозащита** используйте флажок **Защищать процессы приложения от внешних угроз**, чтобы включить или выключить механизмы самозащиты.
7. Закройте замок для применения политики на компьютерах.
8. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Поддержка технологии AM-PPL

Kaspersky Industrial CyberSecurity for Nodes поддерживает технологию Antimalware Protected Process Light (далее AM-PPL) от Microsoft. AM-PPL защищает процессы Kaspersky Industrial CyberSecurity for Nodes от вредоносных действий (например, завершение работы приложения). AM-PPL разрешает запуск только доверенных процессов. Процессы Kaspersky Industrial CyberSecurity for Nodes подписаны в соответствии с требованиями безопасности Windows, поэтому являются доверенными. Подробнее о технологии AM-PPL см. на сайте Microsoft. По умолчанию технология AM-PPL включена.

Kaspersky Industrial CyberSecurity for Nodes также имеет встроенные механизмы защиты процессов приложения. Поддержка AM-PPL позволяет делегировать функции защиты процессов операционной системе. Таким образом, вы увеличиваете быстродействие приложения и уменьшаете потребление ресурсов компьютера.

Программа регистрирует службу Kaspersky Industrial CyberSecurity for Nodes (AVP) и службу Kaspersky Seamless Update Service (AVPSUS). Технология AM-PPL защищает только службу AVP.

Используйте технологию AM-PPL постоянно. AM-PPL является важным компонентом защиты операционной системы. Разрешается выключать поддержку технологии AM-PPL только в отдельной тестовой среде для диагностики неисправностей в работе приложения.

Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

Чтобы включить или выключить поддержку технологии AM-PPL, выполните следующие действия:

1. Выключите механизм самозащиты приложения.

   Механизм самозащиты предотвращает изменение и удаление процессов приложения в памяти компьютера, в том числе изменение статуса AM-PPL.

2. Запустите интерпретатор командной строки cmd от имени администратора.

3. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Industrial CyberSecurity for Nodes.

4. Для включения поддержки технологии AM-PPL выполните команду:

   ```
   klpsm.exe enable
   ```

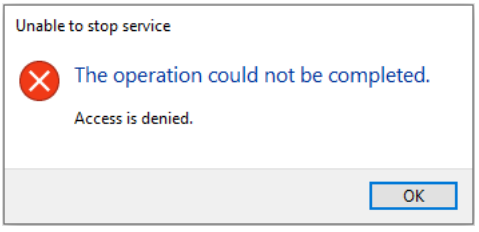
5. Для выключения поддержки технологии AM-PPL выполните команду:

   ```
   klpsm.exe disable
   ```

6. Перезапустите Kaspersky Industrial CyberSecurity for Nodes.

7. Возобновите работу механизма самозащиты приложения.

В результате при попытке пользователя остановить работу службы AVP отображается системное окно с ошибкой. Пользователь может управлять службами приложения только из интерфейса Kaspersky Industrial CyberSecurity for Nodes.



Ошибка доступа к службам приложения

Защита сервисов операционной системы

Вы можете разрешить или запретить сторонним приложениям совершать действия в отношении сервисов операционной системы с помощью функции Защищать сервисы операционной системы.

Как включить или выключить защиту сервисов ОС в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Параметры приложения**.
4. В блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.
5. В открывшемся окне выберите вкладку **Безопасность**.
6. Используйте флажок **Защищать сервисы операционной системы**, чтобы включить или выключить защиту сервисов операционной системы.

   Если защита сервисов операционной системы включена, сторонние приложения не могут совершать действия в отношении процессов операционной системы.

   Если защита сервисов операционной системы выключена, сторонние приложения могут совершать действия в отношении процессов операционной системы.

   После включения или выключения функции необходимо перезагрузить компьютер, чтобы изменения вступили в силу.
7. Закройте замок для применения политики на компьютерах.
8. Нажмите на кнопку **ОК** для сохранения внесенных изменений.

Как включить или выключить защиту сервисов ОС в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в панели результатов перейдите по ссылке **Свойства приложения**.
2. В открывшемся окне выберите вкладку **Настройки безопасности**.
3. Используйте флажок **Защищать сервисы операционной системы**, чтобы включить или выключить защиту сервисов операционной системы.

   Если защита сервисов операционной системы включена, сторонние приложения не могут совершать действия в отношении процессов операционной системы.

   Если защита сервисов операционной системы выключена, сторонние приложения могут совершать действия в отношении процессов операционной системы.

   После включения или выключения функции необходимо перезагрузить компьютер, чтобы изменения вступили в силу.
4. Нажмите на кнопку **ОК** для сохранения внесенных изменений.

Как включить или выключить защиту сервисов ОС в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Настройки приложения**.
5. В блоке **Безопасность и надежность** нажмите на кнопку **Настроить**.

   Откроется окно **Безопасность и надежность**.
6. Используйте флажок **Защищать сервисы операционной системы**, чтобы включить или выключить защиту сервисов операционной системы.

   Если защита сервисов операционной системы включена, сторонние приложения не могут совершать действия в отношении процессов операционной системы.

   Если защита сервисов операционной системы выключена, сторонние приложения могут совершать действия в отношении процессов операционной системы.

   После включения или выключения функции необходимо перезагрузить компьютер, чтобы изменения вступили в силу.
7. Закройте замок для применения политики на компьютерах.
8. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Настройка прав пользователей на управление Kaspersky Industrial CyberSecurity for Nodes

По умолчанию доступ ко всем функциям Kaspersky Industrial CyberSecurity for Nodes имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, пользователи группы KICS Administrators, созданной на защищаемом устройстве при установке Kaspersky Industrial CyberSecurity for Nodes, а также системная группа SYSTEM.

Пользователи, не зарегистрированные в списке пользователей Kaspersky Industrial CyberSecurity for Nodes, не могут открыть Консоль приложения.

Вы можете разрешить или запретить доступ к конкретным функциям Kaspersky Industrial CyberSecurity for Nodes для отдельных пользователей или групп пользователей.

Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Industrial CyberSecurity for Nodes.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение настроек	Возможности: • Импортировать в конфигурационный файл параметры работы Kaspersky Industrial CyberSecurity for Nodes. • Изменять параметры приложения.

Права доступа	Описание
Чтение настроек	Возможности: • Просматривать общие параметры Kaspersky Industrial CyberSecurity for Nodes и параметры задач; • Экспортировать в конфигурационный файл параметры Kaspersky Industrial CyberSecurity for Nodes; • Просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • Помещать объекты на карантин. • Удалять объекты из карантина и резервного хранилища. • Восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Industrial CyberSecurity for Nodes.
Лицензирование приложения	Возможность активировать Kaspersky Industrial CyberSecurity for Nodes.
Удаление приложения	Возможность удалить Kaspersky Industrial CyberSecurity for Nodes.
Чтение прав	Возможность просматривать список и права доступа пользователей Kaspersky Industrial CyberSecurity for Nodes.
Изменение прав	Возможности: • Изменять список пользователей, имеющих доступ к управлению приложением. • изменять права доступа пользователей к функциям Kaspersky Industrial CyberSecurity for Nodes.
Удаленное подключение к приложению	Возможность удаленно подключаться к приложению через Консоль приложения. Для удаленного доступа пользователь также должен обладать правами доступа к функции **Чтение настроек**.
Завершение работы приложения	Возможность завершать работу приложения через Консоль приложения.
Выключение политики Kaspersky Security Center	Возможность выключать политику Kaspersky Security Center.
Экспорт настроек	Возможность экспортировать настройки Kaspersky Industrial CyberSecurity for Nodes.
Изменение Диагностики сбоев	Возможность настраивать параметры трассировки работы приложения и записи дампов памяти.

Как настроить права пользователей на управление Kaspersky Industrial CyberSecurity for Nodes в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Дополнительные возможности**.
4. В разделе **Права пользователей на управление приложением** нажмите **Настройка**.
5. В открывшемся окне установите флажок **Разрешать подтверждение операций с приложением вводом учетных данных вручную созданных пользователей** и задайте пароль для учетной записи KLAdmin. Учетная запись будет автоматически добавлена в список учетных записей.
6. Если требуется, добавьте учетные записи, которым вы хотите предоставить доступ на управление приложением. Для этого нажмите на кнопку **Добавить** в таблице учетных записей.

   Откроется форма для настройки прав доступа пользователя.

7. Выберите способ добавления пользователей:

   - **Выбрать пользователя / группу из Active Directory**. Вы можете предоставить доступ к Kaspersky Industrial CyberSecurity for Nodes для отдельных пользователей или групп внутри домена Active Directory. Например, если группе "Все" запрещено завершать работу приложения, вы можете предоставить отдельному пользователю разрешение **Завершение работы приложения**.

   - **Добавить пользователя / группу вручную**. Вы можете создать учетную запись, которой нет в Active Directory, и назначить этой учетной записи отдельные разрешения. То есть вы можете создать *сервисную учетную запись* и использовать эту учетную запись вместо KLAdmin. Таким образом, вам не нужно делиться паролем от KLAdmin с другими пользователями или создавать новые учетные записи Active Directory. Вы можете задать любое имя пользователя и пароль. Например, вы можете предоставить пользователю сервисной учетной записи разрешение **Чтение журналов**. В результате, если для группы "Все" просмотр отчетов запрещен, вы можете открыть отчеты приложения с помощью сервисной учетной записи или учетной записи KLAdmin.

     Для добавления пользователя / группы пользователей вручную нужно включить Защиту паролем.

8. Выберите пользователя или группу пользователей, которым вы хотите предоставить доступ на управление приложением.

9. В списке **Разрешения** настройте права доступа пользователей к функциям приложениям.

10. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как настроить права пользователей на управление Kaspersky Industrial CyberSecurity for Nodes в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Права пользователей на управление приложением**.

2. В открывшемся окне установите флажок **Разрешать подтверждение операций с приложением вводом учетных данных вручную созданных пользователей** и задайте пароль для учетной записи KLAdmin. Учетная запись будет автоматически добавлена в список учетных записей.

3. Если требуется, добавьте учетные записи, которым вы хотите предоставить доступ на управление приложением. Для этого нажмите на кнопку **Добавить** в таблице учетных записей.

   Откроется форма для настройки прав доступа пользователя.

4. Выберите способ добавления пользователей:

   - **Выбрать пользователя / группу из Active Directory**. Вы можете предоставить доступ к Kaspersky Industrial CyberSecurity for Nodes для отдельных пользователей или групп внутри домена Active Directory. Например, если группе "Все" запрещено завершать работу приложения, вы можете предоставить отдельному пользователю разрешение **Завершение работы приложения**.

   - **Добавить пользователя / группу вручную**. Вы можете создать учетную запись, которой нет в Active Directory, и назначить этой учетной записи отдельные разрешения. То есть вы можете создать *сервисную учетную запись* и использовать эту учетную запись вместо KLAdmin. Таким образом, вам не нужно делиться паролем от KLAdmin с другими пользователями или создавать новые учетные записи Active Directory. Вы можете задать любое имя пользователя и пароль. Например, вы можете предоставить пользователю сервисной учетной записи разрешение **Чтение журналов**. В результате, если для группы "Все" просмотр отчетов запрещен, вы можете открыть отчеты приложения с помощью сервисной учетной записи или учетной записи KLAdmin.

     Для добавления пользователя / группы пользователей вручную нужно включить Защиту паролем.

5. Выберите пользователя или группу пользователей, которым вы хотите предоставить доступ на управление приложением.

6. В списке **Разрешения** настройте права доступа пользователей к функциям приложениям.

7. Сохраните внесенные изменения.

Как настроить права пользователей на управление Kaspersky Industrial CyberSecurity for Nodes в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Дополнительные возможности → Права пользователей на управление приложением** и нажмите на кнопку **Настроить**.

5. В открывшемся окне установите флажок **Разрешать подтверждение операций с приложением вводом учетных данных вручную созданных пользователей** и задайте пароль для учетной записи KLAdmin. Учетная запись будет автоматически добавлена в список учетных записей.

6. Если требуется, добавьте учетные записи, которым вы хотите предоставить доступ на управление приложением. Для этого нажмите на кнопку **Добавить** в таблице учетных записей.

   Откроется форма для настройки прав доступа пользователя.

7. Выберите способ добавления пользователей:

   - **Выбрать пользователя / группу из Active Directory**. Вы можете предоставить доступ к Kaspersky Industrial CyberSecurity for Nodes для отдельных пользователей или групп внутри домена Active Directory. Например, если группе "Все" запрещено завершать работу приложения, вы можете предоставить отдельному пользователю разрешение **Завершение работы приложения**.

   - **Добавить пользователя / группу вручную**. Вы можете создать учетную запись, которой нет в Active Directory, и назначить этой учетной записи отдельные разрешения. То есть вы можете создать *сервисную учетную запись* и использовать эту учетную запись вместо KLAdmin. Таким образом, вам не нужно делиться паролем от KLAdmin с другими пользователями или создавать новые учетные записи Active Directory. Вы можете задать любое имя пользователя и пароль. Например, вы можете предоставить пользователю сервисной учетной записи разрешение **Чтение журналов**. В результате, если для группы "Все" просмотр отчетов запрещен, вы можете открыть отчеты приложения с помощью сервисной учетной записи или учетной записи KLAdmin.

     Для добавления пользователя / группы пользователей вручную нужно включить Защиту паролем.

8. Выберите пользователя или группу пользователей, которым вы хотите предоставить доступ на управление приложением.

9. В списке **Разрешения** настройте права доступа пользователей к функциям приложениям.

10. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Настройка прав пользователей на управление службой Kaspersky Industrial CyberSecurity for Nodes Service

При установке Kaspersky Industrial CyberSecurity for Nodes регистрирует в Windows службу приложения – *Kaspersky Industrial CyberSecurity for Nodes Service*. Таким образом, приложение включает функциональные компоненты, запускаемые при запуске операционной системы. Чтобы снизить риск стороннего доступа к функциям приложения и параметрам безопасности защищаемого устройства с помощью службы приложения, можно ограничить права на управление службой Kaspersky Industrial CyberSecurity for Nodes Service.

По умолчанию доступ к управлению службой Kaspersky Industrial CyberSecurity for Nodes Service имеют пользователи, входящие в группу Администраторы на защищаемом устройстве. Права на чтение имеют группы SERVICE и INTERACTIVE, а права на чтение и исполнение имеет группа SYSTEM.

Вы не можете удалить учетную запись пользователя SYSTEM или изменять права этой учетной записи. Если права учетной записи SYSTEM были изменены, то при сохранении изменений для этой учетной записи восстанавливаются максимальные права.

Пользователи, имеющие доступ к функциям уровня Изменение прав, могут предоставлять права на управление службой Kaspersky Industrial CyberSecurity for Nodes Service другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Industrial CyberSecurity for Nodes один из следующих стандартных уровней доступа для управления службой Kaspersky Industrial CyberSecurity for Nodes Service:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Industrial CyberSecurity for Nodes Service, а также запускать и останавливать службу Kaspersky Industrial CyberSecurity for Nodes Service.
- **Чтение** – возможность просматривать общие параметры и права пользователей для службы Kaspersky Industrial CyberSecurity for Nodes Service.
- **Изменение** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Industrial CyberSecurity for Nodes Service.
- **Исполнение** – возможность запускать и останавливать службу Kaspersky Industrial CyberSecurity for Nodes Service.

Также вы можете выполнять расширенную настройку прав доступа: разрешить или запретить доступ к определенным функциям Kaspersky Industrial CyberSecurity for Nodes (см. таблицу ниже).

Права доступа к функциям службы Kaspersky Industrial CyberSecurity for Nodes Service

Функция	Описание
Чтение настроек службы	Возможность просматривать общие параметры и права пользователей для службы Kaspersky Industrial CyberSecurity for Nodes Service.
Запрос статуса службы у Диспетчера управления службами	Возможность запрашивать статус выполнения службы Kaspersky Industrial CyberSecurity for Nodes Service у Диспетчера управления службами Microsoft Windows.
Запрос статуса службы	Возможность запрашивать статус выполнения службы у Kaspersky Industrial CyberSecurity for Nodes Service.
Чтение списка зависимых служб	Возможность просматривать список служб, от которых зависит служба Kaspersky Industrial CyberSecurity for Nodes Service, а также служб, зависимых от службы Kaspersky Industrial CyberSecurity for Nodes Service.
Настройка службы	Возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Industrial CyberSecurity for Nodes Service.
Запуск службы	Возможность запускать выполнение службы Kaspersky Industrial CyberSecurity for Nodes Service.
Остановка службы	Возможность останавливать выполнение службы Kaspersky Industrial CyberSecurity for Nodes Service.
Приостановка / Возобновление службы	Возможность приостанавливать и возобновлять выполнение службы Kaspersky Industrial CyberSecurity for Nodes Service.
Чтение прав	Возможность просматривать список пользователей службы Kaspersky Industrial CyberSecurity for Nodes Service и права доступа каждого пользователя.
Изменение прав	Возможности: • добавлять и удалять пользователей службы Kaspersky Industrial CyberSecurity for Nodes Service; • изменять права доступа пользователей к службе Kaspersky Industrial CyberSecurity for Nodes Service.
Удаление службы	Возможность отмены регистрации службы Kaspersky Industrial CyberSecurity for Nodes Service в диспетчере управления службами Microsoft Windows.
Пользовательские запросы к службе	Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Industrial CyberSecurity for Nodes Service.

Вы можете изменить список пользователей и групп пользователей, которым разрешено управление службой Kaspersky Industrial CyberSecurity for Nodes Service, а также изменять права доступа этих пользователей и групп пользователей.

Как настроить права пользователей на управление службой Kaspersky Industrial CyberSecurity for Nodes Service в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Дополнительные возможности**.
4. В разделе **Права пользователей на управление службой KICS for Nodes Service** нажмите **Настройка**.

   Откроется форма для настройки прав доступа пользователя.
5. Добавьте пользователя или группу пользователей из Active Directory, для которых вы хотите настроить права доступа к службе Kaspersky Industrial CyberSecurity for Nodes Service.
6. Выберите пользователя или группу пользователей, которым вы хотите предоставить доступ на управление приложением.
7. В списке разрешений настройте права пользователей на управление службой Kaspersky Industrial CyberSecurity for Nodes Service.
8. Если требуется, настройте особые разрешения для пользователей:
   a. Нажмите на кнопку **Дополнительно**.
   b. В открывшемся окне выберите учетную запись пользователя.
   c. Откройте свойства учетной записи двойным щелчком мыши.
   d. В открывшемся окне перейдите по ссылке **Показать дополнительные разрешения**.
   e. В открывшемся окне настройте особые разрешения для пользователя.
9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как настроить права пользователей на управление службой Kaspersky Industrial CyberSecurity for Nodes Service в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Права пользователей на управление службой KICS for Nodes Service**.
2. В открывшемся окне в блоке **Разрешения** нажмите на кнопку **Добавить**.

   Откроется форма для настройки прав доступа пользователя.
3. Добавьте пользователя или группу пользователей из Active Directory, для которых вы хотите настроить права доступа к службе Kaspersky Industrial CyberSecurity for Nodes Service.
4. Выберите пользователя или группу пользователей, которым вы хотите предоставить доступ на управление приложением.
5. В списке разрешений настройте права пользователей на управление службой Kaspersky Industrial CyberSecurity for Nodes Service.

6. Если требуется, настройте особые разрешения для пользователей:

   a. Нажмите на кнопку **Дополнительно**.

   b. В открывшемся окне выберите учетную запись пользователя.

   c. Откройте свойства учетной записи двойным щелчком мыши.

   d. В открывшемся окне перейдите по ссылке **Показать дополнительные разрешения**.

   e. В открывшемся окне настройте особые разрешения для пользователя.

7. Сохраните внесенные изменения.

Как настроить права пользователей на управление службой Kaspersky Industrial CyberSecurity for Nodes Service в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Дополнительные возможности** → **Права пользователей на управление службой KICS for Nodes Service** и нажмите на кнопку **Настроить**.

   Откроется окно **Права пользователей на управление службой KICS for Nodes Service**.

5. Добавьте пользователя или группу пользователей из Active Directory, для которых вы хотите настроить права доступа к службе Kaspersky Industrial CyberSecurity for Nodes Service.

6. Выберите пользователя или группу пользователей, которым вы хотите предоставить доступ на управление приложением.

   Настроить особые разрешения на управление службой приложения в Web Console невозможно.

7. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению приложением и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить Защиту паролем в параметрах Kaspersky Industrial CyberSecurity for Nodes.

При попытке пользователя выполнить действие, защищенное паролем, Kaspersky Industrial CyberSecurity for Nodes предложит пользователю ввести имя пользователя и пароль или авторизоваться с помощью токена.

Имя пользователя и пароль

Защита паролем поддерживает работу со следующими учетными записями:

- **KLAdmin**. Учетная запись администратора без ограничений доступа к Kaspersky Industrial CyberSecurity for Nodes. Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем. Отменить разрешение для учетной записи KLAdmin невозможно. Kaspersky Industrial CyberSecurity for Nodes требует задать пароль для учетной записи KLAdmin во время включения Защиты паролем.

- **Учетная запись, добавленная вручную**. Учетная запись вне домена Active Directory. Это сервисная учетная запись, которую вы можете использовать вместо KLAdmin, чтобы не делиться паролем от учетной записи администратора. Вы можете задать любые имя пользователя и пароль, а также настроить отдельные разрешения.

- **Группа "Все"**. Стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети. Пользователи из группы "Все" могут получить доступ к приложению в соответствии с предоставленными разрешениями.

- **Отдельные пользователи или группы**. Учетные записи пользователей, для которых вы можете настроить отдельные разрешения. Например, если для группы "Все" выполнение действия запрещено, то вы можете разрешить выполнение действия для отдельного пользователя или группы.

Интерфейс Kaspersky Industrial CyberSecurity for Nodes скрывает вводимый пароль на экране. Kaspersky Industrial CyberSecurity for Nodes хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Industrial CyberSecurity for Nodes не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A–Z);
  - строчные латинские буквы (a–z);
  - цифры (0–9);
  - символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

Токен

Для доступа к функциям Kaspersky Industrial CyberSecurity for Nodes необходимо выбрать нужный сертификат пользователя из списка сертификатов, хранящихся на подключенном токене, и ввести PIN-код. Аутентификация по токену доступна только для пользователей внутри домена Active Directory. Администратор может настроить разрешения для отдельного пользователя или группы. Для работы аутентификации по токену необходимо развернуть доверенную инфраструктуру PKI, а также установить специальное программного обеспечение для работы с токеном.

Как защитить доступ к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Дополнительные возможности**.
4. В разделе **Права пользователей на управление приложением** нажмите на кнопку **Настройка**.
5. В открывшемся окне установите флажок **Разрешать подтверждение операций с приложением вводом учетных данных вручную созданных пользователей**.
6. Если требуется, снимите флажок **Запрашивать пароль для подтверждения критических действий**.

   Если функция включена, приложение будет запрашивать имя и пароль пользователя при удалении/изменении/восстановлении приложения и при выполнении действий в командной строке, которые могут привести к снижению уровня защиты устройства.

   Если эта функция выключена, и текущий пользователь обладает необходимыми правами, Kaspersky Industrial CyberSecurity for Nodes не будет запрашивать учетные данные. По умолчанию функция включена.

   > Если для учетной записи текущего пользователя установлен пустой пароль Windows, вам необходимо ввести учетные данные пользователя с необходимыми правами, для которого задан пароль.

7. Задайте пароль для учетной записи KLAdmin.
8. Если требуется, добавьте учетные записи, которым вы хотите предоставить доступ на управление приложением:

   a. Нажмите на кнопку **Добавить**.

      Откроется форма для настройки прав доступа пользователя.

   b. В открывшемся окне выберите способ добавления пользователей **Добавить пользователя / группу вручную**.

   c. Задайте имя пользователя и пароль.

   d. В списке **Разрешения** настройте права доступа пользователей к функциям приложениям.

9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как защитить доступ к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Права пользователей на управление приложением**.
2. В открывшемся окне установите флажок **Разрешать подтверждение операций с приложением вводом учетных данных вручную созданных пользователей**.
3. Если требуется, снимите флажок **Запрашивать пароль для подтверждения критических действий**.

Если функция включена, приложение будет запрашивать имя и пароль пользователя при удалении/изменении/восстановлении приложения и при выполнении действий в командной строке, которые могут привести к снижению уровня защиты устройства.

Если эта функция выключена, и текущий пользователь обладает необходимыми правами, Kaspersky Industrial CyberSecurity for Nodes не будет запрашивать учетные данные. По умолчанию функция включена.

> Если для учетной записи текущего пользователя установлен пустой пароль Windows, вам необходимо ввести учетные данные пользователя с необходимыми правами, для которого задан пароль.

4. Задайте пароль для учетной записи KLAdmin.

5. Если требуется, добавьте учетные записи, которым вы хотите предоставить доступ на управление приложением:

   a. Нажмите на кнопку **Добавить**.

      Откроется форма для настройки прав доступа пользователя.

   b. В открывшемся окне выберите способ добавления пользователей **Добавить пользователя / группу вручную**.

   c. Задайте имя пользователя и пароль.

   d. В списке **Разрешения** настройте права доступа пользователей к функциям приложениям.

6. Сохраните внесенные изменения.

Как защитить доступ к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Дополнительные возможности → Права пользователей на управление приложением** и нажмите на кнопку **Настроить**.

5. В открывшемся окне установите флажок **Разрешать подтверждение операций с приложением вводом учетных данных вручную созданных пользователей**.

6. Если требуется, снимите флажок **Запрашивать пароль для подтверждения критических действий**.

   Если функция включена, приложение будет запрашивать имя и пароль пользователя при удалении/изменении/восстановлении приложения и при выполнении действий в командной строке, которые могут привести к снижению уровня защиты устройства.

   Если эта функция выключена, и текущий пользователь обладает необходимыми правами, Kaspersky Industrial CyberSecurity for Nodes не будет запрашивать учетные данные. По умолчанию функция включена.

Если для учетной записи текущего пользователя установлен пустой пароль Windows, вам необходимо ввести учетные данные пользователя с необходимыми правами, для которого задан пароль.

7. Задайте пароль для учетной записи KLAdmin.
8. Если требуется, добавьте учетные записи, которым вы хотите предоставить доступ на управление приложением:
   a. Нажмите на кнопку **Добавить**.

      Откроется форма для настройки прав доступа пользователя.

   b. В открывшемся окне выберите способ добавления пользователей **Добавить пользователя / группу вручную**.

   c. Задайте имя пользователя и пароль.

   d. В списке **Разрешения** настройте права доступа пользователей к функциям приложениям.
9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Установленный пароль невозможно восстановить. Утеря пароля ведет к полной потере контроля над приложением. Кроме того, невозможно будет удалить приложение с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Разрешать подтверждение операций с приложением вводом учетных данных вручную созданных пользователей** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

Уведомления Безопасного рабочего стола

Kaspersky Industrial CyberSecurity for Nodes поддерживает функцию *Безопасного рабочего стола* (англ. Secure Desktop). Эта функция предназначена для подтверждения действий, которые могут снизить безопасность компьютера. Функция позволяет приложению показывать диалоговое окно подтверждения, изолированное от других процессов. Функция обеспечивает безопасность запроса за счет повышенных прав. Таким образом, подтвердить действие может только пользователь, а не вредоносное ПО.

Kaspersky Industrial CyberSecurity for Nodes показывает уведомления Безопасного рабочего стола для подтверждения следующих действий:

- включение и выключение записи трассировок;
- экспорт и импорт настроек приложения;
- приостановка защиты;
- завершение работы приложения;
- удаление активного ключа;
- удаление Kaspersky Industrial CyberSecurity for Nodes;

- выключение Контроля устройств;
- выключение Постоянной защиты файлов;
- выключение политики Kaspersky Security Center;
- просмотр отчетов;
- восстановление файлов из резервного хранилища;
- изменение параметров Kaspersky Industrial CyberSecurity for Nodes;
- управление задачами приложения, кроме запуска задач.

Как включить или выключить уведомления Безопасного рабочего стола в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Параметры приложения**.
4. В блоке **Безопасность и надежность** нажмите на кнопку **Настройка**.
5. В открывшемся окне выберите вкладку **Безопасность**.
6. В блоке **Самозащита** используйте флажок **Включить уведомления Безопасного рабочего стола**, чтобы включить или выключить уведомления Безопасного рабочего стола.

   Если механизмы самозащиты выключены, флажок **Включить уведомления Безопасного рабочего стола** недоступен.

7. Закройте замок для применения политики на компьютерах.
8. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как включить или выключить уведомления Безопасного рабочего стола в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в панели результатов перейдите по ссылке **Свойства приложения**.
2. В открывшемся окне выберите вкладку **Настройки безопасности**.
3. В блоке **Самозащита** используйте флажок **Включить уведомления Безопасного рабочего стола**, чтобы включить или выключить уведомления Безопасного рабочего стола.

   Если механизмы самозащиты выключены, флажок **Включить уведомления Безопасного рабочего стола** недоступен.

4. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как включить или выключить уведомления Безопасного рабочего стола в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Настройки приложения**.
5. В блоке **Безопасность и надежность** нажмите на кнопку **Настроить**.

   Откроется окно **Безопасность и надежность**.
6. В блоке **Самозащита** используйте флажок **Включить уведомления Безопасного рабочего стола**, чтобы включить или выключить уведомления Безопасного рабочего стола.

   Если механизмы самозащиты выключены, флажок **Включить уведомления Безопасного рабочего стола** недоступен.
7. Закройте замок для применения политики на компьютерах.
8. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые Kaspersky Industrial CyberSecurity for Nodes не контролирует в процессе работы.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от приложений, установленных на компьютере. Включение объектов и приложений в доверенную зону может потребоваться, например, если Kaspersky Industrial CyberSecurity for Nodes блокирует доступ к какому-либо объекту или приложению, в то время как вы уверены, что этот объект или приложение безвредны. Также администратор может разрешить пользователю формировать собственную локальную доверенную зону для отдельного компьютера. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений и доверенных приложений.

Также вы можете добавить EDR-телеметрию в доверенную зону. Это позволяет оптимизировать данные, которые приложение отправляет на Сервер сбора телеметрии для решения Kaspersky Anti Targeted Attack Platform (EDR).

В доверенную зону добавлены предустановленные исключения из проверки и доверенные приложения. Предустановленные исключения из проверки и доверенные приложения предназначены для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes без необходимости формирования доверенной зоны вручную.

Создание исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Industrial CyberSecurity for Nodes не проверяет объект на вирусы и другие приложения, представляющие угрозу.

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач приложения:

- **Постоянная защита файлов**;
- **Проверка по требованию**;
- **Защита от шифрования**;
- **AMSI-защита**;
- **Защита от сетевых угроз**.

Kaspersky Industrial CyberSecurity for Nodes не проверяет объект, если при запуске одной из задач проверки в область проверки включен диск, на котором находится объект, или папка, в которой находится объект. Однако при запуске задачи выборочной проверки именно для этого объекта исключение из проверки не применяется.

Kaspersky Industrial CyberSecurity for Nodes не поддерживает работу со списком исключений, содержащим более 5000 объектов.

Как создать исключение из проверки в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Дополнительные возможности → Доверенная зона** и нажмите на кнопку **Настройка**.

4. Перейдите на закладку **Исключения из проверки**.

5. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список исключений для всех компьютеров организации. Списки исключений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Исключения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление исключений родительской политики невозможно.

6. Установите флажок **Разрешить использование локальных исключений**, если вы хотите чтобы у пользователя была возможность создать локальный список исключений. Таким образом, кроме общего списка исключений, сформированного в политике, пользователь может создавать собственный локальный список исключений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список исключений, сформированный в политике. Также, если флажок снят, Kaspersky Industrial CyberSecurity for Nodes скрывает для просмотра общий список исключений из проверки в Консоли приложения.

7. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.

   - **Новое исключение**. Kaspersky Industrial CyberSecurity for Nodes добавляет новое исключение из проверки в корень списка.

   - **Новое исключение в выбранную категорию**. Для добавления нового исключения из проверки в отдельную категорию выберите категорию.

   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes вы можете добавить исключения из списка предустановленных исключений из проверки.

8. Если вы хотите исключить из проверки файл или папку, установите флажок **Файл или папка**. Нажмите на ссылку **выберите файл или папку**, и в открывшемся окне выберите файл или папку нажав на кнопку **Обзор**.

Также вы можете ввести путь вручную. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

  Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

9. Если вы хотите исключить из проверки предопределенную область, установите флажок **Предопределенная область**. Нажмите на ссылку **выберите предопределенную область** и в открывшемся окне укажите одну из стандартных областей на защищаемом устройстве.

10. Если вы хотите исключить из проверки определенные объекты, установите флажок **Тип обнаруживаемого объекта**. Нажмите на ссылку **введите названия объектов**, нажмите на кнопку **Добавить** и в открывшемся окне введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

    Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Industrial CyberSecurity for Nodes исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

11. Если вы хотите исключить из проверки отдельный файл, установите флажок **Хеш объекта**. Нажмите на ссылку **введите хеш объекта** и в открывшемся окне укажите хеш файла.

    Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

12. В блоке **Область применения правил** выберите компоненты, на работу которых должно распространяться исключение из проверки.

13. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

14. Сохраните изменения, чтобы добавить исключение в список. Вы можете в любое время остановить работу исключения с помощью флажка напротив объекта.

Как создать исключение из проверки в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Дополнительные возможности → Доверенная зона** и нажмите на кнопку **Настроить**.

5. Перейдите на закладку **Исключения из проверки**.

6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список исключений для всех компьютеров организации. Списки исключений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Исключения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление исключений родительской политики невозможно.

7. Установите флажок **Разрешить использование локальных исключений**, если вы хотите чтобы у пользователя была возможность создать локальный список исключений. Таким образом, кроме общего списка исключений, сформированного в политике, пользователь может создавать собственный локальный список исключений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список исключений, сформированный в политике. Также, если флажок снят, Kaspersky Industrial CyberSecurity for Nodes скрывает для просмотра общий список исключений из проверки в Консоли приложения.

8. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.

   - **Новое исключение**. Kaspersky Industrial CyberSecurity for Nodes добавляет новое исключение из проверки в корень списка.

   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes вы можете добавить исключения из списка предустановленных исключений из проверки.

9. Если вы хотите исключить из проверки файл или папку, выберите вариант **Файл или папка** и установите флажок в одноименном поле. Укажите путь к файлу или папке.

   Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски:

   - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

   - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

   - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

     Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

10. Если вы хотите исключить из проверки предопределенную область, выберите вариант **Предопределенные области**. В раскрывающемся списке укажите одну из стандартных областей на защищаемом устройстве.

11. Если вы хотите исключить из проверки определенные объекты, установите флажок **Тип обнаруживаемого объекта** и введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

    Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Industrial CyberSecurity for Nodes исключает из проверки объекты типов *Client-IRC*, *Client-P2P* и *Client-SMTP*.

12. Если вы хотите исключить из проверки отдельный файл, установите флажок **Хеш объекта** и добавьте хеш из файла или из списка событий.

    Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

13. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

14. В блоке **Компоненты защиты** выберите компоненты, на работу которых должно распространяться исключение из проверки.

15. Новое исключение будет добавлено в список. Вы можете в любое время остановить работу исключения с помощью флажка в графе **Статус**.

16. Сохраните внесенные изменения.

Как создать исключение из проверки в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Доверенная зона**.

   Откроется окно **Настроить доверенную зону**.

2. В секции **Исключения** нажмите на кнопку **Настройка** напротив блока **Исключения из проверки**.

3. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.
   - **Новое исключение**. Kaspersky Industrial CyberSecurity for Nodes добавляет новое исключение из проверки в корень списка.
   - **Новое исключение в выбранную категорию**. Для добавления нового исключения из проверки в отдельную категорию выберите категорию.
   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes вы можете добавить исключения из списка предустановленных исключений из проверки.

4. Если вы хотите исключить из проверки файл или папку, установите флажок **Файл или папка**. Нажмите на ссылку **Выберите файл или папку**, и в открывшемся окне выберите файл или папку нажав на кнопку **Обзор**.

Также вы можете ввести путь вручную. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

  Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

5. Если вы хотите исключить из проверки предопределенную область, установите флажок **Предопределенная область**. Нажмите на ссылку **выберите предопределенную область** и в открывшемся окне укажите одну из стандартных областей на защищаемом устройстве.

6. Если вы хотите исключить из проверки определенные объекты, установите флажок **Тип обнаруживаемого объекта**. Нажмите на ссылку **введите названия объектов**, нажмите на кнопку **Добавить** и в открывшемся окне введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

   Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Industrial CyberSecurity for Nodes исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

7. Если вы хотите исключить из проверки отдельный файл, установите флажок **Хеш объекта**. Нажмите на ссылку **введите хеш объекта** и в открывшемся окне укажите хеш файла.

   Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

8. В блоке **Область применения правил** выберите компоненты, на работу которых должно распространяться исключение из проверки.

9. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

10. Сохраните изменения, чтобы добавить исключение в список. Вы можете в любое время остановить работу исключения с помощью флажка напротив объекта.

Примеры масок пути:
Пути к файлам, расположенным в любой из папок:

- Маска `*.exe` будет включать все пути к файлам с расширением exe.
- Маска `example*` будет включать все пути к файлам с именем EXAMPLE.

Пути к файлам, расположенным в указанной папке:

- маска `C:\dir\*.*` будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
- маска `C:\dir\*` будет включать все пути к файлам в папке C:\dir\, включая подпапки;
- маска `C:\dir\` будет включать все пути к файлам в папке C:\dir\, включая подпапки;
- маска `C:\dir\*.exe` будет включать все пути к файлам с расширением .EXE в папке C:\dir\, но не в подпапках папки C:\dir\;
- маска `C:\dir\test` будет включать все пути к файлам с именем test в папке C:\dir\, но не в подпапках папки C:\dir\;
- маска `C:\dir\*\test` будет включать все пути к файлам с именем test в папке C:\dir\ и в подпапках папки C:\dir\;
- маска `C:\dir1\*\dir3\` будет включать все пути к файлам в подпапках dir3 в папке C:\dir1\ через один уровень;
- маска `C:\dir1\**\dirN\` будет включать все пути к файлам в подпапках dirN в папке C:\dir1\ на любом уровне.

Пути к файлам, расположенным во всех папках с указанным именем:

- маска `dir\*.*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*.exe` будет включать все пути к файлам с расширением .EXE в папках с именем dir, но не в подпапках этих папок;
- маска `dir\test` будет включать все пути к файлам с именем test в папках с именем dir, но не в подпапках этих папок.

Выбор типов обнаруживаемых объектов

Чтобы выбрать типы обнаруживаемых объектов:

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:

   - В панели результатов узла перейдите по ссылке **Настроить доверенную зону**.
   - В контекстном меню узла выберите пункт **Доверенная зона**.

   Откроется окно **Настроить доверенную зону**.

2. В разделе **Типы обнаруживаемых объектов** нажмите на кнопку **Настройка**.

3. В открывшемся окне установите флажки для типов объектов, которые должен обнаруживать Kaspersky Industrial CyberSecurity for Nodes:

   - **Вирусы и черви**

     Подкатегория: вирусы и черви (Viruses_and_Worms)

     Уровень опасности: высокий

Классические вирусы и черви выполняют на компьютере действия, не разрешенные пользователем. Они могут создавать свои копии, которые обладают способностью дальнейшего самовоспроизведения.

Классический вирус

Попав в систему, классический вирус заражает какой-либо файл, активизируется в нем, выполняет свое вредоносное действие, а затем добавляет свои копии в другие файлы.

Классический вирус размножается только на локальных ресурсах компьютера и не может самостоятельно проникать на другие компьютеры. Он может попасть на другой компьютер только в том случае, если добавит свою копию в файл, который хранится в папке общего доступа или на установленном компакт-диске, или если пользователь сам перешлет сообщение электронной почты с вложенным в него зараженным файлом.

Код классического вируса может внедряться в различные области компьютера, операционной системы или приложения. В зависимости от среды обитания вирусы подразделяют на *файловые*, *загрузочные*, *скриптовые* и *макро-вирусы*.

Вирусы могут заражать файлы различными способами. *Перезаписывающие* (Overwriting) вирусы записывают свой код вместо кода заражаемого файла, уничтожая его содержимое. Зараженный файл перестает работать, и его нельзя восстановить. *Паразитические* (Parasitic) вирусы изменяют файлы, оставляя их полностью или частично работоспособными. *Вирусы-компаньоны* (Companion) не изменяют файлы, но создают их двойники. При открытии зараженного файла запускается его двойник, то есть вирус. Среди вирусов встречаются также *вирусы-ссылки* (Link), вирусы, *заражающие объектные модули* (OBJ), вирусы, *заражающие библиотеки компиляторов* (LIB), вирусы, *заражающие исходные тексты программ*, и другие.

Червь

Код червя, как и код классического вируса, попав в систему, активизируется и выполняет свое вредоносное действие. Свое название червь получил благодаря способности "переползать" с компьютера на компьютер – без разрешения пользователя распространять свои копии через различные информационные каналы.

Основной признак, по которому черви различаются между собой, – способ их распространения. Описание типов червей по способу распространения приводится в следующей таблице.

Способы распространения червей

Тип	Название	Описание
Email-Worm	Почтовые черви	Распространяются через электронную почту. Зараженное сообщение электронной почты содержит прикрепленный файл с копией червя или ссылку на такой файл на веб-сайте, например, взломанном или специально созданном. Когда вы запускаете прикрепленный файл, червь активизируется; когда вы щелкаете на ссылке, загружаете, а затем открываете файл, червь также начинает выполнять свое вредоносное действие. После этого он продолжает распространять свои копии, разыскивая другие адреса электронной почты и отправляя по ним зараженные сообщения.
IM-Worm	Черви IM-клиентов	Распространяются через IM-клиенты. Обычно такой червь рассылает по контакт-листам сообщения, содержащие ссылку на файл с его копией на веб-сайте. Когда пользователь загружает файл и открывает его, червь активизируется.
IRC-Worm	Черви интернет-чатов	Распространяются через ретранслируемые интернет-чаты (Internet Relay Chats) – сервисные системы, с помощью которых можно общаться через интернет с другими людьми в реальном времени. Такой червь публикует в интернет-чате файл со своей копией или ссылку на файл. Когда пользователь загружает файл и открывает его, червь активизируется.

Тип	Название	Описание
Net-Worm	Сетевые черви (черви компьютерных сетей)	Распространяются через компьютерные сети. В отличие от червей других типов, сетевой червь распространяется без участия пользователя. Он ищет в локальной сети компьютеры, на которых используются программы, содержащие уязвимости. Для этого он посылает специально сформированный сетевой пакет (эксплойт), который содержит код червя или его часть. Если в сети находится "уязвимый" компьютер, он принимает такой сетевой пакет. Полностью проникнув на компьютер, червь активизируется.
P2P-Worm	Черви файлообменных сетей	Распространяются через файлообменные пиринговые сети. Чтобы внедриться в файлообменную сеть, червь копирует себя в каталог обмена файлами, обычно расположенный на компьютере пользователя. Файлообменная сеть отображает информацию об этом файле, и пользователь может "найти" зараженный файл в сети так же, как и любой другой, загрузить его и открыть. Более сложные черви имитируют сетевой протокол конкретной файлообменной сети: они положительно отвечают на поисковые запросы и предлагают для загрузки свои копии.
Worm	Прочие черви	К прочим сетевым червям относятся: • Черви, которые распространяют свои копии через сетевые ресурсы. Используя функции операционной системы, они перебирают доступные сетевые папки, подключаются к компьютерам в глобальной сети и пытаются открыть их диски на полный доступ. В отличие от описанных выше разновидностей червей, прочие черви активизируются не самостоятельно, а как только пользователь открывает файл с копией червя. • Черви, которые не относятся ни к одному из описанных в этой таблице способов распространения (например, те, которые распространяются через мобильные телефоны).

- **Троянские приложения**

  Подкатегория: троянские программы (Trojan_programs)

  Уровень опасности: высокий

  В отличие от червей и вирусов, троянские программы не создают свои копии. Они проникают на компьютер, например, через электронную почту или через браузер, когда пользователь посещает зараженную веб-страницу. Троянские программы запускаются при участии пользователя. Они начинают выполнять свое вредоносное действие сразу после запуска.

  Разные троянские программы ведут себя на зараженном компьютере по-разному. Основные функции троянских программ – блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Кроме этого, троянские программы могут принимать или отправлять файлы, выполнять их, выводить на экран сообщения, обращаться к веб-страницам, загружать и устанавливать программы, перезагружать компьютер.

  Злоумышленники часто используют "наборы" из разных троянских программ.

  Типы поведения троянских программ описаны в следующей таблице.

  Типы поведения троянских программ на зараженном компьютере

Тип	Название	Описание
Trojan-ArcBomb	Троянские программы – "архивные бомбы"	Архивы; при распаковке увеличиваются до таких размеров, что нарушают работу компьютера. Когда пользователь пытается распаковать такой архив, компьютер может начать работать медленно или "зависнуть", диск может заполниться "пустыми" данными. "Архивные бомбы" особенно опасны для файловых и почтовых серверов. Если на сервере используется система автоматической обработки входящей информации, такая "архивная бомба" может остановить сервер.
Backdoor	Троянские программы удаленного администрирования	Считаются наиболее опасными среди троянских программ. По своим функциям напоминают устанавливаемые на компьютеры программы удаленного администрирования. Эти программы устанавливают себя в компьютере незаметно для пользователя и позволяют злоумышленнику удаленно управлять компьютером.

Тип	Название	Описание
Trojan	Троянские программы	Включают следующие вредоносные программы: • **Классические троянские программы**. Эти программы выполняют только основные функции троянских программ: блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Они не имеют дополнительных функций, свойственных другим типам троянских программ, описанным в этой таблице. • **"Многоцелевые" троянские программы**. Эти программы имеют дополнительные функции, присущие сразу нескольким типам троянских программ.
Trojan-Ransom	Троянские программы, требующие выкупа	"Берут в заложники" информацию на компьютере пользователя, изменяя или блокируя ее, или нарушают работу компьютера таким образом, чтобы пользователь не мог воспользоваться информацией. Злоумышленник требует от пользователя выкуп за обещание выслать программу, которая восстановит работоспособность компьютера и данные на нем.
Trojan-Clicker	Троянские программы-кликеры	С компьютера пользователя обращаются к веб-страницам: они или сами посылают команды браузеру, или заменяют хранящиеся в системных файлах веб-адреса. С помощью этих программ злоумышленники организовывают сетевые атаки, повышают посещаемость сайтов, чтобы увеличить количество показов рекламных баннеров.
Trojan-Downloader	Троянские программы-загрузчики	Обращаются к веб-странице злоумышленника, загружают с нее другие вредоносные программы и устанавливают их на компьютере пользователя; могут хранить имя файла загружаемой вредоносной программы в себе или получать его с веб-страницы, к которой обращаются.
Trojan-Dropper	Троянские программы-установщики	Сохраняют на диске компьютера, а затем устанавливают другие троянские программы, которые хранятся в теле этих программ. Злоумышленники могут использовать троянские программы-установщики, чтобы достичь следующих целей: • установить вредоносную программу незаметно для пользователя: троянские программы-установщики не отображают никаких сообщений или выводят на экран ложные сообщения, например, об ошибке в архиве или неверной версии операционной системы; • защитить от обнаружения другую известную вредоносную программу: не все антивирусы могут распознать вредоносную программу внутри троянской программы-установщика.
Trojan-Notifier	Троянские программы-уведомители	Сообщают злоумышленнику о том, что зараженный компьютер находится "на связи"; передают ему информацию о компьютере: IP-адрес, номер открытого порта или адрес электронной почты. Они связываются со злоумышленником по электронной почте, через FTP, обращаясь к его веб-странице или другим способом. Троянские программы-уведомители часто используются в наборах из разных троянских программ. Они извещают злоумышленника о том, что другие троянские программы успешно установлены на компьютере пользователя.
Trojan-Proxy	Троянские программы-прокси	Позволяют злоумышленнику анонимно обращаться через компьютер пользователя к веб-страницам; часто используются для рассылки спама.
Trojan-PSW	Троянские программы, крадущие пароли	Троянские программы, крадущие пароли (Password Stealing Ware); крадут учетные записи пользователей, например, регистрационную информацию к программному обеспечению. Они отыскивают конфиденциальные данные в системных файлах и реестре и пересылают ее "хозяину" по электронной почте, через FTP, обращаясь к веб-странице злоумышленника или другим способом. Некоторые из этих троянских программ выделены в отдельные типы, описанные в этой таблице. Это троянские программы, крадущие банковские счета (Trojan-Banker), троянские программы, крадущие данные пользователей IM-клиентов (Trojan-IM) и троянские программы, крадущие данные пользователей сетевых игр (Trojan-GameThief).
Trojan-Spy	Троянские программы-шпионы	Ведут электронный шпионаж за пользователем: собирают информацию о его действиях на компьютере, например, перехватывают данные, которые пользователь вводит с клавиатуры, делают снимки экрана или собирают списки активных приложений. Получив эту информацию, они передают ее злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.

Тип	Название	Описание
Trojan-DDoS	Троянские программы – сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании). Такими программами часто заражают многие компьютеры, чтобы с них одновременно атаковать один сервер. DoS-программы реализуют атаку с одного компьютера с ведома пользователя. DDoS-программы (Distributed DoS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера.
Trojan-IM	Троянские программы, крадущие данные пользователей IM-клиентов	Крадут номера и пароли пользователей IM-клиентов. Передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Rootkit	Руткиты	Скрывают другие вредоносные программы и их активность и таким образом продлевают пребывание этих программ в системе; могут скрывать файлы, процессы в памяти зараженного компьютера или ключи реестра, которые запускают вредоносные программы; могут скрывать обмен данными между приложениями на компьютере пользователя и других компьютерах в сети.
Trojan-SMS	Троянские программы – SMS-сообщения	Заражают мобильные телефоны и с них отправляют SMS-сообщения на платные номера.
Trojan-GameThief	Троянские программы, крадущие данные пользователей сетевых игр	Крадут учетные данные пользователей сетевых компьютерных игр; передают их злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-Banker	Троянские программы, крадущие банковские счета	Крадут данные банковских счетов или счетов в системах электронных денег; передают данные злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом.
Trojan-Mailfinder	Троянские программы – сборщики адресов электронной почты	Собирают адреса электронной почты на компьютере и передают их злоумышленнику по электронной почте, через FTP, обращаясь к его веб-странице или другим способом. По собранным адресам злоумышленники могут рассылать спам.

- **Вредоносные утилиты**

  Подкатегория: вредоносные утилиты (Malicious_tools)

  Уровень опасности: средний

  Вредоносные утилиты, в отличие от других вредоносных программ, не выполняют своих действий сразу при запуске и могут безопасно храниться и запускаться на компьютере пользователя. Злоумышленники используют функции этих программ для создания вирусов, червей и троянских программ, организации сетевых атак на удаленные серверы, "взлома" компьютеров или других вредоносных действий.

  Разнообразные функции вредоносных утилит делятся на типы, которые описаны в следующей таблице.

  Функции вредоносных утилит

Тип	Название	Описание
Constructor	Конструкторы	Позволяют создавать новые вирусы, черви и троянские программы. Некоторые конструкторы имеют стандартный оконный интерфейс, в котором с помощью меню можно выбирать тип создаваемой вредоносной программы, способ ее противодействия отладчику и другие свойства.
Dos	Сетевые атаки	Отправляют с компьютера пользователя многочисленные запросы на удаленный сервер. У сервера не хватает ресурсов для обработки запросов, и он перестает работать (Denial-of-Service (DoS) – отказ в обслуживании).

Тип	Название	Описание
Exploit	Эксплойты	*Эксплойт* – это набор данных или программный код, использующий уязвимости приложения, в котором он обрабатывается, чтобы выполнить на компьютере вредоносное действие. Например, эксплойт может записывать или считывать файлы либо обращаться к "зараженным" веб-страницам. Разные эксплойты используют уязвимости разных приложений или сетевых служб. Эксплойт в виде сетевого пакета передается по сети на многие компьютеры, выискивая компьютеры с уязвимыми сетевыми службами. Эксплойт в файле DOC использует уязвимости текстового редактора. Он может начать выполнять заложенные в него злоумышленником функции, когда пользователь откроет зараженный файл. Эксплойт, внедренный в сообщение электронной почты, ищет уязвимости в каком-либо почтовом клиенте. Он может начать выполнять вредоносное действие, как только пользователь откроет зараженное сообщение в этом почтовом клиенте. С помощью эксплойтов распространяются сетевые черви (Net-Worm). Эксплойты-ньюкеры (Nuker) представляют собой сетевые пакеты, которые выводят компьютеры из строя.
FileCryptor	Шифровальщики	Шифруют другие вредоносные программы, чтобы скрыть их от антивирусного приложения.
Flooder	Программы для "замусоривания" сетей	Рассылают многочисленные сообщения по сетевым каналам. К этому типу относятся, например, программы для замусоривания ретранслируемых интернет-чатов (Internet Relay Chats). К типу Flooder не относятся программы, "забивающие мусором" каналы электронной почты, IM-клиентов и мобильных систем. Эти программы выделяют в отдельные типы, описанные в этой таблице (Email-Flooder, IM-Flooder и SMS-Flooder).
HackTool	Инструменты хакера	Позволяют взламывать компьютер, на котором они установлены, или атаковать другой компьютер (например, без разрешения пользователя добавлять других пользователей системы; очищать системные журналы, чтобы скрыть следы присутствия в системе). К этому типу относят некоторые снифферы, которые обладают вредоносными функциями, например перехватывают пароли. Снифферы (Sniffers) – это программы, которые позволяют просматривать сетевой трафик.
Hoax	Злые шутки	Пугают пользователя вирусоподобными сообщениями: могут "обнаружить" вирус в незараженном файле или объявить о форматировании диска, которого на самом деле не происходит.
Spoofer	Утилиты-имитаторы	Отправляют сообщения и сетевые запросы с поддельным адресом отправителя. Злоумышленники используют утилиты-имитаторы, чтобы, например, выдать себя за отправителя.
VirTool	Инструменты для модификации вредоносных программ	Позволяют модифицировать другие вредоносные программы так, чтобы скрыть их от антивирусных приложений.
Email-Flooder	Программы для "замусоривания" адресов электронной почты	Отправляют многочисленные сообщения по адресам электронной почты ("забивают их мусором"). Большой поток сообщений не дает пользователям просматривать полезную входящую почту.
IM-Flooder	Программы для "замусоривания" IM-клиентов	Отправляют многочисленные сообщения пользователям IM-клиентов. Большой поток сообщений не дает пользователям просматривать полезные входящие сообщения.
SMS-Flooder	Программы для "замусоривания" SMS-сообщениями	Отправляют многочисленные SMS-сообщения на мобильные телефоны.

- **Рекламные приложения**

  Подкатегория: рекламные программы (Adware)

  Уровень опасности: средний

  Рекламные программы связаны с показом пользователю рекламной информации. Они отображают в интерфейсе других программ рекламные баннеры, перенаправляют поисковые запросы на рекламные веб-страницы. Некоторые из них собирают и переправляют своему разработчику маркетинговую информацию о пользователе: например, сведения о том, какие тематические веб-сайты он посещает, какие поисковые запросы делает. В отличие от троянских программ-шпионов, рекламные программы передают эту информацию разработчику с разрешения пользователя.

- **Приложения автодозвона**

  Подкатегория: Приложения автодозвона (Dialer).

  Уровень опасности: средний

  Приложения автодозвона могут устанавливать телефонные соединения через модем в скрытом режиме.

- **Легальные приложения, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**

  Подкатегория: легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

  Уровень опасности: средний

  Большинство этих программ являются полезными, и многие пользователи применяют их. Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

  Однако если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые их функции для нарушения безопасности.

  Подобные программы различают по функциям, типы которых описаны в таблице ниже.

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на компьютере, на котором установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники.
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры пользователей для наблюдения за удаленными компьютерами и управления ими. Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на локальном компьютере	Дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).

Тип	Название	Описание
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

- **Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода**

  Подкатегория: Упакованные файлы, которые могут нанести вред.

  Уровень опасности: средний.

  Файл упакован специальным упаковщиком, который используется для упаковки вредоносных программ: вирусов, червей, троянских программ. Kaspersky Industrial CyberSecurity for Nodes проверяет модуль-распаковщик в составе самораспаковывающихся архивов SFX (self-extracting archive).

  Чтобы скрыть вредоносные программы от обнаружения антивирусом, злоумышленники упаковывают их с помощью специальных упаковщиков. Специалисты "Лаборатории Касперского" выделили упаковщики, которые злоумышленники используют чаще всего.

- **Многократно упакованные объекты**

  Подкатегория: Многократно упакованные файлы.

  Уровень опасности: средний.

  Файл упакован одним или несколькими упаковщиками три или более раз.

  Чтобы скрыть вредоносные программы от обнаружения антивирусом, злоумышленники многократно упаковывают один файл. Kaspersky Industrial CyberSecurity for Nodes проверяет упакованные файлы.

4. Сохраните внесенные изменения.

Формирование списка доверенных приложений

Список доверенных приложений – это список приложений, у которых Kaspersky Industrial CyberSecurity for Nodes не контролирует файловую и сетевую активности (в том числе и вредоносную), а также обращения этих приложений к системному реестру. По умолчанию Kaspersky Industrial CyberSecurity for Nodes контролирует объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех приложений и создаваемый ими сетевой трафик. После добавления приложения в список доверенных приложений Kaspersky Industrial CyberSecurity for Nodes перестает контролировать активность приложения.

Отличие исключений из проверки от доверенных приложений заключается в том, что для исключений Kaspersky Industrial CyberSecurity for Nodes не проверяет файлы, а для доверенных приложений инициируемые процессы. То есть, если доверенное приложение создаст вредоносный файл в папке, которая не включена в исключения, Kaspersky Industrial CyberSecurity for Nodes обнаружит этот файл и устранит угрозу. Если папка добавлена в исключения, Kaspersky Industrial CyberSecurity for Nodes пропустит этот файл.

Например, если вы считаете объекты, используемые приложением Microsoft Windows Блокнот, безопасными, то есть доверяете этому приложению, вам следует добавить приложение Microsoft Windows Блокнот в список доверенных приложений, чтобы не контролировать объекты, используемые этим приложением. Это позволит увеличить производительность компьютера, что особенно важно при использовании серверных приложений.

Кроме того, некоторые действия, которые Kaspersky Industrial CyberSecurity for Nodes классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда приложений. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием приложения автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких приложений и отключить контроль их активности, рекомендуется добавить их в список доверенных приложений.

Доверенные приложения позволяют избежать проблемы совместимости Kaspersky Industrial CyberSecurity for Nodes с другими приложениями (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Industrial CyberSecurity for Nodes и другого антивирусного приложения).

В то же время исполняемый файл и процесс доверенного приложения по-прежнему проверяются на наличие в них вирусов и других приложений, представляющих угрозу. Для полного исключения приложения из проверки Kaspersky Industrial CyberSecurity for Nodes следует пользоваться исключениями из проверки.

Kaspersky Industrial CyberSecurity for Nodes не поддерживает работу со списком доверенных приложений, содержащим более 5000 объектов.

Как добавить приложение в список доверенных в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Дополнительные возможности**.
4. В блоке **Доверенная зона** нажмите на кнопку **Настройка**.
5. В открывшемся окне выберите закладку **Доверенные приложения**.

   Откроется окно со списком доверенных приложений.
6. Установите флажок **Не проверять файловые операции резервного копирования**, если вы хотите пропустить проверку операций чтения файлов, которые выполняются средствами резервного копирования, установленными на защищаемом устройстве.
7. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных приложений для всех компьютеров организации. Списки доверенных приложений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные приложения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных приложений родительской политики невозможно

8. Установите флажок **Разрешать редактирование локальных доверенных приложений**, если вы хотите чтобы у пользователя была возможность создать локальный список доверенных приложений. Таким образом, кроме общего списка доверенных приложений, сформированного в политике, пользователь может создавать собственный локальный список доверенных приложений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список доверенных приложений, сформированный в политике. Также, если флажок снят, Kaspersky Industrial CyberSecurity for Nodes скрывает для просмотра общий список доверенных приложений в Консоли приложения.

9. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

10. Нажмите на кнопку **Добавить** и выберите нужное действие:

    - **Категорию**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.
    - **Новое исключение**. Kaspersky Industrial CyberSecurity for Nodes добавляет новое доверенное приложение в корень списка.
    - **Новое исключение в выбранную категорию**. Для добавления нового доверенного приложения в отдельную категорию выберите категорию.
    - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes вы можете добавить приложения из списка предустановленных доверенных приложений.

11. В открывшемся окне установите флажок **Использовать полный путь для определения доверенности процессов** и введите путь к файлу для определения, является ли процесс доверенным.

    Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски.

    > Kaspersky Industrial CyberSecurity for Nodes не поддерживает переменную среды `%userprofile%` при формировании списка доверенных приложений через консоль Kaspersky Security Center. Чтобы применить запись ко всем учетным записям, вы можете использовать символ * (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.

12. Настройте дополнительные параметры доверенного приложения (см. таблицу ниже).

13. Нажмите на кнопку **OK**.

    Новое доверенное приложение будет добавлено в список. Вы можете в любое время исключить приложение из доверенной зоны с помощью флажка напротив объекта.

14. Сохраните внесенные изменения.

Как добавить приложение в список доверенных в Web Console

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

4. Выберите закладку **Параметры приложения**.

5. Перейдите в раздел **Дополнительные возможности → Доверенная зона** и нажмите на кнопку **Настроить**.

6. В открывшемся окне перейдите на закладку **Доверенные приложения**.

7. Установите флажок **Не проверять файловые операции резервного копирования**, если вы хотите пропустить проверку операций чтения файлов, которые выполняются средствами резервного копирования, установленными на защищаемом устройстве.

8. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных приложений для всех компьютеров организации. Списки доверенных приложений родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные приложения родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных приложений родительской политики невозможно

9. Установите флажок **Разрешать редактирование локальных доверенных приложений**, если вы хотите чтобы у пользователя была возможность создать локальный список доверенных приложений. Таким образом, кроме общего списка доверенных приложений, сформированного в политике, пользователь может создавать собственный локальный список доверенных приложений. Администратор с помощью Kaspersky Security Center может просматривать, добавлять, изменять или удалять элементы списка в свойствах компьютера.

   Если флажок снят, пользователю доступен только общий список доверенных приложений, сформированный в политике. Также, если флажок снят, Kaspersky Industrial CyberSecurity for Nodes скрывает для просмотра общий список доверенных приложений в Консоли приложения.

10. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

11. Нажмите на кнопку **Добавить** и выберите нужное действие:

    - **Категорию**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.

    - **Новое исключение**. Kaspersky Industrial CyberSecurity for Nodes добавляет новое доверенное приложение в корень списка.

    - **Новое исключение в выбранную категорию**. Для добавления нового доверенного приложения в отдельную категорию, выберите категорию.

    - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes вы можете добавить приложения из списка предустановленных доверенных приложений.

12. В открывшемся окне установите флажок **Использовать полный путь для определения доверенности процессов** и введите путь к файлу для определения, является ли процесс доверенным.

    Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски.

Kaspersky Industrial CyberSecurity for Nodes не поддерживает переменную среды `%userprofile%` при формировании списка доверенных приложений через консоль Kaspersky Security Center. Чтобы применить запись ко всем учетным записям, вы можете использовать символ * (например, `C:\Users\*\Documents\File.exe`). При добавлении новой переменной среды нужно перезапустить приложение.

13. Настройте дополнительные параметры доверенного приложения (см. таблицу ниже).

14. Нажмите на кнопку **OK**.

    Новое доверенное приложение будет добавлено в список. Вы можете в любое время исключить приложение из доверенной зоны с помощью флажка в графе **Действие**.

15. Сохраните внесенные изменения.

Как добавить приложение в список доверенных в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Доверенная зона**.

   Откроется окно **Настроить доверенную зону**.

2. В секции **Исключения** нажмите на кнопку **Настройка** напротив блока **Доверенные приложения**.

3. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.
   - **Новое исключение**. Kaspersky Industrial CyberSecurity for Nodes добавляет новое доверенное приложение в корень списка.
   - **Новое исключение в выбранную категорию**. Для добавления нового доверенного приложения в отдельную категорию выберите категорию.
   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes вы можете добавить приложения из списка предустановленных доверенных приложений.

4. Выберите файл из списка или введите путь к исполняемому файлу доверенного приложения.

   Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски.

Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды. При этом Kaspersky Industrial CyberSecurity for Nodes конвертирует путь в локальном интерфейсе приложения. То есть, если вы ввели путь к файлу `%userprofile%\Documents\File.exe`, в локальном интерфейсе приложения для пользователя Fred123 будет добавлена запись `C:\Users\Fred123\Documents\File.exe`. Соответственно, Kaspersky Industrial CyberSecurity for Nodes игнорирует доверенное приложение `File.exe` для других пользователей. Чтобы применить запись ко всем учетным записям, вы можете использовать символ `*` (например, `C:\Users\*\Documents\File.exe`).

При добавлении новой переменной среды нужно перезапустить приложение.

5. Настройте дополнительные параметры доверенного приложения (см. таблицу ниже).

6. Нажмите на кнопку **OK**.

   Новое доверенное приложение будет добавлено в список. Вы можете в любое время исключить приложение из доверенной зоны с помощью флажка напротив названия объекта.

7. Сохраните внесенные изменения.

Параметры доверенного приложения

Параметр	Описание
Использовать полный путь для определения доверенности процесса	Kaspersky Industrial CyberSecurity for Nodes использует полный путь к файлу для определения, является ли процесс доверенным.
Использовать хеш файла для определения доверенности процессов	Kaspersky Industrial CyberSecurity for Nodes использует хеш выбранного файла для определения, является ли процесс доверенным. Если флажок не установлен, хеш файла не учитывается при определении статуса доверенности процесса.
Использование правила	Вы можете настроить перечень компонентов Kaspersky Industrial CyberSecurity for Nodes, которые не будут контролировать активность доверенного приложения: • **Постоянная защита файлов**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes исключает из проверки все файлы, открываемые с помощью доверенного приложения. По умолчанию функция включена. • **Мониторинг доступа к реестру**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes не контролирует изменения ключей реестра из области мониторинга компонента Контроль целостности системы, выполняемые доверенным приложением. По умолчанию функция выключена. • **Анализ поведения и Защита от эксплойтов**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes не контролирует файловую и сетевую активности доверенного приложения в операционной системе с помощью компонентов Защита от шифрования и Защита от эксплойтов. По умолчанию функция выключена. • **Взаимодействие с компонентом AMSI-защита**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes не контролирует запросы доверенного приложения к компоненту AMSI-защита. По умолчанию функция выключена. • **Мониторинг файловых операций**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes не контролирует изменения в файлах из области мониторинга компонента Контроль целостности системы, выполняемые доверенным приложением. По умолчанию функция выключена. • **Телеметрия Endpoint Agent**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes не отправляет данные телеметрии об активности доверенного приложения. По умолчанию функция выключена. Если функция выключена, вы можете отдельно настроить отправку данных телеметрии об управлении доверенным приложением через консоль с помощью флажка **Перехват консольного ввода для телеметрии Endpoint Agent**. • **Контроль запуска программ**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes не контролирует запуск доверенного приложения с помощью компонента Контроль запуска программ. По умолчанию функция выключена. Для предустановленных доверенных приложений по умолчанию включены все функции, кроме **Контроль запуска программ**. Если компонент Обнаружение аномалий с помощью Sigma-правил установлен, функция **Телеметрия Endpoint Agent** также по умолчанию будет выключена.
Разрешить взаимодействие с интерфейсом приложения	Kaspersky Industrial CyberSecurity for Nodes блокирует все попытки управления службами приложения с удаленного компьютера. Если флажок установлен, то приложению удаленного доступа к компьютеру разрешено управлять параметрами Kaspersky Industrial CyberSecurity for Nodes через интерфейс Kaspersky Industrial CyberSecurity for Nodes.
Не контролировать активность дочерних приложений	Kaspersky Industrial CyberSecurity for Nodes не контролирует файловую и сетевую активности приложений, которые запускает приложение. Вы можете применить исключение рекурсивно. В таком случае приложение не контролирует активность всей цепочки дочерних приложений.
Не наследовать ограничения родительского процесса (приложения)	Kaspersky Industrial CyberSecurity for Nodes не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает приложение, для которой настроены права приложения и сетевые правила приложения.
Не проверять память процесса	Kaspersky Industrial CyberSecurity for Nodes не проверяет память процесса.

Создание локальной доверенной зоны

У пользователя есть возможность формировать собственную локальную доверенную зону для отдельного компьютера. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений из проверки и доверенных приложений. Администратор может разрешить или запретить использование локальных исключений или локальных доверенных приложений в параметрах политики. Для этого предназначены флажки **Разрешить использование локальных исключений** и **Разрешать редактирование локальных доверенных приложений** на закладках **Исключения из проверки** и **Доверенные приложения** в разделе политики **Доверенная зона**.

Если администратор разрешил формировать локальную доверенную зону, пользователь может добавлять собственные исключения из проверки и доверенные приложения в Консоли приложения. При этом у пользователя нет прав на изменение или удаление объектов из доверенной зоны, заданной в политике. Также администратор может просматривать, добавлять, изменять или удалять элементы списка в консоли Kaspersky Security Center, если необходимо добавить исключения для отдельного компьютера.

Kaspersky Industrial CyberSecurity for Nodes скрывает для просмотра списки исключений из проверки и доверенных приложений в Консоли приложения, если администратор в консоли запретил настройку доверенной зоны ("замок" закрыт) и запретил использование локальных исключений из проверки и доверенных приложений.

Как добавить объект в локальную доверенную зону в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
2. В рабочей области выберите закладку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. В окне свойств компьютера выберите раздел **Приложения**.
5. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите **Kaspersky Industrial CyberSecurity for Nodes** и откройте свойства приложения двойным щелчком мыши.
6. В окне параметров приложения выберите раздел **Дополнительные возможности** → **Доверенная зона** и нажмите на кнопку **Настройка**.
7. На закладке **Исключения из проверки** сформируйте список локальных исключений из проверки.

   Правила создания локальных исключений из проверки не отличаются от правил создания общих исключений. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски.
8. На закладке **Доверенные приложения** сформируйте список локальных доверенных приложений. Откроется окно со списком локальных доверенных приложений.

   Правила добавления приложений в список локальных доверенных приложений не отличаются от правил добавления в общий список. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски.
9. Сохраните внесенные изменения.

Как добавить объект в локальную доверенную зону в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите предоставить пользователю разрешение на выполнение запрещенного действия.
3. Выберите закладку **Приложения**.
4. Нажмите на **Kaspersky Industrial CyberSecurity for Nodes**.

   Откроются локальные параметры приложения.
5. Выберите закладку **Параметры приложения**.
6. В окне параметров приложения выберите раздел **Дополнительные возможности** → **Доверенная зона** и нажмите на кнопку **Настроить**.

   Откроется окно **Исключения и типы обнаруживаемых объектов**.
7. На закладке **Исключения из проверки** сформируйте список локальных исключений из проверки.

   Правила создания локальных исключений не отличаются от правил создания общих исключений. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски.
8. На закладке **Доверенные приложения** сформируйте список локальных доверенных приложений.

   Правила добавления приложений в список локальных доверенных приложений не отличаются от правил добавления в общий список. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски.
9. Сохраните внесенные изменения.

Как создать локальное исключение из проверки в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Доверенная зона**.

   Откроется окно **Настроить доверенную зону**.
2. В секции **Исключения из проверки и доверенные приложения** нажмите на кнопку **Настройка** напротив блока **Локальные исключения из проверки**.

   > Kaspersky Industrial CyberSecurity for Nodes скрывает для просмотра список исключений из проверки в Консоли приложения, если администратор в Консоли администрирования Kaspersky Security Center запретил настройку исключений из проверки ("замок" закрыт) и запретил использование локальных исключений из проверки (флажок **Разрешить использование локальных исключений** снят).
3. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать исключения из проверки в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно исключение из проверки.
   - **Новое исключение**. Kaspersky Industrial CyberSecurity for Nodes добавляет новое исключение из проверки в корень списка.

- **Новое исключение в выбранную категорию**. Для добавления нового исключения из проверки в отдельную категорию выберите категорию.

- **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes вы можете добавить исключения из списка предустановленных исключений из проверки.

4. Если вы выбрали вариант **Новое исключение**, то откроется окно **Исключение из проверки**.

5. Если вы хотите исключить из проверки файл или папку, установите флажок **Файл или папка**. Нажмите на ссылку **Выберите файл или папку**, и в открывшемся окне выберите файл или папку нажав на кнопку **Обзор**.

   Также вы можете ввести путь вручную. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски:

   - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

   - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

   - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

     Вы можете использовать маски в начале, в середине или в конце пути к файлам. Например, если вы хотите добавить в исключения из проверки папку для всех пользователей, введите маску `?:\Users\*\Folder\`.

6. Если вы хотите исключить из проверки предопределенную область, установите флажок **Предопределенная область**. Нажмите на ссылку **выберите предопределенную область** и в открывшемся окне укажите одну из стандартных областей на защищаемом устройстве.

7. Если вы хотите исключить из проверки определенные объекты, установите флажок **Тип обнаруживаемого объекта**. Нажмите на ссылку **введите названия объектов**, нажмите на кнопку **Добавить** и в открывшемся окне введите название типа объекта по классификации Энциклопедии "Касперского" (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

   Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Industrial CyberSecurity for Nodes исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

8. Если вы хотите исключить из проверки отдельный файл, установите флажок **Хеш объекта**. Нажмите на ссылку **введите хеш объекта** и в открывшемся окне укажите хеш файла.

   Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

9. В блоке **Область применения правил** выберите компоненты, на работу которых должно распространяться исключение из проверки.

10. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

11. Сохраните изменения, чтобы добавить исключение в список. Вы можете в любое время остановить работу исключения с помощью флажка напротив объекта.

Как добавить приложение в список локальных доверенных приложений в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Доверенная зона**.

   Откроется окно **Настроить доверенную зону**.

2. В секции **Исключения** нажмите на кнопку **Настройка** напротив блока **Локальные доверенные приложения**.

   Kaspersky Industrial CyberSecurity for Nodes скрывает для просмотра список доверенных приложений в Консоли приложения, если администратор в Консоли администрирования Kaspersky Security Center запретил настройку доверенных приложений ("замок" закрыт) и запретил использование локальных доверенных приложений (флажок **Разрешать редактирование локальных доверенных приложений** снят).

3. Нажмите на кнопку **Добавить** и выберите нужное действие:

   - **Категорию**. Вы можете группировать доверенные приложения в отдельные категории. Для создания новой категории вам нужно ввести название категории и добавить в категорию хотя бы одно доверенное приложение.
   - **Новое исключение**. Kaspersky Industrial CyberSecurity for Nodes добавляет новое доверенное приложение в корень списка.
   - **Новое исключение в выбранную категорию**. Для добавления нового доверенного приложения в отдельную категорию выберите категорию.
   - **Выбрать исключение из списка**. Для быстрой настройки работы Kaspersky Industrial CyberSecurity for Nodes вы можете добавить приложения из списка предустановленных доверенных приложений.

4. Если вы выбрали вариант **Новое исключение**, то откроется окно **Исключение из проверки**.

5. Установите флажок **Использовать полный путь для определения доверенности процессов** и введите путь к исполняемому файлу доверенного приложения.

   Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски.

   Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды. При этом Kaspersky Industrial CyberSecurity for Nodes конвертирует путь в локальном интерфейсе приложения. То есть, если вы ввели путь к файлу `%userprofile%\Documents\File.exe`, в локальном интерфейсе приложения для пользователя Fred123 будет добавлена запись `C:\Users\Fred123\Documents\File.exe`. Соответственно, Kaspersky Industrial CyberSecurity for Nodes игнорирует доверенное приложение `File.exe` для других пользователей. Чтобы применить запись ко всем учетным записям, вы можете использовать символ `*` (например, `C:\Users\*\Documents\File.exe`).

При добавлении новой переменной среды нужно перезапустить приложение.

6. В окне свойств доверенного приложения настройте дополнительные параметры.

7. Сохраните изменения, чтобы добавить исключение в список.

Экспорт и импорт доверенной зоны

Доверенная зона – это сформированный администратором системы список объектов и приложений, которые Kaspersky Industrial CyberSecurity for Nodes не контролирует в процессе работы. Доверенная зона состоит из следующих списков: *исключения из проверки* и *доверенные приложения*. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных исключений. Также вы можете использовать функцию экспорта/импорта для резервного копирования списков исключений и доверенных приложений или для миграции списков на другой сервер.

Для работы функции экспорта/импорта *списка исключений* и доверенных приложений используется XML формат.

Kaspersky Industrial CyberSecurity for Nodes не поддерживает работу со списками исключений и доверенных приложений, содержащими более 5000 объектов.

Как экспортировать/импортировать доверенную зону в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Дополнительные возможности** → **Доверенная зона** и нажмите на кнопку **Настройка**.

4. Для экспорта списка исключений выполните следующие действия:

   a. Выберите вкладку **Исключения из проверки**.

   b. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

   c. Если вы хотите экспортировать только часть списка, выполните следующие действия:

      1. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A.**

      2. Нажмите на кнопку и выберите **Экспортировать выбранное**.

   d. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список в XML-файл.

5. Для экспорта списка доверенных приложений выполните следующие действия:

   a. Выберите вкладку **Доверенные приложения**.

   b. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

   c. Если вы хотите экспортировать только часть списка, выполните следующие действия:

      1. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A.**

      2. Нажмите на кнопку и выберите **Экспортировать выбранное**.

   d. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список в XML-файл.

6. Для импорта списка исключений выполните следующие действия:

   a. Выберите вкладку **Исключения из проверки**.

      Откроется окно со списком исключений.

   b. Нажмите на значок папки и в выпадающем списке выберите **Импорт**.

   c. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   d. Откройте файл.

      Если на компьютере уже есть список исключений, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

7. Для импорта списка доверенных приложений выполните следующие действия:

   a. Выберите вкладку **Доверенные приложения**.

      Откроется окно со списком доверенных приложений.

   b. Нажмите на кнопку **Импорт**.

   c. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных приложений.

   d. Откройте файл.

      Если на компьютере уже есть список доверенных приложений, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

8. Сохраните внесенные изменения.

Как экспортировать/импортировать доверенную зону в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Дополнительные возможности → Доверенная зона** и нажмите на кнопку **Настроить**.

5. Для экспорта списка исключений выполните следующие действия:

   a. На закладке **Исключения из проверки и доверенные приложения** выберите исключения, которые вы хотите экспортировать.

   b. Нажмите на три точки и выберите **Экспорт**.

   c. Подтвердите, что вы хотите экспортировать только выбранные исключения, или экспортируйте весь список.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список в XML-файл.

6. Для экспорта списка доверенных приложений выполните следующие действия:

   a. На закладке **Исключения из проверки и доверенные приложения** выберите приложения, которые вы хотите экспортировать.

   b. Нажмите на три точки и выберите **Экспорт**.

   c. Подтвердите, что вы хотите экспортировать только выбранные приложения, или экспортируйте весь список.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список в XML-файл.

7. Для импорта списка исключений выполните следующие действия:

   a. На закладке **Исключения из проверки и доверенные приложения** нажмите **Импорт из предыдущей версии**, если хотите импортировать список исключений из XML-файла, созданного в приложении версии 4.0 или ранее.

      При импорте правил из XML-файла, созданного в приложении версии 4.5 и выше, нажмите **Импорт**.

   b. Если на компьютере уже есть список исключений, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

   c. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   d. Нажмите на кнопку **Импорт**.

8. Для импорта списка доверенных приложений выполните следующие действия:

   a. На закладке **Исключения из проверки и доверенные приложения** нажмите **Импорт из предыдущей версии**, если хотите импортировать список доверенных приложений из XML-файла, созданного в приложении версии 4.0 или ранее.

      При импорте доверенных приложений из XML-файла, созданного в приложении версии 4.5 и выше, нажмите **Импорт**.

   b. Если на компьютере уже есть список доверенных приложений, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

   c. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных приложений.

   d. Нажмите на кнопку **Импорт**.

9. Сохраните внесенные изменения.

Как экспортировать/импортировать доверенную зону в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Доверенная зона**.

   Откроется окно **Настроить доверенную зону**.

2. Для экспорта списка исключений или доверенных приложений выполните следующие действия:

   a. В секции **Исключения** нажмите на кнопку **Настройка** напротив блока **Исключения из проверки** или **Доверенные приложения**.

      Откроется окно со списком исключений из проверки или списком доверенных приложений.

   b. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

   c. Если вы хотите экспортировать только часть списка, выполните следующие действия:

      1. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A.**

      2. Нажмите на кнопку и выберите **Экспортировать выбранное**.

   d. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список в XML-файл.

3. Для импорта списка исключений или доверенных приложений выполните следующие действия:

   a. В секции **Исключения** нажмите на кнопку **Настройка** напротив блока **Исключения из проверки** или **Доверенные приложения**.

   b. Выберите исключения или доверенные приложения, которые вы хотите импортировать.

   c. Нажмите на значок папки и выберите вариант **Импортировать**.

   d. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений или доверенных приложений.

   e. Откройте файл.

      Если на компьютере уже есть список исключений, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

4. Сохраните внесенные изменения.

Использование доверенного системного хранилища сертификатов

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки приложения, подписанные доверенной цифровой подписью. Kaspersky Industrial CyberSecurity for Nodes автоматически помещает такие приложения в группу *Доверенные*.

Как настроить использование доверенного системного хранилища сертификатов в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Дополнительные возможности** → **Доверенная зона** и нажмите на кнопку **Настройка**.
4. Выберите закладку **Доверенное системное хранилище сертификатов**.
5. Установите флажок **Использовать доверенное системное хранилище сертификатов** и в раскрывающемся списке выберите, какое системное хранилище Kaspersky Industrial CyberSecurity for Nodes должен считать доверенным.
6. Сохраните внесенные изменения.

Как настроить использование доверенного системного хранилища сертификатов в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Дополнительные возможности** → **Доверенная зона** и нажмите на кнопку **Настроить**.
5. Выберите закладку **Доверенное системное хранилище сертификатов**.
6. Установите флажок **Использовать доверенное системное хранилище сертификатов** и в раскрывающемся списке выберите, какое системное хранилище Kaspersky Industrial CyberSecurity for Nodes должен считать доверенным.
7. Сохраните внесенные изменения.

Как настроить использование доверенного системного хранилища сертификатов в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Доверенная зона**.

   Откроется окно **Настроить доверенную зону**.
2. В блоке **Доверенное системное хранилище сертификатов** установите флажок **Использовать доверенное системное хранилище сертификатов** и в раскрывающемся списке выберите, какое системное хранилище Kaspersky Industrial CyberSecurity for Nodes должен считать доверенным.
3. Сохраните внесенные изменения.

Предустановленные исключения из проверки и доверенные приложения

Предустановленные исключения из проверки и доверенные приложения предназначены для быстрого добавления в доверенную зону процессов и файлов следующего программного обеспечения:

- Промышленное программное обеспечение;
- Microsoft Exchange Server;
- Microsoft SQL Server;
- Microsoft Hyper-V;
- Процесс дедупликации данных в Microsoft Windows Server;
- Microsoft System Center Configuration Manager.

Вы можете выбрать предустановленные исключения и доверенные приложения следующими способами:

- Установка приложения.
  - Локальная установка приложения с помощью мастера.
  - Свойства инсталляционного пакета.
- Настройка политики.
  - Мастер создания политики.
  - Свойства политики: исключения из проверки и доверенные приложения.
  - Через интерфейс командной строки.

Профили исключений для промышленных программ

Профили исключений – это наборы правил исключений в формате XML, предназначенных для добавления процессов и файлов промышленной программы в списки доверенных приложений и исключений из проверки, а также для настройки правил Контроля запуска программ.

В таблице ниже перечислены все доступные профили исключений для промышленных программ.

Правила каждого профиля исключений составлены с учетом того, что промышленная программа установлена в папку по умолчанию. Если промышленная программа установлена не в папку по умолчанию, то правила соответствующего профиля исключений необходимо скорректировать вручную после установки Kaspersky Industrial CyberSecurity for Nodes.

Профиль исключений	Правила конфигурации доверенной зоны	Правила конфигурации Контроля запуска программ	Имя профиля исключений для командной строки
ABB 800xA DCS	Да	Нет	ABB_800xA_DCS
ABB MicroSCADA	Да	Нет	ABB_MicroSCADA
AVADS Archiving Server 1.2	Да	Нет	AVADS_AS_1.2
AVADS SAR Expert 1.0	Да	Нет	AVADS_SAR_Expert_1.0
Bently Nevada System 1	Да	Да	BakerHughes_BentlyNevadaSystem
Bosch Building Integration System	Да	Нет	BOSCH_BIS
BRIC	Да	Нет	BRIC_IDE
Consen SC9000	Да	Нет	Consen
Emerson DeltaV	Да	Да	Emerson_DeltaV
Emerson OpenEnterprise	Да	Да	Emerson_OpenEnterprise
Emerson Ovation	Да	Нет	Emerson_Ovation
Emerson PipelineManager	Да	Нет	Emerson_Pipeline
GE Cimplicity	Да	Нет	GE_Cimplicity
Honeywell Experion PKS	Да	Нет	Honeywell_Experion_PKS
MasterSCADA4D	Да	Нет	MasterSCADA4D
Mitsubishi MAPS	Да	Нет	Mitsubishi_MAPS
Nefteavtomatika “NaftaManagement PCM” 25.01	Да	Нет	Nefteavtomatika_NaftaManagement_PCM_25.01
OMRON CX-Supervisor	Да	Нет	OMRON_CX-Supervisor
PcVue Solutions 15	Да	Да	PcVue_PcVue15
RegLab PC “AstraRegul” 2025.08.15.00	Да	Нет	RegLab_AstraRegul_2025.08.15.00
Rexroth IndraWorks	Да	Нет	Rexroth_IndraWorks
Rockwell Automation FactoryTalk View	Да	Нет	Rockwell_Automation_FactoryTalk_View
Schneider Electric Citect SCADA	Да	Нет	Schneider_Electric_Citect_SCADA
Schneider Electric Clear SCADA	Да	Да	Schneider_Electric_Clear_SCADA
Schneider Electric EcoStruxure Foxboro DCS	Да	Нет	Schneider_Electric_EcoStruxure_Foxboro_DCS
Schneider Electric Unity Pro	Да	Нет	Schneider_Electric_Unity_Pro
Siemens SIMATIC PCS 7 v8.2	Да	Нет	Siemens_SIMATICPCS7-8.2SP1
Siemens SIMATIC PCS 7 v9.0	Да	Нет	Siemens_SIMATICPCS7-9.0SP2
Siemens SIMATIC PCS 7 v9.1	Да	Да	Siemens_SIMATICPCS7-9.1
Siemens SIMATIC WinCC OA	Да	Да	Siemens_SIMATIC_WinCC_OA
Siemens SIMATIC WinCC	Да	Нет	Siemens_SIMATIC_WinCC
Siemens SIMATIC STEP7	Да	Нет	Siemens_SIMATIC_STEP7
Siemens TIA Portal	Да	Нет	Siemens_TIA_Portal
Siemens DIGSI	Да	Нет	Siemens_DIGSI

Профиль исключений	Правила конфигурации доверенной зоны	Правила конфигурации Контроля запуска программ	Имя профиля исключений для командной строки
Siemens SICAM PAS	Да	Нет	`Siemens_SICAM_PAS`
Valmet DNA	Да	Да	`Valmet_DNA`
Wonderware InTouch	Да	Нет	`Wonderware_InTouch`
Wonderware System Platform 2017	Да	Нет	`Wonderware_System-Platform-2017`
Yokogawa CENTUM VP	Да	Нет	`Yokogawa_CENTUM_VP`
Yokogawa ProSafe-RS	Да	Нет	`Yokogawa_ProSafe-RS`
Yokogawa FAST/TOOLS	Да	Нет	`Yokogawa_FAST_TOOLS`
АВАДС САР Эксперт 1.0	Да	Нет	`AVADS_SAR_Expert_1.0`
АВАДС Сервер Архивирования 1.2	Да	Нет	`AVADS_AS_1.2`
АВМ-Энерго SCADA Соника 7.90.26	Да	Нет	`AVM_Energo_SCADA_Sonica_7.90.26`
Альфа платформа	Да	Да	`AutomiqSoft_AlphaPlatform`
ВАКС	Да	Да	`SPEMT_VACSStandart`
ГАУС	Да	Нет	`GAUS`
ИСУБ АРБИТР	Да	Нет	`ARBITR`
Конкор_ПП КТ	Да	Нет	`Software_Platform_KT_1.2`
ПК AstraRegul	Да	Нет	`AstraRegul`
РСУ NaftaProcess	Да	Да	`NaftaProcess_DCS`
Сапкон_ПК i-OMC	Да	Нет	`SUPCON i-OMC_1.2`
Сиб МИР Sibmir_SCADA 1.3	Да	Нет	`SibMir_SCADA`
СимпЛайт_Linux СимпЛайт_Windows	Да	Нет	`SIMP_Light`
ТЕКОН	Да	Нет	`TECON`
Торнадо-N	Да	Да	`Tornado_Tornado-N`
ТРЭИ	Да	Нет	`TREI`
Цифровая Платформа КАСКАД 3.18	Да	Нет	`Kaskad_3.18`
Цифровая Платформа КАСКАД 4	Да	Нет	`KASKAD_4.0`
ЭКРА (EKRASMS, EKRASMS-SP)	Да	Да	`EKRA`

Чтобы применить профиль исключения для промышленных программ во время установки Kaspersky Industrial CyberSecurity for Nodes:

- Выберите нужный профиль исключения на соответствующем шаге Мастера установки приложения.
- Укажите значение параметра установки приложения через интерфейс командной строки `ADDEXCLUSION=<exclusion profile name 1>;<exclusion profile name 2>;...;<exclusion profile name n>`.

Постоянная защита файлов

Компонент Постоянная защита файлов Kaspersky Industrial CyberSecurity for Nodes проверяет следующие объекты защищаемого устройства при доступе к ним:

- файлы;
- альтернативные потоки данных NTFS;
- основную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств;
- файлы-контейнеры Windows Server 2016 и Windows Server 2019.

При записи или считывании файла любым приложением на защищаемом устройстве, Kaspersky Industrial CyberSecurity for Nodes перехватывает этот файл, проверяет его на наличие угроз и при обнаружении угрозы выполняет действия, указанные в параметрах компонента или заданные по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Перед лечением или удалением Kaspersky Industrial CyberSecurity for Nodes сохраняет зашифрованную копию исходного файла в папку резервного хранилища.

Kaspersky Industrial CyberSecurity for Nodes перехватывает файловые операции, исполняемые в контейнерах Windows Server 2016 и Windows Server 2019.

Контейнер – это изолированная среда, где программа может работать без прямого взаимодействия с операционной системой. Если контейнер расположен в области защиты компонента, Kaspersky Industrial CyberSecurity for Nodes проверяет файлы контейнера, к которому получают доступ пользователи, на наличие компьютерных угроз. При обнаружении угрозы, программа пытается вылечить контейнер. Если лечение успешно, контейнер продолжает работу. Если лечение невозможно, контейнер выключается.

Kaspersky Industrial CyberSecurity for Nodes также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem for Linux®. Для таких процессов компонент Постоянная защита файлов применяет действие, указанное в текущих параметрах.

Об области защиты и параметрах безопасности задачи

По умолчанию под действие компонента Постоянная защита файлов подпадают все объекты файловой системы устройства. Если по требованиям к безопасности нет необходимости защищать все объекты файловой системы или вы намеренно хотите исключить некоторые объекты из области действия задачи постоянной защиты, вы можете ограничить область защиты.

В Консоли приложения область защиты представляет собой список файловых ресурсов устройства, контролируемых Kaspersky Industrial CyberSecurity for Nodes.

Параметры безопасности

Параметры безопасности задачи можно настроить как едиными для всех узлов или элементов, входящих в область защиты, так и индивидуальными для каждого узла или элемента списка файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты одним из следующих способов:

- Выбрать один из трех стандартных уровней безопасности.
- Настроить параметры безопасности вручную для выбранных узлов или элементов в списке файловых ресурсов (уровень безопасности изменится на **Другой**).

Стандартные области защиты

В списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие стандартные области защиты:

- **Локальные жесткие диски**. Kaspersky Industrial CyberSecurity for Nodes защищает файлы на жестких дисках устройства.
- **Съемные диски**. Kaspersky Industrial CyberSecurity for Nodes защищает файлы на внешних устройствах, например, на компакт-дисках или съемных дисках. Вы можете включать в область защиты или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Сетевое окружение**. Kaspersky Industrial CyberSecurity for Nodes защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на устройстве. Kaspersky Industrial CyberSecurity for Nodes не защищает файлы, когда к ним обращаются программы с других защищаемых устройств.

Стандартные области защиты по умолчанию отображаются и доступны для изменения в списке областей; можно также добавлять стандартные области защиты в список при его формировании в параметрах области защиты.

Подключенные сетевые диски также не отображаются в списке файловых ресурсов защищаемого устройства. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Стандартные уровни безопасности

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый**, **Максимальная защита** или **Информировать**. Каждый из этих уровней имеет свой стандартный набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Industrial CyberSecurity for Nodes на защищаемых устройствах и рабочих станциях, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность устройств. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты устройств в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если в сети организации предъявляются повышенные требования к безопасности устройств.

Информировать

Уровень безопасности **Информировать** рекомендуется, если в сети организации потенциально много зараженных компьютеров и их блокировка может существенно нарушить работу организации.

Стандартные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности			
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**	**Информировать**
Защита объектов	Объекты, проверяемые по списку расширений, указанному в антивирусных базах	Объекты, проверяемые по формату	Объекты, проверяемые по формату	Объекты, проверяемые по формату
Проверять только новые и измененные файлы	Включено	Включено	Выключено	Включено
Проверка составных файлов	Выключено	Проверять файлы офисных форматов	Проверять файлы офисных форматов	Проверять файлы офисных форматов
Действия над зараженными и другими обнаруженными объектами	Блокировать доступ и лечить. Удалить, если не удалось вылечить	Блокировать доступ и выполнять рекомендованное специалистами "Лаборатории Касперского" действие	Блокировать доступ и лечить. Удалить, если не удалось вылечить	Информировать
Применять действие к выбранным типам объектов	Выключено	Выключено	Выключено	Выключено
Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением	Выключено	Выключено	Включено	Выключено

Системно-критические объекты – это файлы, необходимые для работы операционной системы и Kaspersky Industrial CyberSecurity for Nodes. Такие объекты нельзя удалить. Процессы, относящиеся к таким объектам, не могут быть прекращены.

Параметры	Уровень безопасности			
	Максимальное быстродействие	Рекомендуемый	Максимальная защита	Информировать
Распаковывать в фоновом режиме составные файлы размером более (МБ)				
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.	60 сек.
Не проверять составные объекты размером более (МБ)	8 МБ	8 МБ	Не установлен	8 МБ
Использовать технологию iSwift	Включено	Включено	Включено	Включено
Использовать технологию iChecker	Включено	Включено	Включено	Включено

Расширения файлов, проверяемые по умолчанию компонентом Постоянная защита файлов

По умолчанию Kaspersky Industrial CyberSecurity for Nodes проверяет файлы, имеющие следующие расширения:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*

- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *exe;*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*

- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*

- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?*

Настройка компонента Постоянная защита файлов

По умолчанию компонент Постоянная защита файлов использует параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Параметры компонента Постоянная защита файлов по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Защищаемое устройство целиком, исключая виртуальные диски.	Используйте этот параметр, чтобы изменить область защиты.
Параметры безопасности	Единые для всей области защиты; соответствует уровню безопасности **Рекомендуемый**.	Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия: • выбрать другой стандартный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла.
Режим защиты объектов	**Интеллектуальный режим**.	Этот параметр используется, чтобы указать, при каком типе доступа к объектам Kaspersky Industrial CyberSecurity for Nodes проверяет их.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Вы можете включать и выключать эвристический анализатор, а также регулировать уровень анализа.
Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность	Не применяется.	Этот параметр используется, чтобы заблокировать текущий сеанс и добавить IP-адрес или локально уникальный идентификатор (LUID) узла, для которого была обнаружена вредоносная активность, в раздел Хранилище заблокированных хостов.
Запустить проверку важных областей при обнаружении активного заражения	Применяется.	При обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes создает и запускает Проверку важных областей.
Останавливать контейнер, если лечение невозможно	Применяется.	У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект.
Не проверять файловые операции, исполняемые в контейнерах Windows	Применяется.	Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.

Как включить антивирусную проверку файлов в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Постоянная защита компьютера**.
4. В разделе **Настройки Постоянной защиты файлов** нажмите **Настройка**.
5. Установите флажок **Постоянная защита файлов**.
6. В блоке **Режим защиты объектов** выберите режим работы Постоянной защиты файлов на вкладке **Общие**:

   - **Интеллектуальный режим**. Kaspersky Industrial CyberSecurity for Nodes выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Industrial CyberSecurity for Nodes повторно проверяет объект только после его последнего сохранения этим процессом.

   - **При открытии и изменении**. Kaspersky Industrial CyberSecurity for Nodes проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен. Этот вариант выбран по умолчанию.

- **При открытии**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты при их открытии на чтение, выполнение и изменение.

- **При выполнении**. Kaspersky Industrial CyberSecurity for Nodes проверяет файл только при открытии на выполнение.

7. Снимите или установите флажок **Использовать эвристический анализ**.

8. Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**.

9. Снимите или установите флажок **Запустить проверку важных областей при обнаружении активного заражения**.

   Если флажок установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes запускает предустановленную задачу *Проверка важных областей*. По умолчанию флажок установлен.

10. Укажите настройки проверки файловых операций, исполняемых в контейнерах Windows.

11. Сохраните внесенные изменения.

Как включить антивирусную проверку файлов в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Постоянная защита компьютера → Постоянная защита файлов** и нажмите на кнопку **Настроить**.

5. Установите флажок **Включить Постоянную защиту файлов**.

6. В блоке **Режим защиты объектов** выберите режим работы Постоянной защиты файлов на вкладке **Общие**:

   - **Интеллектуальный режим**. Kaspersky Industrial CyberSecurity for Nodes выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Industrial CyberSecurity for Nodes повторно проверяет объект только после его последнего сохранения этим процессом.

   - **При открытии и изменении**. Kaspersky Industrial CyberSecurity for Nodes проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен. Этот вариант выбран по умолчанию.

   - **При открытии**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты при их открытии на чтение, выполнение и изменение.

   - **При выполнении**. Kaspersky Industrial CyberSecurity for Nodes проверяет файл только при открытии на выполнение.

7. Снимите или установите флажок **Использовать эвристический анализ**.

8. Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для сетевых сессий, с которых ведется вредоносная активность**.

9. Снимите или установите флажок **Запустить проверку важных областей при обнаружении активного заражения**.

   Если флажок установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes запускает предустановленную задачу *Проверка важных областей*. По умолчанию флажок установлен.

10. Укажите настройки проверки файловых операций, исполняемых в контейнерах Windows.

11. Сохраните внесенные изменения.

Как включить антивирусную проверку файлов в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера → Постоянная защита файлов**.

2. В панели результатов узла **Постоянная защита файлов** нажмите **Свойства**.

   Откроется окно **Свойства: Постоянная защита файлов**.

3. Установите флажок **Постоянная защита файлов**.

4. В блоке **Режим защиты объектов** выберите режим работы Постоянной защиты файлов на вкладке **Общие**:

   - **Интеллектуальный режим**. Kaspersky Industrial CyberSecurity for Nodes выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Industrial CyberSecurity for Nodes повторно проверяет объект только после его последнего сохранения этим процессом.

   - **При открытии и изменении**. Kaspersky Industrial CyberSecurity for Nodes проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен. Этот вариант выбран по умолчанию.

   - **При открытии**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты при их открытии на чтение, выполнение и изменение.

   - **При выполнении**. Kaspersky Industrial CyberSecurity for Nodes проверяет файл только при открытии на выполнение.

5. Снимите или установите флажок **Использовать эвристический анализ**.

6. Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для сессий, с которых ведется вредоносная активность**.

7. Снимите или установите флажок **Запустить проверку важных областей при обнаружении активного заражения**.

   Если флажок установлен, то при обнаружении активного заражения Kaspersky Industrial CyberSecurity for Nodes запускает предустановленную задачу *Проверка важных областей*. По умолчанию флажок установлен.

8. Укажите настройки проверки файловых операций, исполняемых в контейнерах Windows.

9. Сохраните внесенные изменения.

Настройка области защиты для компонента Постоянная защита файлов

По умолчанию для компонента Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в списке файловых ресурсов устройства.

Если один объект входит в несколько записей области защиты и эти записи имеют разные уровни безопасности, то приоритет последнего правила в списке выше. Например, область защиты включает в себя две записи: **Все жесткие диски** (уровень безопасности **Информировать**) и `*\Users\*\Downloads\*` (уровень безопасности **Другой**). Приложение будет проверять память жестких дисков в соответствии с уровнем безопасности Информировать, кроме папки `Downloads`. Папку `Downloads` приложение будет проверять в соответствии с параметрами, заданными вручную, так как эта запись последняя в списке области защиты.

Как настроить область защиты для проверки файлов в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Постоянная защита компьютера**.
4. В разделе **Постоянная защита файлов** нажмите **Настройка**.
5. Перейдите на закладку **Область защиты**.
6. В списке файловых ресурсов защищаемого устройства выберите элементы, для которых вы хотите задать стандартный уровень безопасности.
7. Если файлового ресурса нет в списке, добавьте его вручную:
   a. Нажмите на кнопку **Добавить**.
   b. С помощью дерева папок укажите путь к нужному объекту или введите путь в поле **Объект**.

Если необходимо, используйте специальные символы для ввода маски пути к объекту:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Объект **Этот компьютер** в списке файловых ресурсов компьютера включает в себя следующие объекты: **Все жесткие диски**, **Все сетевые диски** и **Все съемные диски**.

c. Нажмите на кнопку **OK**.

8. Убедитесь, что выбранный файловый ресурс включен в область защиты.

9. Укажите стандартный уровень безопасности для выбранной области защиты по кнопке **Настроить**. По умолчанию применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**. Также вы можете изменить значения параметров безопасности, заданные по умолчанию.

10. Сохраните внесенные изменения.

Как настроить область защиты для проверки файлов в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Постоянная защита компьютера** → **Постоянная защита файлов** и нажмите на кнопку **Настроить**.

5. Перейдите на закладку **Область защиты**.

6. В списке файловых ресурсов защищаемого устройства выберите элементы, для которых вы хотите задать стандартный уровень безопасности.

7. Если файлового ресурса нет в списке, добавьте его вручную:

   a. Нажмите на кнопку **Добавить**.

   b. В списке **Тип объекта** выберите нужный вариант.

Для варианта **Маска** используйте специальные символы для ввода маски пути к объекту:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Объект **Этот компьютер** в списке файловых ресурсов компьютера включает в себя следующие объекты: **Все жесткие диски**, **Все сетевые диски** и **Все съемные диски**.

c. Нажмите на кнопку **OK**.

8. Убедитесь, что выбранный файловый ресурс включен в область защиты с помощью переключателя рядом с элементом списка.

9. Укажите стандартный уровень безопасности для выбранной области защиты по кнопке **Изменить**. По умолчанию применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**. Также вы можете изменить значения параметров безопасности, заданные по умолчанию.

10. Сохраните внесенные изменения.

Как настроить область защиты для проверки файлов в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера → Постоянная защита файлов**.

2. В панели результатов узла **Постоянная защита файлов** нажмите **Настройка области защиты**.

   Откроется окно **Свойства: Постоянная защита файлов**.

3. В списке файловых ресурсов защищаемого устройства выберите элементы, для которых вы хотите задать стандартный уровень безопасности.

4. Если файлового ресурса нет в списке, добавьте его вручную:

   a. Нажмите на кнопку **Добавить**.

   b. С помощью дерева папок укажите путь к нужному объекту или введите путь в поле **Объект**.

Если необходимо, используйте специальные символы для ввода маски пути к объекту:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Объект **Этот компьютер** в списке файловых ресурсов компьютера включает в себя следующие объекты: **Все жесткие диски**, **Все сетевые диски** и **Все съемные диски**.

c. Нажмите на кнопку **OK**.

5. Убедитесь, что выбранный файловый ресурс включен в область защиты.

6. Укажите стандартный уровень безопасности для выбранной области защиты по кнопке **Настроить**. По умолчанию применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**. Также вы можете изменить значения параметров безопасности, заданные по умолчанию.

7. Сохраните внесенные изменения.

Настройка параметров безопасности вручную

По умолчанию в задачах постоянной защиты компьютера применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

При работе с деревом файловых ресурсов защищаемого устройства параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Как настроить параметры безопасности вручную в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне свойств политики выберите **Постоянная защита компьютера**.

4. В разделе **Постоянная защита файлов** нажмите **Настройка**.

5. В окне **Постоянная защита файлов** перейдите на вкладку **Область защиты**.

6. Выберите ресурс, параметры безопасности которого вы хотите настроить.

7. Нажмите на кнопку **Настроить**.

8. В открывшемся окне выберите требуемый уровень безопасности и нажмите на кнопку **Настройка**.

9. На закладке **Общие** укажите следующие настройки:

   - Объекты, которые требуется включить в область защиты:

     - **Все объекты**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты.

     - **Объекты, проверяемые по формату**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании формата файла. Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

     - **Объекты, проверяемые по указанному списку расширений**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений задается пользователем вручную.

   - В блоке **Оптимизация** установите или снимите флажок **Проверять только новые и измененные файлы**.

   - В блоке **Проверка составных файлов** укажите составные объекты, которые вы хотите включить в область проверки:

     - **Проверять архивы**

     - **Проверять дистрибутивы**

     - **Проверять файлы офисных форматов**

     - **Проверять файлы почтовых форматов**

10. На закладке **Действия** укажите следующие настройки:

    - Выберите действие над зараженными и другими обнаруживаемыми объектами:

      - **Информировать**

      - **Блокировать**

      - **Выполнять дополнительное действие**

Выберите действие из раскрывающегося списка:

- **Лечить**
- **Лечить. Удалять, если не удалось вылечить**
- **Удалять**
- **Рекомендуемое**

- Настройте действия над объектами в зависимости от типа обнаруженного объекта:

  a. Снимите или установите флажок **Применять действие к выбранным типам объектов**.

  b. Нажмите на кнопку **Настройка** и выберите типы обнаруживаемых объектов.

- Настройте действия над составными файлами, недоступными для изменения: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением**.

11. На закладке **Оптимизация** укажите следующие настройки:

- **Распаковывать в фоновом режиме составные файлы размером более (МБ)**
- **Останавливать проверку, если она длится более (сек.)**
- **Не проверять составные объекты размером более (МБ)**
- **Использовать технологию iSwift**
- **Использовать технологию iChecker**

12. Сохраните новые параметры безопасности.

Как настроить параметры безопасности вручную в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера** → **Постоянная защита файлов** и нажмите на кнопку **Настроить**.
5. Перейдите на закладку **Область защиты**.
6. Выполните одно из следующих действий:

- Нажмите на кнопку **Добавить**, чтобы добавить новое правило и указать для него настройки безопасности.
- Выберите существующее правило и нажмите на кнопку **Изменить**.

Откроется окно **Изменить область**.

7. Установите переключатель в положение **Активный**.

8. Выберите уровень безопасности и укажите нужные настройки безопасности.

9. В разделе **Режим защиты объектов** выберите тип объекта, который вы хотите включить в область защиты:

   - Объекты, которые требуется включить в область защиты:

     - **Все объекты**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты.

     - **Объекты, проверяемые по формату**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании формата файла. Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

     - **Объекты, проверяемые по указанному списку расширений**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений задается пользователем вручную.

10. В разделе **Оптимизация** установите или снимите флажок **Защита только новых и измененных файлов**.

11. В разделе **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

    - **Проверять архивы**
    - **Проверять дистрибутивы**
    - **Проверять файлы офисных форматов**
    - **Проверять файлы почтовых форматов**

12. Выберите действие над зараженными и другими обнаруживаемыми объектами:

    - **Информировать**
    - **Блокировать**
    - **Выполнять дополнительное действие**

      Выберите действие из раскрывающегося списка:

      - **Лечить**
      - **Лечить. Удалять, если лечение невозможно**

- **Удалять**
- **Рекомендуемое**

13. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

    a. Снимите или установите флажок **Применять действие к выбранным типам объектов**.

    b. Если флажок установлен, нажмите на кнопку **Настройка** и выберите типы обнаруживаемых объектов.

14. Настройте действия над составными файлами, недоступными для изменения: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением**.

15. В разделе **Оптимизация** настройте следующие параметры:

    - **Распаковывать составные файлы в фоновом режиме**
    - **Останавливать проверку, если она длится более (сек.)**
    - **Не проверять составные объекты размером более (МБ)**
    - **Использовать технологию iSwift**
    - **Использовать технологию iChecker**

16. Сохраните новые параметры безопасности.

Как настроить параметры безопасности вручную в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера** → **Постоянная защита файлов**.

2. В панели результатов узла **Постоянная защита файлов** нажмите **Настройка области защиты**.

   Откроется окно **Свойства: Постоянная защита файлов**.

3. Выберите ресурс, параметры безопасности которого вы хотите настроить.

4. Нажмите на кнопку **Настроить**.

5. В открывшемся окне выберите требуемый уровень безопасности и нажмите на кнопку **Настройка**.

6. На вкладке **Общие** укажите следующие настройки:

   - Объекты, которые требуется включить в область защиты:

     - **Все объекты**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты.

     - **Объекты, проверяемые по формату**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании формата файла. Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.

- **Объекты, проверяемые по указанному списку расширений**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений задается пользователем вручную.

- В блоке **Оптимизация** установите или снимите флажок **Защита только новых и измененных файлов**.

- В блоке **Проверка составных файлов** укажите составные объекты, которые вы хотите включить в область проверки:

  - **Проверять архивы**. Проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).

  - **Проверять дистрибутивы**. Флажок включает или выключает проверку дистрибутивов сторонних приложений.

  - **Проверять файлы офисных форматов**. Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам офисных форматов также относятся OLE-объекты. Kaspersky Industrial CyberSecurity for Nodes проверяет файлы офисных форматов, размер которых меньше 1 МБ, независимо от состояния флажка.

  - **Проверять файлы почтовых форматов**.

7. На вкладке **Действия** укажите следующие настройки:

- Выберите действие над зараженными и другими обнаруживаемыми объектами:

  - **Информировать**;

  - **Блокировать**;

  - **Выполнять дополнительное действие**.

    Выберите действие из раскрывающегося списка:

    - **Лечить**;

    - **Лечить. Удалять, если не удалось вылечить**;

    - **Удалять**;

    - **Рекомендуемое**.

- Настройте действия над объектами в зависимости от типа обнаруженного объекта:

  a. Снимите или установите флажок **Применять действие к выбранным типам объектов**.

  b. Нажмите на кнопку **Настройка** и выберите типы обнаруживаемых объектов.

- Настройте действия над составными файлами, недоступными для изменения: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением**.

8. На вкладке **Оптимизация** укажите следующие настройки:

   - **Распаковывать в фоновом режиме составные файлы размером более (МБ)**;
   - **Останавливать проверку, если она длится более (сек.)**;
   - **Не проверять составные объекты размером более (МБ)**;
   - **Использовать технологию iSwift**;
   - **Использовать технологию iChecker**.

9. Сохраните новые параметры безопасности.

Проверка контейнеров

Контейнер – это изолированная среда, где приложение может работать без прямого взаимодействия с операционной системой. Использование контейнеров включает в себя следующие риски:

- Уязвимости в процессе контейнеризации могут быть использованы злоумышленниками для компрометации приложений внутри контейнера.
- Небезопасная конфигурация контейнерной среды может быть использована злоумышленниками для получения несанкционированного доступа к данным компьютера или нарушения целостности системы.
- Взлом контейнера может позволить злоумышленнику получить доступ к данным компьютера.
- Сетевые уязвимости могут быть использованы злоумышленниками для перехвата сетевого трафика.

Kaspersky Industrial CyberSecurity for Nodes является внешним инструментом для обнаружения вредоносной активности внутри контейнеров. Это позволяет сохранить производительность контейнеров и избежать конфликтов с другими приложениями внутри контейнера. Установка Kaspersky Industrial CyberSecurity for Nodes внутрь контейнера не поддерживается.

Кроме обеспечения безопасности контейнеров, Kaspersky Industrial CyberSecurity for Nodes позволяет управлять работой приложений внутри контейнеров с помощью компонента Контроль запуска программ. Настройка компонента Контроль запуска программ для контейнеров не отличается от настройки компонента для приложений, установленных на компьютере. Компонент Контроль целостности системы также поддерживает контейнеры.

Требования к контейнерам

- Контейнер создан на платформе Docker. Другие средства контейнеризации не поддерживаются.
- Контейнер запущен в режиме изоляции процессов. Режим изоляции Hyper-V не поддерживается.
- Контейнер расположен на сервере под управлением Windows Server 2016, 2019 или 2022 (Docker Host).
- Контейнер включает в себя образ Windows (Docker Image). ОС Windows 10 и 11 не поддерживаются. Образы Linux не поддерживаются.
- Не поддерживается проверка контейнеров, запущенных в режиме WSL2 – Windows Subsystem for Linux v2 (Docker Wine).

Действие при обнаружении угрозы

При обнаружении угрозы внутри контейнера, приложение применяет действие, выбранное для компонента Постоянная защита файлов. Также проверка контейнеров имеет дополнительные параметры (см. инструкцию ниже). При обнаружении угрозы, приложение блокирует вредоносную активность и выполняет выбранное действие (например, пытается вылечить объект). Kaspersky Industrial CyberSecurity for Nodes может остановить контейнер, если вылечить обнаруженный объект не удалось. По умолчанию функция остановки контейнеров включена.

Как настроить проверку контейнеров в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Постоянная защита компьютера**.
4. В разделе **Постоянная защита файлов** нажмите **Настройка**.
5. В блоке **Проверка файловых операций, исполняемых в контейнерах Windows** настройте параметры проверки контейнеров:
   - **Останавливать контейнер, если лечение невозможно.** У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект.
   - **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.
6. Сохраните новые параметры безопасности.

Как настроить проверку контейнеров в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Постоянная защита компьютера → Постоянная защита файлов** и нажмите на кнопку **Настроить**.

5. В блоке **Проверка файловых операций, исполняемых в контейнерах Windows** настройте параметры проверки контейнеров:

   - **Останавливать контейнер, если лечение невозможно.** У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект.

   - **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.

6. Сохраните новые параметры безопасности.

Как настроить проверку контейнеров в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера → Постоянная защита файлов**.

2. В панели результатов узла **Постоянная защита файлов** нажмите **Свойства**.

   Откроется окно **Свойства: Постоянная защита файлов**.

3. В блоке **Проверка файловых операций, исполняемых в контейнерах Windows** настройте параметры проверки контейнеров:

   - **Останавливать контейнер, если лечение невозможно.** У приложения может не быть прав на чтение и запись обнаруженного объекта. В этом случае вылечить или удалить обнаруженный объект невозможно. Если флажок установлен, приложение блокирует обнаруженный объект и останавливает контейнер. Если флажок снят, приложение только блокирует обнаруженный объект.

   - **Не проверять файловые операции, исполняемые в контейнерах Windows**. Если флажок установлен, приложение проверяет контейнер только при запуске контейнера. Если флажок снят, приложение проверяет контейнер постоянно в режиме реального времени.

4. Сохраните внесенные изменения.

Использование KSN

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Industrial CyberSecurity for Nodes использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть Kaspersky Security Network.

Функциональность KSN может быть недоступна в приложении на территории США.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Industrial CyberSecurity for Nodes на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Industrial CyberSecurity for Nodes получает от служб KSN сведения о репутации проверяемых веб-адресов, а также сведения о категории и репутации проверяемых файлов. Подробнее о настройке доступа к KSN см. в справке Kaspersky Security Center.

Использование Kaspersky Security Network является добровольным. Приложение предлагает использовать KSN во время первоначальной настройки приложения. Начать или прекратить использование KSN можно в любой момент.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского". Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки приложения.

Инфраструктура репутационных баз "Лаборатории Касперского"

Kaspersky Industrial CyberSecurity for Nodes поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от "Лаборатории Касперского", а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Industrial CyberSecurity for Nodes или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к сети Интернет;

  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Включение использования Kaspersky Security Network

Как включить использование Kaspersky Security Network с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Network выберите папку **Политики**.
2. Выберите нужную политику Kaspersky Industrial CyberSecurity for Nodes и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне в списке разделов выберите **Постоянная защита компьютера → Использование KSN**.
4. Нажмите на кнопку **Настройка**.
5. Установите флажок **Kaspersky Security Network**, чтобы включить компонент.

   Если вы включили использование KSN, Kaspersky Industrial CyberSecurity for Nodes покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования KSN.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes использует расширенный режим Kaspersky Security Network. Расширенный режим Kaspersky Security Network – режим работы приложения, при котором Kaspersky Industrial CyberSecurity for Nodes передает в "Лабораторию Касперского" дополнительные данные.
6. Если требуется, снимите флажок **Включить расширенный режим KSN**.
7. Сохраните внесенные изменения.

Если использование Kaspersky Security Network включено, Kaspersky Industrial CyberSecurity for Nodes использует информацию о репутации файлов, веб-ресурсов и приложений, полученную из Kaspersky Security Network.

Как включить использование Kaspersky Security Network с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Kaspersky Security Network**.
3. В главном окне приложения нажмите **Свойства**.
4. Установите флажок **Kaspersky Security Network**, чтобы включить компонент.

   Если вы включили использование KSN, Kaspersky Industrial CyberSecurity for Nodes покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования KSN.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes использует расширенный режим Kaspersky Security Network. Расширенный режим Kaspersky Security Network – режим работы приложения, при котором Kaspersky Industrial CyberSecurity for Nodes передает в "Лабораторию Касперского" дополнительные данные.
5. Если требуется, снимите флажок **Включить расширенный режим KSN**.
6. Сохраните внесенные изменения.

Если использование Kaspersky Security Network включено, Kaspersky Industrial CyberSecurity for Nodes использует информацию о репутации файлов, веб-ресурсов и приложений, полученную из Kaspersky Security Network.

Как включить использование Kaspersky Security Network с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера → Использование KSN** и нажмите на кнопку **Настроить.**
5. В открывшемся окне установите флажок **Включить Kaspersky Security Network**, чтобы включить компонент.

   Если вы включили использование KSN, Kaspersky Industrial CyberSecurity for Nodes покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования Kaspersky Security Network.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes использует расширенный режим Kaspersky Security Network. Расширенный режим Kaspersky Security Network – режим работы приложения, при котором Kaspersky Industrial CyberSecurity for Nodes передает в "Лабораторию Касперского" дополнительные данные.
6. Если требуется, снимите флажок **Включить расширенный режим KSN**.
7. Сохраните внесенные изменения.

В результате, если использование Kaspersky Security Network включено, Kaspersky Industrial CyberSecurity for Nodes использует информацию о репутации файлов, веб-ресурсов и приложений, полученную из Kaspersky Security Network.

Статистика использования Kaspersky Security Network

Во время выполнения задачи *Использование Kaspersky Security Network* вы можете просматривать в реальном времени информацию о количестве объектов, обработанных Kaspersky Industrial CyberSecurity for Nodes с момента запуска задачи до текущего момента.

Чтобы просмотреть статистику использования KSN, выполните следующие действия:

1. В дереве Консоли приложения выберите раздел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Kaspersky Security Network**.

   В панели результатов в разделе **Статистика** отобразится статистика выполнения задачи (см. таблицу ниже).

Статистика KSN

Поле	Описание
Отправлено файловых запросов	Количество запросов о репутации объектов, отправленных Kaspersky Industrial CyberSecurity for Nodes в KSN.
Недоверенных заключений по файлам	Количество объектов, репутация которых признана недоверенной согласно ответу KSN.
Ошибок отправки запросов	Количество запросов в KSN, во время обработки которых возникла ошибка.
Пакетов статистик сформировано	Количество пакетов с данными, которые были отправлены на обработку в KSN.
Удалено объектов	Количество объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes успешно удалило.
Не удалено объектов	Количество объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes не смогло удалить, например, если доступ к объекту был заблокирован другой программой.
Помещено в резервное хранилище	Количество объектов, копии которых приложение Kaspersky Industrial CyberSecurity for Nodes успешно сохранило в резервном хранилище.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых приложение Kaspersky Industrial CyberSecurity for Nodes не смогло сохранить в резервном хранилище, например, из-за отсутствия доступного пространства на диске. Приложение не лечит и не удаляет файлы, которые не удалось поместить в резервное хранилище.
Ограниченный режим	Статус отправки запросов о репутации файлов в ограниченном режиме. В ограниченном режиме Kaspersky Industrial CyberSecurity for Nodes отправляет только часть запросов о репутации файлов, в соответствии с рекомендациями специалистов "Лаборатории Касперского".

Значения полей **Удалено объектов**, **Не удалено объектов**, **Помещено в резервное хранилище**, **Объектов, не помещенных в резервное хранилище** формируются на основе статистики работы компонента Постоянная защита файлов.

Ограничения работы с Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Industrial CyberSecurity for Nodes или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. Kaspersky Private Security Network позволяет использовать собственную базу данных репутаций объектов (файлов или веб-адресов) с помощью локальной репутационной базы. Репутация объекта, добавленного в локальную репутационную базу, имеет приоритет выше, чем в KSN/KPSN. То есть, если Kaspersky Industrial CyberSecurity for Nodes при проверке компьютера запросит репутацию файла в KSN/KPSN, и в локальной репутационной базе файл имеет репутацию *Недоверенные*, а в KSN/KPSN объект имеет репутацию *Доверенные*, то Kaspersky Industrial CyberSecurity for Nodes обнаружит файл как *Недоверенные* и выполнит действие, заданное для обнаруженных угроз.

Однако в некоторых случаях Kaspersky Industrial CyberSecurity for Nodes может не запрашивать репутацию объекта в KSN/KPSN. В результате Kaspersky Industrial CyberSecurity for Nodes не получит данные из локальной репутационной базы KPSN. Kaspersky Industrial CyberSecurity for Nodes может не запрашивать репутацию объекта в KSN/KPSN, например, по следующим причинам:

- Приложения "Лаборатории Касперского" используют офлайн репутационные базы. Офлайн репутационные базы предназначены для оптимизации ресурсов при работе приложений "Лаборатории Касперского" и защите критически важных объектов компьютера. Офлайн репутационные базы формируют специалисты "Лаборатории Касперского" на основании данных Kaspersky Security Network. приложения "Лаборатории Касперского" обновляют офлайн репутационные базы с антивирусными базами приложения. Если информация о проверяемом объекте содержится в офлайн репутационных базах, приложение не запрашивает репутацию этого объекта в KSN/KPSN.

- В параметрах приложения настроены исключения из проверки (доверенная зона). В этом случае приложение не учитывает репутацию объекта в локальной репутационной базе.

- Приложение использует технологии оптимизации проверки, например, технологии iSwift, iChecker или кеширование запросов репутации в KSN/KPSN. В этом случае приложение может не запрашивать репутацию ранее проверенных объектов.

- Для оптимизации нагрузки приложение проверяет файлы определенного формата и размера. Список форматов и ограничения по размеру определяют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами приложения.

Настройка KSN Proxy

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.

- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал связи с внешней сетью и ускоряя получение компьютером пользователя запрошенной информации.

По умолчанию после включения использования KSN и принятия Положения об использовании KSN приложение использует прокси-сервер для связи с Kaspersky Security Network. В качестве прокси-сервера приложение использует Сервер администрирования Kaspersky Security Center и TCP-порт 13111. Таким образом, если KSN Proxy недоступен, требуется проверить работу устройства как прокси-сервера KSN. Вам нужно проверить следующие параметры:

- На Сервере администрирования запущена служба *ksnproxy*.

- На компьютере Сетевой экран не блокирует порт 13111.

Вы можете настроить использование KSN Proxy: включить или выключить KSN Proxy, настроить порт для соединения. Для этого вам нужно открыть свойства Сервера администрирования. Подробнее о настройке KSN Proxy см. в справке Kaspersky Security Center. Также вы можете включить или выключить KSN Proxy для отдельных компьютеров в политике Kaspersky Industrial CyberSecurity for Nodes.

Как включить KSN Proxy с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику Kaspersky Industrial CyberSecurity for Nodes и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне в списке разделов выберите **Постоянная защита компьютера → Использование KSN**.
4. Нажмите на кнопку **Настройка**.
5. В блоке **Настройки KSN Proxy** используйте флажок **Использовать Сервер администрирования как прокси-сервер KSN**, чтобы включить или выключить KSN Proxy.
6. Если требуется, установите флажок **Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен**.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как в "Лаборатории Касперского", так и на сторонних серверах, в случае использования Kaspersky Private Security Network.
7. Сохраните внесенные изменения.

Как включить KSN Proxy с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Kaspersky Security Network**.
3. В главном окне приложения нажмите **Свойства**.
4. В блоке **Настройки KSN Proxy** используйте флажок **Использовать Сервер администрирования как прокси-сервер KSN**, чтобы включить или выключить KSN Proxy.
5. Если требуется, установите флажок **Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен**.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как в "Лаборатории Касперского", так и на сторонних серверах, в случае использования Kaspersky Private Security Network.
6. Сохраните внесенные изменения.

Как включить KSN Proxy с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера → Использование KSN** и нажмите на кнопку **Настроить**.
5. С помощью флажка **Использовать Сервер администрирования как прокси-сервер KSN** включите или выключите KSN Proxy.

6. Если требуется, установите флажок **Использовать серверы Kaspersky Security Network, если прокси-сервер KSN недоступен**.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует серверы KSN, когда служба KSN Proxy недоступна. Серверы KSN могут быть расположены как в "Лаборатории Касперского", так и на сторонних серверах, в случае использования Kaspersky Private Security Network.

7. Сохраните внесенные изменения.

Адрес KSN Proxy совпадает с адресом Сервера администрирования. При изменении доменного имени Сервера администрирования необходимо обновить адрес KSN Proxy вручную.

Защита от эксплойтов

Kaspersky Industrial CyberSecurity for Nodes предоставляет возможность защитить память процессов от эксплойтов. Эта возможность реализована в компоненте Защита от эксплойтов, с помощью которого вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимое приложение. При обработке этих данных уязвимое приложение выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО. Если попытка запустить исполняемый файл из уязвимого приложения не была произведена пользователем, то Kaspersky Industrial CyberSecurity for Nodes блокирует запуск этого файла или информирует пользователя. Компонент выполняет защиту памяти процессов от эксплойтов с помощью внедрения внешнего Агента защиты процессов в защищаемый процесс.

Агент защиты процессов (далее *Агент*) – это динамически загружаемый модуль Kaspersky Industrial CyberSecurity for Nodes, который внедряется в защищаемые процессы с целью контроля их целостности и снижения рисков эксплуатации уязвимостей.

Функционирование Агента внутри защищаемого процесса зависит от итераций запуска и остановки этого процесса: первичная загрузка Агента в процесс, добавленный в список защищаемых, возможна только при перезапуске процесса. Выгрузка Агента из процесса после его удаления из списка защищаемых также возможна только после перезапуска процесса.

Выгрузка Агента из защищаемых процессов предполагает необходимость их остановки: при удалении компонента Защита от эксплойтов программа выполняет заморозку среды и форсирует выгрузку Агента из защищаемых процессов. Если при удалении компонента Агент внедрен хотя бы в один из защищаемых процессов, вам нужно завершить данный процесс. Может потребоваться перезагрузка защищаемого устройства (например, при защите системного процесса).

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Industrial CyberSecurity for Nodes выполняет одно из следующих действий:

- завершает процесс при попытке эксплуатации уязвимости;
- сообщает о факте дискредитации уязвимости в процессе.

Вы можете остановить защиту процессов одним из следующих способов:

- удалить компонент;
- удалить процесс из списка защищаемых и перезапустить его.

Режимы защиты от эксплойтов

Вы можете настраивать действия по снижению рисков эксплуатации уязвимостей в защищаемых процессах, выбрав один из следующих режимов:

- **Блокировать**. Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

  При обнаружении попытки эксплуатации уязвимости в защищаемом процессе, которому присвоен уровень "критический" в операционной системе, Kaspersky Industrial CyberSecurity for Nodes не выполняет завершение такого процесса независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

- **Информировать** (при работе с помощью Web Console – **Информировать**). Применяйте этот режим, чтобы получать данные о фактах эксплуатации уязвимостей в защищаемых процессах с помощью событий в журнале безопасности. Скомпрометированный процесс продолжает выполняться.

  В этом режиме Kaspersky Industrial CyberSecurity for Nodes регистрирует все попытки эксплуатации уязвимостей посредством создания событий. Выбран по умолчанию.

Включение и выключение Защиты от эксплойтов

Kaspersky Industrial CyberSecurity for Nodes позволяет отслеживать исполняемые файлы, запускаемые уязвимыми приложениями. Если Kaspersky Industrial CyberSecurity for Nodes обнаруживает, что исполняемый файл из уязвимого приложения был запущен не пользователем, то Kaspersky Industrial CyberSecurity for Nodes выполняет выбранное действие (например, блокирует операцию).

Как включить или выключить Защиту от эксплойтов с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику Kaspersky Industrial CyberSecurity for Nodes и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне в списке разделов выберите **Постоянная защита компьютера → Защита от эксплойтов**.
4. Нажмите на кнопку **Настройка**.
5. Установите флажок **Защита от эксплойтов**, чтобы включить компонент.
6. На вкладке **Общие** выберите режим защиты от эксплойтов: **Блокировать** или **Информировать**.
7. Если требуется, вы можете снять флажок **Защита от эксплойтов**, чтобы выключить компонент.
8. Сохраните внесенные изменения.

Как включить или выключить Защиту от эксплойтов с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от эксплойтов**.
3. В главном окне приложения нажмите **Свойства**.
4. Установите флажок **Защита от эксплойтов**, чтобы включить компонент.
5. На вкладке **Общие** выберите режим защиты от эксплойтов: **Блокировать** или **Информировать**.
6. Если требуется, вы можете снять флажок **Защита от эксплойтов**, чтобы выключить компонент.
7. Сохраните внесенные изменения.

Как включить или выключить Защиту от эксплойтов с помощью Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера** → **Защита от эксплойтов** и нажмите на кнопку **Настроить**.
5. В открывшемся окне в блоке **Режим Защиты от эксплойтов** установите флажок **Защищать процессы от эксплуатации уязвимостей в режиме**, чтобы включить компонент.
6. Выберите режим защиты от эксплойтов: **Блокировать** или **Информировать**.
7. Если требуется, снимите флажок **Защищать процессы от эксплуатации уязвимостей в режиме**, чтобы выключить компонент.
8. Сохраните внесенные изменения.

Включение и выключение защиты памяти

Kaspersky Industrial CyberSecurity for Nodes блокирует сторонние процессы, которые осуществляют попытки доступа к системным процессам. По умолчанию защита памяти системных процессов включена.

Как включить или выключить защиту памяти с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику Kaspersky Industrial CyberSecurity for Nodes и откройте свойства политики двойным щелчком мыши.

3. В открывшемся окне в списке разделов выберите **Постоянная защита компьютера → Защита от эксплойтов**.
4. Нажмите на кнопку **Настройка**.
5. На вкладке **Общие** установите флажок **Включить защиту памяти системных процессов**.
6. Если требуется, снимите флажок **Включить защиту памяти системных процессов**.
7. Сохраните внесенные изменения.

Как включить или выключить защиту памяти с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от эксплойтов**.
3. В главном окне приложения нажмите **Свойства**.
4. На вкладке **Общие** установите флажок **Включить защиту памяти системных процессов**.
5. Если требуется, снимите флажок **Включить защиту памяти системных процессов**.
6. Сохраните внесенные изменения.

Как включить или выключить защиту памяти с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера → Защита от эксплойтов** и нажмите на кнопку **Настроить**.
5. В открывшемся окне в блоке **Защита памяти системных процессов** установите флажок **Защита памяти системных процессов**.
6. Если требуется, снимите флажок **Защита памяти системных процессов**, чтобы выключить защиту памяти системных процессов.
7. Сохраните внесенные изменения.

Формирование списка защищаемых процессов

По умолчанию компонент Защита от эксплойтов обеспечивает защиту нескольких процессов. Список защищаемых процессов может быть сформирован программой автоматически. Вы также можете добавлять или удалять процессы вручную.

Как сформировать список защищаемых процессов с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику Kaspersky Industrial CyberSecurity for Nodes и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне в списке разделов выберите **Постоянная защита компьютера → Защита от эксплойтов**.
4. Нажмите на кнопку **Настройка**.
5. На вкладке **Защищаемые процессы** выберите один из следующих вариантов защиты процессов от вторжения вредоносного кода:
   - **Автоматически определять защищаемые процессы**. При выборе этого варианта программа автоматически сформирует список защищаемых процессов.
   - **Защищать только процессы из списка ниже**. При выборе этого варианта вы можете выбрать процессы для защиты.
6. Если вы выбрали **Защищать только процессы из списка ниже**, вы можете изменить список защищаемых процессов, выполнив одно из следующих действий:
   - Если требуется, нажмите на кнопку **Добавить** и выберите процесс для добавления в список защищаемых процессов.
   - Если требуется, выберите процесс в списке и нажмите на кнопку **Удалить** для удаления процесса из сформированного списка защищаемых процессов.

     Кнопка **Удалить** становится активной после выбора одного или нескольких процессов из списка.
7. Сохраните внесенные изменения.

Как сформировать список защищаемых процессов с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от эксплойтов**.
3. В главном окне приложения нажмите **Свойства**.
4. На вкладке **Защищаемые процессы** выберите один из следующих вариантов защиты процессов от вторжения вредоносного кода:
   - **Автоматически определять защищаемые процессы**. При выборе этого варианта программа автоматически сформирует список защищаемых процессов.
   - **Защищать только процессы из списка ниже**. При выборе этого варианта вы можете выбрать процессы для защиты.

5. Если вы выбрали **Защищать только процессы из списка ниже**, вы можете изменить список защищаемых процессов, выполнив одно из следующих действий:

   - Если требуется, нажмите на кнопку **Добавить** и выберите процесс для добавления в список защищаемых процессов.

   - Если требуется, выберите процесс в списке и нажмите на кнопку **Удалить** для удаления процесса из сформированного списка защищаемых процессов.

     Кнопка **Удалить** становится активной после выбора одного или нескольких процессов из списка.

6. Сохраните внесенные изменения.

Как сформировать список защищаемых процессов с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Постоянная защита компьютера → Защита от эксплойтов** и нажмите на кнопку **Настроить.**

5. В блоке **Список защищаемых процессов** выберите один из следующих вариантов защиты процессов от вторжения вредоносного кода:

   - **Автоматически определять защищаемые процессы**. При выборе этого варианта программа автоматически сформирует список защищаемых процессов.

   - **Защищать только процессы из списка ниже**. При выборе этого варианта вы можете добавлять, изменять и удалять процессы для защиты.

6. Если вы выбрали **Защищать только процессы из списка ниже**, выполните одно из следующих действий:

   - Нажмите на кнопку **Добавить** и в открывшемся окне **Защищаемый процесс** выполните следующие действия:

     a. Установите флажок **Защищаемый процесс**.

     b. В поле **Имя процесса** укажите имя процесса.

     c. Сохраните внесенные изменения.

   - Если требуется, измените параметры процесса в списке защищаемых процессов. Для этого выполните следующие действия:

     a. Выберите процесс в списке защищаемых процессов.

     b. Нажмите на кнопку **Изменить**. Кнопка **Изменить** становится активной после выбора одного или нескольких процессов из списка.

     c. В открывшемся окне **Защищаемый процесс** установите или снимите флажок **Защищаемый процесс**.

d. При необходимости измените имя процесса в поле **Имя процесса**.

e. Сохраните внесенные изменения.

- Если требуется, удалите процесс из списка защищаемых процессов. Для этого выполните следующие действия:

  a. Выберите один или несколько процессов в списке защищаемых процессов.

  b. Нажмите на кнопку **Удалить**. Кнопка **Удалить** становится активной после выбора одного или нескольких процессов из списка.

7. Сохраните внесенные изменения.

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Industrial CyberSecurity for Nodes отменять действия, произведенные вредоносными приложениями в операционной системе.

Во время отката действий вредоносного приложения в операционной системе Kaspersky Industrial CyberSecurity for Nodes выполняет следующие действия:

- **Файловая активность**
  - удаляет исполняемые файлы, созданные вредоносным приложением на всех носителях, кроме сетевых дисков;
  - удаляет исполняемые файлы, созданные приложениями, в которые внедрилось вредоносное приложение;
  - восстанавливает измененные или удаленные вредоносным приложением файлы.

  Функциональность восстановления файлов имеет **ряд ограничений**.
  - Приложение восстанавливает файлы только на устройствах с файловой системой NTFS и FAT32.
  - Приложение восстанавливает файлы следующих расширений: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
  - Невозможно восстановить файлы, размещенные на сетевых дисках, а также на перезаписываемых CD/DVD-дисках.
  - Невозможно восстановить файлы, зашифрованные с помощью Encryption File System (EFS). Подробнее о работе EFS см. на сайте Microsoft.
  - Приложение не контролирует изменения файлов, выполненные процессами на уровне ядра операционной системы.
  - Приложение не контролирует изменения файлов, выполненные через сетевой интерфейс (например, файл размещен в папке общего доступа и процесс запущен удаленно с другого компьютера).
- **Реестровая активность**
  - удаляет разделы и ключи реестра, созданные вредоносным приложением.

  Kaspersky Industrial CyberSecurity for Nodes не восстанавливает измененные или удаленные вредоносным приложением разделы и ключи реестра.
- **Системная активность**
  - завершает процессы, которые запускало вредоносное приложение;
  - завершает процессы, в которые внедрялось вредоносное приложение.

Kaspersky Industrial CyberSecurity for Nodes не возобновляет процессы, которые остановило вредоносное приложение.

- **Сетевая активность**
  - запрещает сетевую активность вредоносного приложения;
  - запрещает сетевую активность тех процессов, в которые внедрялось вредоносное приложение.

Откат действий вредоносного приложения может быть запущен компонентом Постоянная защита файлов или при проверке по требованию.

Откат действий вредоносного приложения затрагивает строго ограниченный набор данных. Откат не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

Как включить или выключить компонент Откат вредоносных действий с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Постоянная защита компьютера**.
4. В блоке **Откат вредоносных действий** нажмите на кнопку **Настройка**.
5. Откроется окно **Откат вредоносных действий** на вкладке **Общие**.
6. Выполните одно из следующих действий:
   - Установите флажок **Откат вредоносных действий**, если вы хотите включить компонент Откат вредоносных действий.
   - Снимите флажок **Откат вредоносных действий**, если вы хотите выключить компонент Откат вредоносных действий.
7. В окне **Откат вредоносных действий** нажмите на кнопку **ОК**.
8. В окне **Свойства: <Имя политики>** нажмите на кнопку **ОК**.

Как включить или выключить компонент Откат вредоносных действий с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Постоянная защита компьютера**.
5. В блоке **Откат вредоносных действий** нажмите на кнопку **Настроить**.

6. Откроется окно **Откат вредоносных действий**.

7. Выполните одно из следующих действий:

   - Установите флажок **Откат вредоносных действий**, если вы хотите включить компонент Откат вредоносных действий.

   - Снимите флажок **Откат вредоносных действий**, если вы хотите выключить компонент Откат вредоносных действий.

8. В окне **Откат вредоносных действий** нажмите на кнопку **OK**.

9. В окне **<Имя политики>** нажмите на кнопку **Сохранить**.

Как включить или выключить компонент Откат вредоносных действий с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Постоянная защита компьютера → Откат вредоносных действий**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Откат вредоносных действий** на вкладке **Общие**.

3. Выполните одно из следующих действий:

   - Установите флажок **Откат вредоносных действий**, если вы хотите включить компонент Откат вредоносных действий.

   - Снимите флажок **Откат вредоносных действий**, если вы хотите выключить компонент Откат вредоносных действий.

4. В окне **Откат вредоносных действий** нажмите на кнопку **OK**.

Защита от шифрования

Компонент Защита от шифрования получает данные о действиях приложений на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы. Компонент Защита от шифрования использует шаблоны опасного поведения приложений. Если активность приложения совпадает с одним из шаблонов опасного поведения, Kaspersky Industrial CyberSecurity for Nodes выполняет выбранное ответное действие. Функциональность Kaspersky Industrial CyberSecurity for Nodes, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

Включение и выключение защиты локальных папок от шифрования

Как включить или выключить компонент Защита от шифрования в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Постоянная защита компьютера**.
4. В разделе **Защита от шифрования** нажмите **Настройка**.
5. Используйте флажок **Защита от шифрования**, чтобы включить или выключить компонент.
6. Перейдите на вкладку **Общие**.
7. Используйте флажок **Включить защиту локальных папок от внешнего шифрования**, чтобы включить или выключить функцию. Если флажок установлен, при обнаружении вредоносной активности Kaspersky Industrial CyberSecurity for Nodes производит действие, указанное ниже.
8. В блоке **Действие при обнаружении вредоносной активности** выберите нужное действие:
   - **Удалять**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в резервном хранилище.
   - **Блокировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes завершает работу этого приложения.
   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes добавляет информацию о вредоносной активности этого приложения в список активных угроз.
9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как включить или выключить компонент Защита от шифрования в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера → Защита от шифрования** и нажмите на кнопку **Настроить**.

   Откроется окно **Защита от шифрования**.
5. Используйте флажок **Включить защиту от шифрования**, чтобы включить или выключить компонент.
6. Перейдите на вкладку **Общие**.
7. Используйте флажок **Включить защиту локальных папок от внешнего шифрования**, чтобы включить или выключить функцию. Если флажок установлен, при обнаружении вредоносной активности Kaspersky Industrial CyberSecurity for Nodes производит действие, указанное ниже.
8. В блоке **При обнаружении внешнего шифрования папок общего доступа** выберите нужное действие:

   - **Удалять**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в резервном хранилище.
   - **Блокировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes завершает работу этого приложения.
   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes добавляет информацию о вредоносной активности этого приложения в список активных угроз.
9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как включить или выключить компонент Защита от шифрования в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера → Защита от шифрования**.
2. В панели результатов узла **Защита от шифрования** нажмите **Свойства**.

   Откроется окно **Свойства: Защита от шифрования**.
3. Установите флажок **Защита от шифрования**.
4. Перейдите на вкладку **Общие**.
5. Используйте флажок **Включить защиту локальных папок от внешнего шифрования**, чтобы включить или выключить функцию. Если флажок установлен, при обнаружении вредоносной активности Kaspersky Industrial CyberSecurity for Nodes производит действие, указанное ниже.

6. В блоке **При обнаружении внешнего шифрования папок общего доступа** выберите нужное действие:

   - **Удалять**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в резервном хранилище.

   - **Блокировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes завершает работу этого приложения.

   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность приложения, Kaspersky Industrial CyberSecurity for Nodes добавляет информацию о вредоносной активности этого приложения в список активных угроз.

7. Сохраните внесенные изменения.

Защита папок общего доступа от внешнего шифрования

Компонент обеспечивает отслеживание операций только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы системой EFS.

Функция защиты папок общего доступа от внешнего шифрования обеспечивает анализ активности в папках общего доступа. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Industrial CyberSecurity for Nodes выполняет выбранное действие.

При обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Industrial CyberSecurity for Nodes выполняет следующие действия:

- блокирует доступ на изменение файлов для сессии, которая инициировала вредоносную активность (файл доступен только на чтение);

- создает резервные копии подверженных изменению файлов;

- добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности;

- если при этом включен компонент Откат вредоносных действий, то выполняется восстановление измененных файлов из резервных копий.

Включение и выключение защиты папок общего доступа от внешнего шифрования

По умолчанию функция защиты папок общего доступа от внешнего шифрования включена и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для настройки функции вы можете сформировать область защиты, а также задать исключения, если требуется. По умолчанию приложение автоматически определяет папки общего доступа и отслеживает файловую активность во всех папках. При обнаружении попытки внешнего шифрования файлов в папках общего доступа Kaspersky Industrial CyberSecurity for Nodes блокирует сессию удаленного пользователя на один час (по умолчанию).

После установки Kaspersky Industrial CyberSecurity for Nodes функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

Как включить или выключить защиту папок общего доступа от внешнего шифрования в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Постоянная защита компьютера**.
4. В разделе **Защита от шифрования** нажмите **Настройка**.
5. Используйте флажок **Защита от шифрования**, чтобы включить или выключить компонент.
6. Перейдите на вкладку **Защита общих папок**.
7. Используйте флажок **Защищать папки общего доступа**, чтобы включить или выключить функцию.
8. В блоке **Защита папок общего доступа от внешнего шифрования** выберите нужное действие:
   - **Блокировать соединение на N мин**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Industrial CyberSecurity for Nodes блокирует доступ на изменение файлов (только чтение) для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов.

     Если включен компонент Откат вредоносных действий и выбран вариант **Блокировать соединение на N мин**, то выполняется восстановление измененных файлов из резервных копий.

   - **Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Industrial CyberSecurity for Nodes добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.
9. Если требуется сформируйте область защиты и задайте исключения.
10. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как включить или выключить защиту папок общего доступа от внешнего шифрования в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера → Защита от шифрования** и нажмите на кнопку **Настроить**.

   Откроется окно **Защита от шифрования**.
5. Используйте флажок **Включить защиту от шифрования**, чтобы включить или выключить компонент.
6. Перейдите на вкладку **Защита общих папок**.
7. Используйте флажок **Включить защиту папок общего доступа от внешнего шифрования**, чтобы включить или выключить функцию.
8. В блоке **Обнаружение внешнего шифрования** выберите нужное действие:

   - **Блокировать соединение**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Industrial CyberSecurity for Nodes блокирует доступ на изменение файлов (только чтение) для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов.

     Если включен компонент Откат вредоносных действий и выбран вариант **Блокировать соединение**, то выполняется восстановление измененных файлов из резервных копий.

   - **Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Industrial CyberSecurity for Nodes добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.
9. Если требуется сформируйте область защиты и задайте исключения.
10. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как включить или выключить защиту папок общего доступа от внешнего шифрования в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера → Защита от шифрования**.
2. В панели результатов узла **Защита от шифрования** нажмите **Свойства**.

   Откроется окно **Свойства: Защита от шифрования**.
3. Установите флажок **Защита от шифрования**.
4. Перейдите на вкладку **Защита общих папок**.
5. Используйте флажок **Защищать папки общего доступа**, чтобы включить или выключить функцию.

6. В блоке **Защита папок общего доступа от внешнего шифрования** выберите нужное действие:

   - **Блокировать соединение на N мин**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Industrial CyberSecurity for Nodes блокирует доступ на изменение файлов (только чтение) для сессии, которая инициировала вредоносную активность, и создает резервные копии измененных файлов.

     Если включен компонент Откат вредоносных действий и выбран вариант **Блокировать соединение на N мин**, то выполняется восстановление измененных файлов из резервных копий.

   - **Информировать**. Если выбран этот вариант, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Industrial CyberSecurity for Nodes добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз, добавляет запись в отчеты локального интерфейса приложения и отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

7. Если требуется сформируйте область защиты и задайте исключения.

8. Сохраните внесенные изменения.

Формирование области защиты

Область защиты – список путей к папкам общего доступа, в которых Kaspersky Industrial CyberSecurity for Nodes отслеживает файловую активность. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. По умолчанию приложение автоматически определяет папки общего доступа и отслеживает файловую активность во всех папках.

Исключение папки из области защиты позволит сократить количество ложных срабатываний, если в вашей организации используется шифрование данных при обмене файлами с помощью папок общего доступа. Например, компонент Защита от шифрования может создавать ложные срабатывания при работе пользователя с файлами с расширением ENC в папке общего доступа. Такая активность совпадает с шаблоном поведения, характерного для внешнего шифрования. Если вы зашифровали файлы в папке общего доступа для защиты данных, добавьте эту папку в исключения.

Вы также можете исключить компьютеры, попытки внешнего шифрования с которых не должны обрабатываться.

Как сформировать область защиты в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне свойств политики выберите **Постоянная защита компьютера**.

4. В разделе **Защита от шифрования** нажмите **Настройка**.

5. Используйте флажок **Защита от шифрования**, чтобы включить или выключить компонент.

6. Перейдите на вкладку **Защита общих папок**.

7. В блоке **Область защиты** нажмите на кнопку **Настроить**.

8. В открывшемся окне выберите режим **Только указанные общие папки**.

9. Нажмите на кнопку **Добавить**.

10. В открывшемся окне введите путь к папке общего доступа, которую вы хотите включить в область защиты (например, `C:\Share`).

    Для добавления папки общего доступа в область защиты используйте локальный путь.

11. Нажмите на кнопку **ОК**.

12. Если требуется, задайте исключения из области защиты:

    a. В блоке **Исключения** нажмите на кнопку **Настроить**.

    b. В открывшемся окне нажмите на кнопку **Добавить**.

    c. В открывшемся окне введите путь к папке или файлу.

    Используйте маски:

    - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

    - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением `txt` в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

    - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением `txt` и именем, состоящим из трех символов.

    Вы можете исключить объект из проверки, не удаляя его из списка объектов области защиты. Для этого снимите флажок рядом с ним.

13. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как сформировать область защиты в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Постоянная защита компьютера** → **Защита от шифрования** и нажмите на кнопку **Настроить**.

   Откроется окно **Защита от шифрования**.

5. Используйте флажок **Включить защиту от шифрования**, чтобы включить или выключить компонент.

6. Перейдите на вкладку **Защита общих папок**.

7. В блоке **Область защиты** выберите режим **Только указанные общие папки**.

8. Нажмите на кнопку **Добавить**.

9. В открывшемся окне введите путь к папке общего доступа, которую вы хотите включить в область защиты (например, `C:\Share`).

   > Для добавления папки общего доступа в область защиты используйте локальный путь.

10. Нажмите на кнопку **ОК**.

11. Если требуется, задайте исключения из области защиты:

    a. В блоке **Объект исключения** нажмите на кнопку **Добавить**.

    b. В открывшемся окне введите путь к папке или файлу.

    Используйте маски:

    - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

    - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

    - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

    Вы можете исключить объект из проверки, не удаляя его из списка объектов области защиты. Для этого снимите флажок рядом с ним.

12. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как сформировать область защиты в Консоли приложения

1. В окне свойств политики выберите **Постоянная защита компьютера**.

2. В разделе **Защита от шифрования** нажмите **Настройка**.

3. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера → Защита от шифрования**.

4. В панели результатов узла **Защита от шифрования** нажмите **Свойства**.

   Откроется окно **Свойства: Защита от шифрования**.

5. Используйте флажок **Защита от шифрования**, чтобы включить или выключить компонент.

6. Перейдите на вкладку **Защита общих папок**.

7. В блоке **Область защиты** нажмите на кнопку **Настроить**.

8. В открывшемся окне выберите режим **Только указанные общие папки**.

9. В блоке **Область защиты** нажмите на кнопку **Добавить**.

10. В открывшемся окне введите путь к папке общего доступа, которую вы хотите включить в область защиты (например, `C:\Share`).

    > Для добавления папки общего доступа в область защиты используйте локальный путь.

11. Нажмите на кнопку **OK**.

12. Если требуется, задайте исключения из области защиты:

    a. В блоке **Исключения** нажмите на кнопку **Настройка**.

    b. В открывшемся окне **Исключения по маске** нажмите на кнопку **Добавить**.

    c. В открывшемся окне введите путь к папке или файлу.

       Используйте маски:

       - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

       - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.

       - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

    Вы можете исключить объект из проверки, не удаляя его из списка объектов области защиты. Для этого снимите флажок рядом с ним.

13. Сохраните внесенные изменения.

Добавление доверенных компьютеров для внешнего шифрования данных

Если в вашей организации используется внешнее шифрование данных при обмене файлами, вам нужно сформировать список доверенных компьютеров. Kaspersky Industrial CyberSecurity for Nodes не отслеживает шифрование данных с доверенных компьютеров.

На защищаемых устройствах под управлением Windows XP или Windows Server 2003 Kaspersky Industrial CyberSecurity for Nodes будет отслеживать попытки шифрования папок общего доступа, даже если вы добавите удаленный компьютер в список доверенных компьютеров.

Для работы функциональности исключений адресов из защиты папок общего доступа от внешнего шифрования необходимо включить службу Аудит входа в систему. По умолчанию служба Аудит входа в систему выключена (подробную информацию о включении службы Аудит входа в систему см. на сайте корпорации Microsoft).

Функциональность исключений адресов из защиты папок общего доступа не работает на удаленном компьютере, если этот удаленный компьютер был включен до запуска Kaspersky Industrial CyberSecurity for Nodes. Вы можете перезагрузить этот удаленный компьютер после запуска Kaspersky Industrial CyberSecurity for Nodes, чтобы обеспечить работу функциональности исключений адресов из защиты папок общего доступа на этом удаленном компьютере.

Как добавить доверенный компьютер для внешнего шифрования данных в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Постоянная защита компьютера**.
4. В разделе **Защита от шифрования** нажмите **Настройка**.
5. Перейдите на вкладку **Защита общих папок**.
6. В блоке **Исключения по IP-адресам** нажмите на кнопку **Настроить**.
7. В открывшемся окне нажмите на кнопку **Добавить**.
8. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как добавить доверенный компьютер для внешнего шифрования данных в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера → Защита от шифрования** и нажмите на кнопку **Настроить**.

   Откроется окно **Защита от шифрования**.
5. Перейдите на вкладку **Защита общих папок**.
6. В блоке **Исключения** нажмите на кнопку **Добавить**.
7. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
8. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как добавить доверенный компьютер для внешнего шифрования данных в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера → Защита от шифрования**.
2. В панели результатов узла **Защита от шифрования** нажмите **Свойства**.

   Откроется окно **Свойства: Защита от шифрования**.
3. Перейдите на вкладку **Защита общих папок**.
4. В блоке **Исключения по IP-адресам** нажмите на кнопку **Настроить**.
5. В открывшемся окне нажмите на кнопку **Добавить**.
6. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
7. Сохраните внесенные изменения.

Настройка периода блокировки недоверенного компьютера

Недоверенный компьютер – удаленный компьютер, с которого ведется вредоносная активность или шифрование данных. По умолчанию Kaspersky Industrial CyberSecurity for Nodes блокирует сессию удаленного пользователя на один час. По истечении периода блокировки Kaspersky Industrial CyberSecurity for Nodes удаляет компьютер из списка заблокированных и восстанавливает доступ к папке общего доступа.

Как настроить период блокировки недоверенного компьютера в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Постоянная защита компьютера**.
4. В разделе **Защита от шифрования** нажмите **Настройка**.
5. Используйте флажок **Защита от шифрования**, чтобы включить или выключить компонент.
6. Перейдите на вкладку **Защита общих папок**.
7. В блоке **При обнаружении внешнего шифрования папок общего доступа** настройте период блокировки удаленного компьютера, с которого ведется вредоносная активность или шифрование данных.
8. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как настроить период блокировки недоверенного компьютера в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера** → **Защита от шифрования** и нажмите на кнопку **Настроить**.

   Откроется окно **Защита от шифрования**.
5. Используйте флажок **Включить защиту от шифрования**, чтобы включить или выключить компонент.
6. Перейдите на вкладку **Защита общих папок**.
7. В блоке **Обнаружение внешнего шифрования** настройте период блокировки удаленного компьютера, с которого ведется вредоносная активность или шифрование данных.
8. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как настроить период блокировки недоверенного компьютера в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера** → **Защита от шифрования**.
2. В панели результатов узла **Защита от шифрования** нажмите **Свойства**.

   Откроется окно **Свойства: Защита от шифрования**.
3. Установите флажок **Защита от шифрования**.
4. Перейдите на вкладку **Защита общих папок**.

5. В блоке **Защита папок общего доступа от внешнего шифрования** настройте период блокировки удаленного компьютера, с которого ведется вредоносная активность или шифрование данных.

6. Сохраните внесенные изменения.

Экспорт и импорт списка исключений из защиты папок общего доступа от внешнего шифрования

Вы можете экспортировать список исключений в файл формата XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных адресов. Также вы можете использовать функцию экспорта / импорта для резервного копирования списка исключений или для миграции списка на другой сервер.

Как экспортировать/импортировать список исключений в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне свойств политики выберите **Постоянная защита компьютера**.

4. В разделе **Защита от шифрования** нажмите **Настройка**.

5. Перейдите на вкладку **Защита общих папок**.

6. В блоке **Исключения по IP-адресам** нажмите на кнопку **Настроить**.

7. Для экспорта списка исключений выполните следующие действия:

   a. Если требуется, выберите исключения, которые вы хотите экспортировать.

   b. Нажмите на кнопку и выберите режим экспорта: экспортировать весь список исключений или только выбранные исключения.

   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список исключений в XML-файл.

8. Для импорта списка исключений выполните следующие действия:

   a. Нажмите на кнопку → **Импортировать**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   b. Откройте файл.

      Kaspersky Industrial CyberSecurity for Nodes импортирует исключения.

9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как экспортировать/импортировать список исключений в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера → Защита от шифрования** и нажмите на кнопку **Настроить**.

   Откроется окно **Защита от шифрования**.
5. Используйте флажок **Включить защиту от шифрования**, чтобы включить или выключить компонент.
6. Перейдите на вкладку **Защита общих папок**.
7. Для экспорта списка исключений в блоке **Исключения** выполните следующие действия:

   a. Если требуется, выберите исключения, которые вы хотите экспортировать.

   b. Нажмите на кнопку **Экспорт** и выберите режим экспорта: экспортировать весь список исключений или только выбранные исключения.

   c. Сохраните файл.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список исключений в XML-файл.
8. Для импорта списка исключений в блоке **Исключения** выполните следующие действия:

   a. Нажмите на кнопку **Импорт** и выберите режим импорта: добавить или заменить правила.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   c. Откройте файл.

      Kaspersky Industrial CyberSecurity for Nodes импортирует исключений в соответствии с выбранным режимом.
9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Защита от сетевых угроз

Компонент Защита от сетевых угроз выполняет проверку входящего сетевого трафика на наличие действий, характерных для сетевых атак. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, Kaspersky Industrial CyberSecurity for Nodes блокирует сетевую активность со стороны атакующего компьютера. Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах приложения. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей приложения.

По умолчанию задача Защита от сетевых угроз выполняется в режиме **Информировать**. В этом режиме Kaspersky Industrial CyberSecurity for Nodes проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, и фиксирует в журнале компонента события об обнаруженной активности, но не блокирует соединение с компьютерами, проявляющими такую активность, и не добавляет IP-адреса компьютеров в список заблокированных сетевых сессий.

В режиме **Блокировать** Kaspersky Industrial CyberSecurity for Nodes блокирует соединение с компьютерами, проявляющими активность, характерную для сетевых атак, а в некоторых случаях добавляет IP-адреса таких компьютеров в список заблокированных сетевых сессий.

Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

Kaspersky Industrial CyberSecurity for Nodes очищает список заблокированных узлов при перезапуске приложения или при изменении настроек Защиты от сетевых угроз.

Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

IP-адреса узлов, проявляющих активность, характерную для сетевых атак, удаляются из списка заблокированных узлов в следующих случаях:

- Приложение Kaspersky Industrial CyberSecurity for Nodes удалено.
- IP-адрес удален из списка заблокированных узлов вручную.
- Истек срок блокировки узла.
- Выключен режим **Блокировать**.

Для корректной работы Kaspersky Industrial CyberSecurity for Nodes на виртуальных машинах в инфраструктуре Microsoft Hyper-V необходимо выполнять настройку виртуальных коммутаторов Hyper-V после установки Kaspersky Industrial CyberSecurity for Nodes.

Включение и настройка общих параметров Защиты от сетевых угроз

Как включить и настроить Защиту от сетевых угроз в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности в сети**.
4. В блоке **Защита от сетевых угроз** нажмите на кнопку **Настройка**.
5. В открывшемся окне установите флажок **Защита от сетевых угроз**.
6. В разделе **Режим работы** выберите режим работы задачи:

   - **Блокировать**. Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, блокирует соединение с компьютерами, проявляющими такую активность, а в некоторых случаях добавляет IP-адреса компьютеров в список заблокированных сетевых сессий. Приложение также фиксирует в журнале компонента события об обнаруженной активности, характерной для сетевых атак.

   - **Информировать**. Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, но не блокирует соединение с компьютерами, проявляющими такую активность, и не добавляет IP-адреса компьютеров в список заблокированных сетевых сессий. Приложение фиксирует в журнале компонента события об обнаруженной активности, характерной для сетевых атак.

7. Используйте флажок **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение соответствующих атак.
8. Если необходимо, установите флажок **Блокировать атакующие устройства на N мин**.
9. В блоке **Защита от MAC-спуфинга** установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.
10. Если необходимо, добавьте исключения из блокирования.
11. Сохраните внесенные изменения.

Как включить и настроить Защиту от сетевых угроз в Консоли приложения

1. В дереве Консоли приложения выберите узел **Постоянная защита компьютера → Защита от сетевых угроз**.
2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Свойства: Защита от сетевых угроз**.
3. Установите флажок **Защита от сетевых угроз**.

4. В разделе **Режим работы** выберите режим работы задачи:

   - **Блокировать**. Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, блокирует соединение с компьютерами, проявляющими такую активность, а в некоторых случаях добавляет IP-адреса компьютеров в список заблокированных сетевых сессий. Приложение также фиксирует в журнале компонента события об обнаруженной активности, характерной для сетевых атак.

   - **Информировать**. Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, но не блокирует соединение с компьютерами, проявляющими такую активность, и не добавляет IP-адреса компьютеров в список заблокированных сетевых сессий. Приложение фиксирует в журнале компонента события об обнаруженной активности, характерной для сетевых атак.

5. Используйте флажок **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение соответствующих атак.

6. Если необходимо, установите флажок **Блокировать атакующие устройства на N мин**.

7. В блоке **Защита от MAC-спуфинга** установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.

8. Если необходимо, добавьте исключения из блокирования.

9. Сохраните внесенные изменения.

Как включить и настроить Защиту от сетевых угроз в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Контроль активности в сети** → **Защита от сетевых угроз**.

5. На вкладке **Общие** установите флажок **Включить Защиту от сетевых угроз**.

6. Выберите режим работы задачи:

   - **Блокировать**. Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, блокирует соединение с компьютерами, проявляющими такую активность, а в некоторых случаях добавляет IP-адреса компьютеров в список заблокированных сетевых сессий. Приложение также фиксирует в журнале компонента события об обнаруженной активности, характерной для сетевых атак.

   - **Информировать**. Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, но не блокирует соединение с компьютерами, проявляющими такую активность, и не добавляет IP-адреса компьютеров в список заблокированных сетевых сессий. Приложение фиксирует в журнале компонента события об обнаруженной активности, характерной для сетевых атак.

7. Используйте флажок **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение соответствующих атак.

8. Если необходимо, установите флажок **Блокировать атакующие устройства на N мин**.
9. Установите или снимите флажок **Включить защиту от атак с подменой MAC-адресов**.
10. Если необходимо, добавьте исключения из блокирования.
11. Сохраните внесенные изменения.

Создание исключения из блокирования

Kaspersky Industrial CyberSecurity for Nodes может распознать сетевую атаку и заблокировать безопасное сетевое соединение, по которому передается большое количество пакетов (например, от камер наблюдения). Для работы с доверенными устройствами вы можете добавить IP-адреса этих устройств в список исключений. Также вы можете выбрать протокол и порт, по которым передаются данные, чтобы разрешить отдельную сетевую активность.

Выбор протокола и портов для исключений добавлен в Kaspersky Industrial CyberSecurity for Nodes версии 4.0. Убедитесь, что приложение и плагин управления обновлены до версии 4.0 или выше. Если вы используете более раннюю версию приложения или плагина управления, Kaspersky Industrial CyberSecurity for Nodes разрешает активность компьютеров только по IP-адресу.

Как создать исключение из блокирования в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности в сети**.
4. В блоке **Защита от сетевых угроз** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от сетевых угроз**.
5. Перейдите на вкладку **Исключения**.
6. Установите флажок **Не контролировать адреса, указанные в исключениях**, чтобы Kaspersky Industrial CyberSecurity for Nodes не проверяло входящий сетевой трафик со стороны исключенных IP-адресов.
7. Нажмите на кнопку **Добавить**.
8. В окне **Исключение** введите IP-адрес устройства, сетевые атаки с которого не должны блокироваться.
9. Если требуется, выберите протокол и укажите порты, по которым передаются данные.
10. Нажмите на кнопку **OK**.
11. Выполните пункты c-f для каждого добавляемого исключения.
12. Сохраните внесенные изменения.

Как создать исключение из блокирования в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Контроль активности в сети → Защита от сетевых угроз** и нажмите на кнопку **Настроить**.
5. Перейдите на вкладку **Исключения**.
6. Установите флажок **Не контролировать IP-адреса, указанные в исключениях**, чтобы Kaspersky Industrial CyberSecurity for Nodes не проверяло входящий сетевой трафик со стороны исключенных IP-адресов.
7. Нажмите на кнопку **Добавить**.
8. В окне **Добавление исключения** введите IP-адрес устройства, сетевые атаки с которого не должны блокироваться.
9. Если требуется, выберите протокол и укажите порты, по которым передаются данные.
10. Нажмите на кнопку **OK**.
11. Выполните пункты c-f для каждого добавляемого исключения.
12. Сохраните внесенные изменения.

Как создать исключение из блокирования в Консоли приложения

1. В дереве Консоли приложения выберите узел **Постоянная защита компьютера → Защита от сетевых угроз**.
2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Свойства: Защита от сетевых угроз**.
3. Перейдите на вкладку **Исключения**.
4. Установите флажок **Не контролировать адреса, указанные в исключениях**, чтобы Kaspersky Industrial CyberSecurity for Nodes не проверяло входящий сетевой трафик со стороны исключенных IP-адресов.
5. Нажмите на кнопку **Добавить**.
6. В окне **Исключение** введите IP-адрес устройства, сетевые атаки с которого не должны блокироваться.
7. Если требуется, выберите протокол и укажите порты, по которым передаются данные.
8. Нажмите на кнопку **OK**.
9. Выполните пункты c-f для каждого добавляемого исключения.
10. Сохраните внесенные изменения.

Экспорт и импорт списка исключений из защиты папок общего доступа от внешнего шифрования

Вы можете экспортировать список исключений в файл формата XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных адресов. Также вы можете использовать функцию экспорта / импорта для резервного копирования списка исключений или для миграции списка на другой сервер.

Как экспортировать/импортировать список исключений в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности в сети**.
4. В блоке **Защита от сетевых угроз** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от сетевых угроз**.
5. Перейдите на вкладку **Исключения**.
6. Для экспорта списка исключений выполните одно из следующих действий:

   - Выберите с помощью флажков исключения, которые вы хотите экспортировать, нажмите на стрелку и выберите из выпадающего списка вариант **Экспортировать выбранное**.
   - Нажмите на стрелку и выберите из выпадающего списка вариант **Экспортировать**, чтобы экспортировать весь список исключений.

     Kaspersky Industrial CyberSecurity for Nodes сохранит в стандартной папке загрузок файл networkExclusions.xml.
7. Для импорта списка исключений выполните следующие действия:

   a. Нажмите на стрелку и выберите вариант **Импортировать**.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   c. Откройте файл.

   Если на компьютере уже есть список исключений, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.
8. Сохраните внесенные изменения.

Как экспортировать/импортировать список исключений в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Постоянная защита компьютера** → **Защита от сетевых угроз** и нажмите на кнопку **Настроить**.

5. В открывшемся окне перейдите на вкладку **Исключения**.

6. Для экспорта списка исключений выполните следующие действия:

   a. Если требуется, выберите исключения, которые вы хотите экспортировать.

   b. Нажмите на кнопку **Экспорт** и выберите режим экспорта: экспортировать весь список исключений или только выбранные исключения.

   c. Нажмите на кнопку **Экспорт**.

      Kaspersky Industrial CyberSecurity for Nodes сохранит в стандартной папке загрузок файл networkExclusions.xml.

7. Для импорта списка исключений выполните следующие действия:

   a. Нажмите на кнопку **Импорт** и выберите режим импорта: **Добавить к существующим записям** или **Заменить существующие записи**.

   b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

   c. Откройте файл.

      Kaspersky Industrial CyberSecurity for Nodes импортирует исключений в соответствии с выбранным режимом.

8. Сохраните внесенные изменения.

AMSI-защита

В ходе выполнения задачи AMSI-защита Kaspersky Industrial CyberSecurity for Nodes контролирует выполнение скриптов, созданных по технологиям Microsoft Windows (Active Scripting), например скриптов VBScript или JScript. Программа может также обрабатывать скрипты PowerShell и скрипты, работающие в программах Microsoft Office в операционных системах с установленным компонентом Antimalware Scan Interface (AMSI).

Технология AMSI позволяет интегрировать программы и службы с любым установленным на устройстве антивирусным программным обеспечением, чтобы это программное обеспечение могло перехватывать и проверять все исполняемые скрипты. Более подробная информация о технологии AMSI приведена на сайте Microsoft.

В настройках компонента вы можете разрешить или запретить исполнение опасных скриптов. Если приложение Kaspersky Industrial CyberSecurity for Nodes признало скрипт опасным, оно выполняет выбранное вами действие: блокирует или разрешает выполнение скрипта. Если выбрано действие **Блокировать**, приложение блокирует выполнение опасных скриптов и разрешает выполнение остальных скриптов.

Kaspersky Industrial CyberSecurity for Nodes поддерживает технологию AMSI в операционных системах Microsoft Windows 10 и Microsoft Windows Server 2016 и более поздних версий.

Включение и выключение AMSI-защиты

Как включить или выключить AMSI-защиту с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Постоянная защита компьютера**.
4. В блоке **AMSI-защита** нажмите на кнопку **Настройка**.

   Откроется окно **AMSI-защита** на вкладке **Общие**.
5. Выполните одно из следующих действий:
   - Установите флажок **AMSI-защита**, если вы хотите включить AMSI-защиту.
   - Снимите флажок **AMSI-защита**, если вы хотите выключить AMSI-защиту.
6. Сохраните внесенные изменения.

Как включить или выключить AMSI-защиту с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Постоянная защита компьютера → AMSI-защита**.
2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **AMSI-защита** на вкладке **Общие**.

3. Выполните одно из следующих действий:

   - Установите флажок **AMSI-защита**, если вы хотите включить AMSI-защиту.
   - Снимите флажок **AMSI-защита**, если вы хотите выключить AMSI-защиту.

4. В окне **AMSI-защита** нажмите на кнопку **OK**.

Как включить или выключить AMSI-защиту с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Постоянная защита компьютера**.
5. В блоке **AMSI-защита** нажмите на кнопку **Настроить**.

   Откроется окно **AMSI-защита**.
6. Выполните одно из следующих действий:

   - Установите флажок **AMSI-защита**, если вы хотите включить AMSI-защиту.
   - Снимите флажок **AMSI-защита**, если вы хотите выключить AMSI-защиту.

7. Сохраните внесенные изменения.

Настройка параметров AMSI-защиты

Как настроить параметры AMSI-защиты с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Постоянная защита компьютера**.
4. В блоке **AMSI-защита** нажмите на кнопку **Настройка**.

   Откроется окно **AMSI-защита** на вкладке **Общие**.
5. Выберите действие, которое выполняет Kaspersky Industrial CyberSecurity for Nodes при запуске опасных скриптов:

   - **Информировать**. Приложение разрешает выполнение предположительно опасных скриптов. В журнале выполнения задачи регистрируется соответствующее событие.
   - **Блокировать**. Приложение запрещает выполнение предположительно опасных скриптов.

6. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.

7. В блоке **Ограничение по размеру** выполните одно из следующих действий:

   - Чтобы запретить компоненту AMSI-защита распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла (МБ)** укажите нужное значение. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.

   - Чтобы разрешить компоненту AMSI-защита распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Компонент AMSI-защита проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

8. В окне **AMSI-защита** нажмите на кнопку **OK**.

9. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Как настроить параметры AMSI-защиты с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Постоянная защита компьютера → AMSI-защита**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **AMSI-защита** на вкладке **Общие**.

3. Выберите действие, которое выполняет Kaspersky Industrial CyberSecurity for Nodes при запуске опасных скриптов:

   - **Информировать**. Приложение разрешает выполнение предположительно опасных скриптов. В журнале выполнения задачи регистрируется соответствующее событие.

   - **Блокировать**. Приложение запрещает выполнение предположительно опасных скриптов.

4. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.

5. В блоке **Ограничение по размеру** выполните одно из следующих действий:

   - Чтобы запретить компоненту AMSI-защита распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла (МБ)** укажите нужное значение. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.

   - Чтобы разрешить компоненту AMSI-защита распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Компонент AMSI-защита проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

6. В окне **AMSI-защита** нажмите на кнопку **OK**.

Как настроить параметры AMSI-защиты с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Постоянная защита компьютера**.
5. В блоке **AMSI-защита** нажмите на кнопку **Настроить**.

   Откроется окно **AMSI-защита**.
6. Выберите действие, которое выполняет Kaspersky Industrial CyberSecurity for Nodes при запуске опасных скриптов:

   - **Информировать**. Приложение разрешает выполнение предположительно опасных скриптов. В журнале выполнения задачи регистрируется соответствующее событие.
   - **Блокировать**. Приложение запрещает выполнение предположительно опасных скриптов.
7. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.
8. В блоке **Ограничение по размеру** выполните одно из следующих действий:

   - Чтобы запретить компоненту AMSI-защита распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла (МБ)** укажите нужное значение. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.
   - Чтобы разрешить компоненту AMSI-защита распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Компонент AMSI-защита проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
9. В окне **AMSI-защита** нажмите на кнопку **OK**.
10. В окне **<Имя политики>** нажмите на кнопку **Сохранить**.

Контроль запуска программ

Компонент Контроль запуска программ Kaspersky Industrial CyberSecurity for Nodes позволяет защитить устройство от несанкционированного запуска приложений. Контроль запуска программ работает по принципу запрета по умолчанию: все приложения, не указанные в качестве разрешенных в параметрах компонента, автоматически блокируются. Вы можете разрешить запуск приложений, создав для них разрешающие правила компонента.

Если правила Контроля запуска программ сформированы максимально полно, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск всех новых, не проверенных администратором локальной сети организации приложений, но обеспечивает работоспособность операционной системы и проверенных приложений, которые нужны пользователям для выполнения должностных обязанностей. Вы можете получать информацию о приложениях, установленных на защищаемых устройствах, с помощью задачи *Формирование правил контроля запуска программ*.

Если компонент Контроль запуска программ включен, Kaspersky Industrial CyberSecurity for Nodes перехватывает каждое событие операционной системы о запросе на создание процесса, возникающее при запуске исполняемого файла на защищаемом устройстве. Далее приложение собирает информацию о запускаемом исполняемом файле, скрипте или пакете MSI и сопоставляет ее с условиями срабатывания правил Контроля запуска программ. Если все условия хотя бы одного разрешающего правила выполнены, Kaspersky Industrial CyberSecurity for Nodes разрешает запуск приложения. В случае, если запускаемое приложение не подходит под условия разрешающих правил, или сработало запрещающее правило, Kaspersky Industrial CyberSecurity for Nodes блокирует запуск приложения путем отмены создания процесса.

Все попытки запуска приложений фиксируются в журнале работы компонента.

Компонент Контроль запуска программ может работать в одном из двух режимов:

- **Блокировать**. Kaspersky Industrial CyberSecurity for Nodes контролирует запуск приложений с помощью правил контроля запуска программ. Область применения правил контроля запуска программ указана в общих настройках компонента Контроль запуска программ. Если приложение удовлетворяет правилам контроля запуска программ, но ни одно из этих правил не соответствует области применения правил контроля запуска программ, то запуск таких приложений будет запрещен.

  Запуск приложений, которые не подпадают под действие правил контроля запуска программ, запрещен.

  > Компонент Контроль запуска программ нельзя запустить в активном режиме, если не создано ни одно правило контроля запуска программ или если для одного защищаемого устройства создано более 65535 правил контроля запуска программ.

- **Информировать**. Kaspersky Industrial CyberSecurity for Nodes разрешает запуск всех приложений. При этом выполняется только запись информации обо всех запусках приложений, правилах, под действие которых подпадают запущенные приложения, и действиях, которые были бы выполнены, если бы задача выполнялась в режиме **Блокировать**. Этот режим установлен по умолчанию.

> При создании правил контроля запуска программ рекомендуем убедиться, что они разрешают запуск приложений операционной системы.

Kaspersky Industrial CyberSecurity for Nodes также перехватывает процессы, запущенные в рамках подсистемы Windows для Linux (за исключением скриптов, запущенных из оболочки UNIX™, или командных интерпретаторов). Для данных целей компонент Контроль запуска программ применяет действия, указанные в текущих настройках. Задача *Формирование правил контроля запуска программ* фиксирует запуск приложений и создает соответствующие правила для приложений, работающих в рамках Windows Subsystem для Linux.

О правилах контроля запуска программ

Как работают правила контроля запуска программ

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.

  Правила контроля запуска программ могут разрешать или запрещать запуск приложений. Соответственно, они называются *разрешающими* или *запрещающими*.

- Область применения правила.

  Правила контроля запуска программ могут применяться к *исполняемым файлам*, *скриптам* и *пакетам MSI*.

- Условия срабатывания правила.

  Правила контроля запуска программ регулируют запуск файлов, удовлетворяющих хотя бы одному из условий срабатывания, указанных в параметрах правила. Например, исполняемые файлы подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256*, расположены по указанному *пути*, соответствуют указанным аргументам *командной строки*. Требуется добавить хотя бы одно условие срабатывания правила. В противном случае правило контроля запуска программ не будет добавлено.

- Исключения из правила.

  Вы можете задать исключения для правила контроля запуска программ, которые могут быть основаны на тех же критериях, что и условия срабатывания правила. Исключения из правила контроля запуска программ могут понадобиться для определенных разрешающих правил: например, если требуется разрешить пользователям запуск приложений по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

- Пользователь или группа пользователей.

  Правила контроля запуска программ контролируют запуск указанных программ указанными пользователями и/или группами пользователей.

При создании правил контроля запуска программ рекомендуем убедиться, что новые правила разрешают запуск приложений операционной системы.

Управление правилами контроля запуска программ

Вы можете выполнять следующие действия с правилами контроля запуска программ:

- Добавлять вручную.

- Формировать и добавлять правила автоматически.

- Удалять.
- Импортировать и экспортировать.
- Фильтровать список правил.

О Контроле пакетов установки

Формирование правил контроля запуска программ может усложниться, если вы хотите контролировать распространение программ. Например, на защищаемых устройствах, где происходит регулярное автоматическое обновление установленных программ. В этом случае требуется обновлять списки разрешающих правил после каждого обновления программ, чтобы в параметрах компонента Контроль запуска программ учитывались новые файлы, созданные в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программ можно использовать Контроль пакетов установки.

Пакет установки (далее также *пакет*) представляет собой одну или несколько программ, устанавливаемых на защищаемое устройство. В пакете установки также могут содержаться обновления и отдельные команды.

Модуль Контроль пакетов установки реализован в виде дополнительного списка исключений. После добавления пакета установки в список он становится доверенным. Для доверенных пакетов разрешается распаковка, а для программ, установленных или обновленных из доверенных пакетов, разрешается автоматический запуск. Извлеченные файлы могут наследовать признак доверенности от основного пакета установки. *Основной пакет установки* – это пакет, добавленный в список исключений контроля пакетов установки и ставший доверенным пакетом.

Kaspersky Industrial CyberSecurity for Nodes контролирует только полный цикл распространения программ и не может корректно обработать запуск файлов, измененных доверенным пакетом, если при первом запуске пакета был выключен Контроль пакетов установки или не был установлен Контроль запуска программ.

Для использования Контроля пакетов установки в общих настройках компонента Контроль запуска программ необходимо включить функцию **Использовать правила для исполняемых файлов**.

Кеш распространения программ

Kaspersky Industrial CyberSecurity for Nodes использует динамически формируемый кеш распространения программ (далее также кеш распространения) для связи между доверенными пакетами и файлами, созданными во время распространения программ. При первом запуске пакета Kaspersky Industrial CyberSecurity for Nodes обнаруживает все файлы, созданные этим пакетом во время распространения программ, и сохраняет контрольные суммы и пути файлов в кеше распространения. Затем по умолчанию разрешается запуск всех файлов, данные о которых сохранены в кеше распространения.

Кеш распространения нельзя просматривать, удалять и изменять вручную через пользовательский интерфейс. Kaspersky Industrial CyberSecurity for Nodes самостоятельно наполняет его, а также контролирует его актуальность.

Кеш распространения можно экспортировать в конфигурационный файл (в формате XML) и удалять с помощью командной строки.

Kaspersky Industrial CyberSecurity for Nodes обновляет кеш распространения раз в сутки. При изменении контрольной суммы разрешенного ранее файла приложение удаляет запись для этого файла из кеша распространения. При активном режиме работы компонента Контроль запуска программ дальнейшие попытки запуска этого файла будут заблокированы. При изменении полного пути к разрешенному ранее файлу последующие попытки запустить этот файл не блокируются, поскольку контрольная сумма хранится в кеше распространения.

Обработка извлеченных файлов

Извлеченные файлы и пакеты, созданные основным доверенным пакетом установки (первого уровня вложенности), наследуют признак доверенности, поскольку их контрольные суммы добавляются в кеш распространения, когда пакет установки из списка исключений открывается в первый раз. Таким образом, сам пакет установки и все извлеченные из него файлы являются доверенными.

Например, если пакет test.msi, содержащий несколько пакетов и программ, добавлен в список исключений и включена функция **Присвоить признак доверенного пакета установки дочерним исполняемым файлам**, то все пакеты и приложения, содержащиеся в пакете test.msi, можно распаковать и запустить, даже если они содержат другие вложенные файлы. Это соблюдается для всех уровней вложенности.

Если пакет test.msi добавлен в список исключений, а функция **Присвоить признак доверенного пакета установки дочерним исполняемым файлам** выключена, приложение присваивает признак доверенности только пакетам и исполняемым файлам, извлеченным непосредственно из основного доверенного пакета (первого уровня вложенности). Контрольные суммы этих файлов хранятся в кеше распространения. Все файлы второго и следующих уровней вложенности блокируются согласно принципу запрета по умолчанию.

Извлеченные файлы сохраняют признак доверенности при перезагрузке операционной системы.

Чтобы отменить признак наследования для всех извлеченных файлов, необходимо удалить кеш распространения и выключить функцию **Присвоить признак доверенного пакета установки дочерним исполняемым файлам** перед следующим запуском доверенного пакета установки.

Работа со списком правил контроля запуска программ

Список доверенных пакетов Контроля пакетов установки – это список исключений, который дополняет, но не заменяет основной список правил контроля запуска программ.

Запрещающие правила контроля запуска программ имеют абсолютный приоритет: распаковка доверенного пакета или запуск созданных и измененных им файлов будут заблокированы, если такие пакеты и файлы подпадают под запрещающие правила контроля запуска программ.

Исключения Контроля пакетов установки учитываются и для доверенных пакетов, и для созданных и измененных ими файлов, если к таким пакетам и файлам не применяются запрещающие правила из списка правил контроля запуска программ.

О формировании правил контроля запуска программ

Вы можете создать списки правил контроля запуска программ с помощью задач и политик Kaspersky Security Center одновременно для всех защищаемых устройств и групп защищаемых устройств в сети организации. Рекомендуем использовать перечисленные сценарии, если в сети организации нет эталонной машины, и вы не можете сформировать список разрешающих правил на основе программ, установленных на такой эталонной машине.

Вы можете запустить задачу *Формирование правил контроля запуска программ* локально с помощью Консоли приложения для создания списка правил на основе программ, запущенных на отдельном защищаемом устройстве.

Вы можете создавать списки правил контроля запуска программ на стороне Kaspersky Security Center двумя способами:

- С помощью групповой задачи *Формирование правил контроля запуска программ*.

  Задача *Формирование правил контроля запуска программ* в зависимости от заданных настроек может собирать данные о программах, запущенных на защищаемых устройствах, а также об исполняемых файлах и файлах скриптов, расположенных в указанных областях. На основании собранных данных задача формирует список разрешающих правил для компонента Контроль запуска программ.

  Вы можете настроить автоматический импорт сформированных правил в список правил компонента Контроль запуска программ или импортировать сформированные правила вручную.

  Рекомендуем использовать этот сценарий, если требуется быстро сформировать списки правил контроля запуска программ. Рекомендуем настраивать запуск задачи *Формирование правил контроля запуска программ* по расписанию, только если область применения разрешающих правил включает папки, содержащие заведомо безопасные файлы.

- На основе отчета о событиях компонента Контроль запуска программ в режиме *Информировать*, сформированного в Kaspersky Security Center.

  В рамках этого сценария Kaspersky Industrial CyberSecurity for Nodes не блокирует запуск приложений. Когда компонент Контроль запуска программ работает в режиме *Информировать*, все разрешенные и запрещенные запуски программ на всех защищаемых устройствах сети регистрируются на вкладке **События** в рабочей области узла Сервера администрирования Kaspersky Security Center. С помощью отчетов в Kaspersky Security Center формируется единый список событий о заблокированных запусках программ.

  Вам нужно, чтобы за время работы компонента выполнились все возможные сценарии работы защищаемых устройств и групп защищаемых устройств и хотя бы одна перезагрузка. Далее вы можете импортировать данные о запусках программ из сохраненного отчета о событиях Kaspersky Security Center (файла в формате TXT) и сформировать на основе этих данных разрешающие правила контроля запуска таких программ.

  Рекомендуем использовать этот сценарий, если в сети организации имеется большое количество защищаемых устройств разных типов с различным набором установленных программ.

- На основе событий блокировки запуска программ, полученных через Kaspersky Security Center, без создания и импорта конфигурационного файла.

  Чтобы воспользоваться данной возможностью, компонент Контроль запуска программ на защищаемом устройстве должна находиться под управлением активной политики Kaspersky Security Center. При этом все события на защищаемом устройстве передаются на Сервер администрирования.

Рекомендуем обновить список правил при изменении состава программ, установленных на управляемых компьютерах в сети (например, при установке обновлений или переустановке операционной системы). Рекомендуем сформировать обновленный список правил, запустив задачу *Формирование правил контроля запуска программ* или компонент Контроль запуска программ в режиме *Информировать* на защищаемых устройствах тестовой группы администрирования. Тестовая группа администрирования включает защищаемые устройства, необходимые для тестового запуска новых программ перед их установкой на остальные защищаемые устройства сети.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа запускаемых программ на защищаемом устройстве. Чтобы при формировании списка правил учесть все используемые в сети программы, рекомендуем запускать задачу *Формирование правил контроля запуска программ* и компонент Контроль запуска программ в режиме *Информировать* на эталонной машине.

Перед формированием разрешающих правил на основе программ, запущенных на эталонной машине организации, убедитесь, что эталонная машина защищена и на ней нет вредоносных программ.

Перед добавлением разрешающих правил выберите один из доступных режимов применения правил. В списке правил политики Kaspersky Security Center отображаются только правила, заданные в этой политике, вне зависимости от режима применения правил. Список локальных правил включает все применимые правила: локальные и добавленные через политику.

Включение и настройка общих параметров Контроля запуска программ

Как включить и настроить общие параметры Контроля запуска программ с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности на компьютерах**.
4. В блоке **Контроль запуска программ** нажмите на кнопку **Настройка**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.
5. Установите флажок **Контроль запуска программ**.

6. В блоке **Режим работы для блокирующих правил** выберите режим работы компонента:

   - **Блокировать**. Kaspersky Industrial CyberSecurity for Nodes применяет все созданные правила контроля запуска программ.

   - **Информировать**. Kaspersky Industrial CyberSecurity for Nodes не использует правила контроля запуска программ, а только фиксирует в журнале работы компонента информацию о запусках программ. Разрешен запуск всех приложений. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале работы компонента.

7. Настройте параметры компонента (см. таблицу ниже).

8. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes немедленно применит новые значения параметров компонента. Данные о дате и времени изменения параметров, а также значения параметров до и после изменения будут сохранены в журнале системного аудита.

Как включить и настроить общие параметры Контроля запуска программ с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Контроль компьютера** → **Контроль запуска программ**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

3. Установите флажок **Контроль запуска программ**.

4. В блоке **Режим работы для блокирующих правил** выберите режим работы компонента:

   - **Блокировать**. Kaspersky Industrial CyberSecurity for Nodes применяет все созданные правила контроля запуска программ.

   - **Информировать**. Kaspersky Industrial CyberSecurity for Nodes не использует правила контроля запуска программ, а только фиксирует в журнале работы компонента информацию о запусках программ. Разрешен запуск всех приложений. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале работы компонента.

5. Настройте параметры компонента (см. таблицу ниже).

6. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes немедленно применит новые значения параметров компонента. Данные о дате и времени изменения параметров, а также значения параметров до и после изменения будут сохранены в журнале системного аудита.

Как включить и настроить общие параметры Контроля запуска программ с помощью Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Контроль активности на компьютерах**.

5. В блоке **Контроль запуска программ** нажмите на кнопку **Настроить**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

6. Установите флажок **Включить Контроль запуска программ**.

7. В блоке **Режим работы для блокирующих правил** выберите режим работы компонента:

   - **Блокировать**. Kaspersky Industrial CyberSecurity for Nodes применяет все созданные правила контроля запуска программ.

   - **Информировать**. Kaspersky Industrial CyberSecurity for Nodes не использует правила контроля запуска программ, а только фиксирует в журнале работы компонента информацию о запусках программ. Разрешен запуск всех приложений. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале работы компонента.

8. Настройте параметры компонента (см. таблицу ниже).

9. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes немедленно применит новые значения параметров компонента. Данные о дате и времени изменения параметров, а также значения параметров до и после изменения будут сохранены в журнале системного аудита.

Общие параметры Контроля запуска программ

Параметр	Описание
Обрабатывать повторные запуски контролируемых приложений по схеме обработки первого запуска	Функция включает или выключает контроль повторного запуска приложений на основе информации о событиях, хранящейся в кеше. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает последующие запуски приложений в зависимости от заключения компонента насчет первого запуска приложений. Например, если первый запуск приложения был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этого приложения будет разрешен без повторной проверки. Если приложение установлено на компьютере под управлением операционной системы Windows XP, при взаимодействии с файлами через Проводник заключения о первом запуске приложений могут переписываться, что приводит к неправильной работе функции. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes проверяет приложение при каждой попытке его запуска.
Запрещать запуск командных интерпретаторов без команды к исполнению	Если функция включена, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск командного интерпретатора при выполнении одного из условий: • Запуск командного интерпретатора запрещен правилами контроля запуска программ. • Командный интерпретатор запускается без параметров. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило контроля запуска программ. Если применимо разрешающее правило контроля запуска программ, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее. Kaspersky Industrial CyberSecurity for Nodes контролирует запуск следующих командных интерпретаторов: • cmd.exe; • powershell.exe; • python.exe; • perl.exe; • wscript.exe. По умолчанию функция выключена.

Параметр	Описание
Использовать правила для исполняемых файлов	Функция включает или выключает контроль запуска исполняемых файлов. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает запуск исполняемых файлов с помощью правил контроля запуска программ. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes не контролирует запуск исполняемых файлов с помощью правил контроля запуска программ. Запуск исполняемых файлов разрешен. По умолчанию функция включена.
Контролировать загрузку DLL-модулей	Контроль загрузки DLL-модулей может влиять на производительность операционной системы. Функция доступна, если включена функция **Использовать правила для исполняемых файлов**. Функция включает или выключает контроль загрузки DLL-модулей. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает загрузку DLL-модулей с помощью правил контроля запуска программ. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes не контролирует загрузку DLL-модулей с помощью правил контроля запуска программ. Загрузка DLL-модулей разрешена. По умолчанию функция выключена.
Использовать правила для скриптов и пакетов MSI	Функция включает или выключает контроль запуска скриптов и пакетов MSI. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает запуск скриптов и пакетов MSI с помощью правил контроля запуска программ. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не контролирует запуск скриптов и пакетов MSI с помощью правил контроля запуска программ. Запуск скриптов и пакетов MSI разрешен. По умолчанию функция включена.
Игнорировать отсутствие метки времени в подписи при проверке сертификата	Если функция включена, Kaspersky Industrial CyberSecurity for Nodes разрешает запуск приложений, подписанных сертификатами, срок действия которых истек или не определен. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes запрещает запуск приложений, подписанных сертификатами, срок действия которых истек или не определен. По умолчанию функция выключена.

Настройка Контроля пакетов установки

Как настроить Контроль пакетов установки с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности на компьютерах**.
4. В блоке **Контроль запуска программ** нажмите на кнопку **Настройка**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.
5. Выберите вкладку **Контроль пакетов установки**.

6. Включите функцию **Автоматически разрешать распространение с помощью указанных приложений и пакетов установки**. Функция автоматически создает исключения для всех файлов, запущенных с помощью указанных в списке исполняемых файлов и пакетов установки.

   Вы можете включить функцию **Автоматически разрешать распространение с помощью указанных приложений и пакетов установки**, если на вкладке **Общие** включена функция **Использовать правила для исполняемых файлов**.

7. Если необходимо, выключите функцию **Всегда разрешать распространение приложений с помощью установщика Windows**. Функция автоматически создает исключения для всех файлов, запущенных с помощью установщика Windows.

   Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

8. Если необходимо, включите функцию **Всегда разрешать распространение приложений через SCCM с помощью фоновой интеллектуальной службы передачи**. Функция разрешает распространение программного обеспечения с помощью решения System Center Configuration Manager.

   Если функция включена, Kaspersky Industrial CyberSecurity for Nodes разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Приложение разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service). Приложение контролирует запуск исполняемых файлов с расширениями .EXE и .MSI.

   Kaspersky Industrial CyberSecurity for Nodes контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Приложение не контролирует процессы, если какой-то из этапов распространения был выполнен до установки Kaspersky Industrial CyberSecurity for Nodes на защищаемое устройство.

9. Добавьте исполняемые файлы и пакеты установки, запуск которых будет разрешен:

   - **Один вручную**

     a. В контекстном меню кнопки **Добавить** выберите пункт **Добавить один вручную**.

     b. В открывшемся окне нажмите на кнопку **Обзор**.

     c. Выберите исполняемый файл или пакет установки.

     Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     d. Если необходимо, включите функцию **Присвоить признак доверенного пакета установки дочерним исполняемым файлам**.

     e. Выберите критерий, на основе которого исполняемый файл или пакет установки будет считаться доверенным: **Данные сертификата** или **SHA256-хеш**.

     f. Нажмите на кнопку **ОК**.

   Исполняемый файл или пакет установки отобразится в списке.

- **Несколько по хешу**

  a. В контекстном меню кнопки **Добавить** выберите пункт **Добавить несколько по хешу**.

  b. В открывшемся окне выберите любое количество файлов или пакетов установки.

  c. Нажмите на кнопку **Открыть**.

  Исполняемые файлы и пакеты установки отобразятся в списке. В их свойствах будет указано значение SHA256-хеша.

- **С помощью импорта из файла**

  a. Нажмите на кнопку **Импортировать**.

  b. В открывшемся окне выберите файл формата .TXT с данными об исполняемых файлах и пакетах установки.

  c. Нажмите на кнопку **Открыть.**

  Исполняемые файлы и пакеты установки отобразятся в списке. В их свойствах будет указано значение SHA256-хеша.

> Если вы создаете доверенный пакет установки на основе исполняемого файла и в параметрах Доверенной зоны на основе того же исполняемого файла вы добавили процесс и сделали его доверенным для компонента Контроль запуска программ, параметры Доверенной зоны имеют больший приоритет. Kaspersky Industrial CyberSecurity for Nodes запрещает запуск этого исполняемого файла, но считает доверенным процесс этого исполняемого файла.

10. Если необходимо, измените добавленные исполняемые файлы и пакеты установки с помощью кнопки **Изменить**.

11. Если необходимо, удалите добавленные исполняемые файлы и пакеты установки с помощью кнопки **Удалить**. Запуск распакованных исполняемых файлов при этом будет разрешен.

> Для блокировки запуска распакованных исполняемых файлов необходимо удалить Kaspersky Industrial CyberSecurity for Nodes с защищаемого устройства или создать для распакованных файлов запрещающие правила контроля запуска программ.

12. Нажмите на кнопку **OK**.

Как настроить Контроль пакетов установки с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Контроль компьютера** → **Контроль запуска программ**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

3. Выберите вкладку **Контроль пакетов установки**.

4. Включите функцию **Автоматически разрешать распространение с помощью указанных приложений и пакетов установки**. Функция автоматически создает исключения для всех файлов, запущенных с помощью указанных в списке исполняемых файлов и пакетов установки.

   Вы можете включить функцию **Автоматически разрешать распространение с помощью указанных приложений и пакетов установки**, если на вкладке **Общие** включена функция **Использовать правила для исполняемых файлов**.

5. Если необходимо, выключите функцию **Всегда разрешать распространение приложений с помощью установщика Windows**. Функция автоматически создает исключения для всех файлов, запущенных с помощью установщика Windows.

   Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

6. Если необходимо, включите функцию **Всегда разрешать распространение приложений через SCCM с помощью фоновой интеллектуальной службы передачи**. Функция разрешает распространение программного обеспечения с помощью решения System Center Configuration Manager.

   Если функция включена, Kaspersky Industrial CyberSecurity for Nodes разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Приложение разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service). Приложение контролирует запуск исполняемых файлов с расширениями .EXE и .MSI.

   Kaspersky Industrial CyberSecurity for Nodes контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Приложение не контролирует процессы, если какой-то из этапов распространения был выполнен до установки Kaspersky Industrial CyberSecurity for Nodes на защищаемое устройство.

7. Добавьте исполняемые файлы и пакеты установки, запуск которых будет разрешен:

   - **Один вручную**

     a. В контекстном меню кнопки **Добавить** выберите пункт **Добавить один вручную**.

     b. В открывшемся окне нажмите на кнопку **Обзор**.

     c. Выберите исполняемый файл или пакет установки.

     Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     d. Если необходимо, включите функцию **Присвоить признак доверенного пакета установки дочерним исполняемым файлам**.

     e. Выберите критерий, на основе которого исполняемый файл или пакет установки будет считаться доверенным: **Данные сертификата** или **SHA256-хеш**.

     f. Нажмите на кнопку **ОК**.

   Исполняемый файл или пакет установки отобразится в списке.

- **Несколько по хешу**

  a. В контекстном меню кнопки **Добавить** выберите пункт **Добавить несколько по хешу**.

  b. В открывшемся окне выберите любое количество файлов или пакетов установки.

  c. Нажмите на кнопку **Открыть**.

  Исполняемые файлы и пакеты установки отобразятся в списке. В их свойствах будет указано значение SHA256-хеша.

- **С помощью импорта из файла**

  a. Нажмите на кнопку **Импортировать**.

  b. В открывшемся окне выберите файл формата .TXT с данными об исполняемых файлах и пакетах установки.

  c. Нажмите на кнопку **Открыть.**

  Исполняемые файлы и пакеты установки отобразятся в списке. В их свойствах будет указано значение SHA256-хеша.

> Если вы создаете доверенный пакет установки на основе исполняемого файла и в параметрах Доверенной зоны на основе того же исполняемого файла вы добавили процесс и сделали его доверенным для компонента Контроль запуска программ, параметры Доверенной зоны имеют больший приоритет. Kaspersky Industrial CyberSecurity for Nodes запрещает запуск этого исполняемого файла, но считает доверенным процесс этого исполняемого файла.

8. Если необходимо, измените добавленные исполняемые файлы и пакеты установки с помощью кнопки **Изменить**.

9. Если необходимо, удалите добавленные исполняемые файлы и пакеты установки с помощью кнопки **Удалить**. Запуск распакованных исполняемых файлов при этом будет разрешен.

> Для блокировки запуска распакованных исполняемых файлов необходимо удалить Kaspersky Industrial CyberSecurity for Nodes с защищаемого устройства или создать для распакованных файлов запрещающие правила контроля запуска программ.

10. Нажмите на кнопку **OK**.

Как настроить Контроль пакетов установки с помощью Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Контроль активности на компьютерах**.

5. В блоке **Контроль запуска программ** нажмите на кнопку **Настроить**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

6. Выберите вкладку **Контроль пакетов установки**.

7. Включите функцию **Автоматически разрешать распространение с помощью указанных приложений и пакетов установки**. Функция автоматически создает исключения для всех файлов, запущенных с помощью указанных в списке исполняемых файлов и пакетов установки.

   Вы можете включить функцию **Автоматически разрешать распространение с помощью указанных приложений и пакетов установки**, если на вкладке **Общие** включена функция **Использовать правила для исполняемых файлов**.

8. Если необходимо, выключите функцию **Всегда разрешать распространение приложений с помощью установщика Windows**. Функция автоматически создает исключения для всех файлов, запущенных с помощью установщика Windows.

   Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

9. Если необходимо, включите функцию **Всегда разрешать распространение приложений через SCCM с помощью фоновой интеллектуальной службы передачи**. Функция разрешает распространение программного обеспечения с помощью решения System Center Configuration Manager.

   Если функция включена, Kaspersky Industrial CyberSecurity for Nodes разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Приложение разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service). Приложение контролирует запуск исполняемых файлов с расширениями .EXE и .MSI.

   Kaspersky Industrial CyberSecurity for Nodes контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Приложение не контролирует процессы, если какой-то из этапов распространения был выполнен до установки Kaspersky Industrial CyberSecurity for Nodes на защищаемое устройство.

10. Добавьте исполняемые файлы и пакеты установки, запуск которых будет разрешен:

    - **Вручную**

      a. Нажмите на кнопку **Добавить**.

      b. В блоке **Критерий доверенности** выберите критерий, на основе которого исполняемый файл или пакет установки будет считаться доверенным: **Использовать цифровой сертификат** или **Использовать SHA256-хеш**.

      c. Если вы выбрали **Использовать цифровой сертификат** введите заголовок и отпечаток сертификата, которым подписан исполняемый файл или пакет установки, а также название исполняемого файла или пакета установки.

      d. Если вы выбрали **Использовать SHA256-хеш**, с помощью кнопки **Обзор** выберите исполняемый файл или пакет установки.

e. Если необходимо, включите функцию **Присвоить признак доверенного пакета установки дочерним исполняемым файлам**.

f. Нажмите на кнопку **OK**.

Исполняемый файл или пакет установки отобразится в списке.

- **С помощью импорта из файла**

a. Нажмите на кнопку **Импортировать**.

b. В открывшемся окне выберите файл формата .TXT с данными об исполняемых файлах и пакетах установки.

c. Нажмите на кнопку **Открыть.**

Исполняемые файлы и пакеты установки отобразятся в списке. В их свойствах будет указано значение SHA256-хеша.

Если вы создаете доверенный пакет установки на основе исполняемого файла и в параметрах Доверенной зоны на основе того же исполняемого файла вы добавили процесс и сделали его доверенным для компонента Контроль запуска программ, параметры Доверенной зоны имеют больший приоритет. Kaspersky Industrial CyberSecurity for Nodes запрещает запуск этого исполняемого файла, но считает доверенным процесс этого исполняемого файла.

11. Если необходимо, измените добавленные исполняемые файлы и пакеты установки с помощью кнопки **Изменить**.

12. Если необходимо, удалите добавленные исполняемые файлы и пакеты установки с помощью кнопки **Удалить**. Запуск распакованных исполняемых файлов при этом будет разрешен.

Для блокировки запуска распакованных исполняемых файлов необходимо удалить Kaspersky Industrial CyberSecurity for Nodes с защищаемого устройства или создать для распакованных файлов запрещающие правила контроля запуска программ.

13. Нажмите на кнопку **OK**.

14. В окне **Контроль запуска программ** нажмите на кнопку **OK**.

Работа с правилами контроля запуска программ

В этом разделе даны инструкции для формирования списка правил контроля запуска программ.

Добавление правил контроля запуска программ

Как добавить правила контроля запуска программ с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности на компьютерах**.
4. В блоке **Контроль запуска программ** нажмите на кнопку **Настройка**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.
5. Выберите вкладку **Правила**.
6. С помощью раскрывающегося списка **Применение правил** выберите режим применения правил:

   - **Добавить правила политики к локальным правилам**. Приложение применяет список правил, заданный в политике, совместно с локальными списками правил.
   - **Заменить локальные правила правилами политики**. Приложение применяет список правил, заданных в политике, для контроля запуска программ на группе защищаемых устройств. Формирование, редактирование и применение локальных списков правил недоступно.
7. Если необходимо, включите функцию **Запретить изменение локальных правил пользователями**.

   Если функция включена, приложение запрещает изменение правил контроля запуска программ локально с помощью Консоли приложения. По умолчанию функция выключена.
8. Добавьте правила контроля запуска программ любым из следующих способов:

   - **Вручную**.

     a. Нажмите на кнопку **Добавить**.

     Откроется окно **Контроль запуска программ**.

     b. В поле **Название** введите название правила.

     c. Если необходимо, в поле **Описание** введите описание правила.

     d. В раскрывающемся списке **Тип** выберите тип правила:

     - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск приложений, описанных в правиле.
     - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск приложений, описанных в правиле.

e. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:

- **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.
- **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI. Поддерживаются файлы со следующими расширениями: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

f. Установите флажок **Доверенные приложения обновления**, если вы хотите, чтобы приложения, удовлетворяющие условиям срабатывания правила, Kaspersky Industrial CyberSecurity for Nodes считало доверенными приложениями обновления. Доверенные приложения обновления – приложения с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

Если приложение соответствует условиям срабатывания нескольких правил, Kaspersky Industrial CyberSecurity for Nodes устанавливает признак *Доверенные приложения обновления* при выполнении следующих условий:

- запуск приложения разрешен во всех правилах;
- хотя бы в одном правиле установлен флажок **Доверенные приложения обновления**.

g. Добавьте условия срабатывания правила контроля запуска программ.

h. Добавьте исключения из условий срабатывания правила контроля запуска программ.

i. Добавьте пользователей и/или группы пользователей, которым будет разрешено или запрещено запускать приложения, удовлетворяющие правилу.

j. Нажмите на кнопку **ОК**.

- **С помощью импорта XML-файла с правилами контроля запуска программ**.

a. В контекстном меню кнопки выберите **Импортировать → Из XML-файла**.

b. Выберите принцип добавления правил контроля устройств из XML-файла к списку уже имеющихся в политике правил контроля устройств:

- **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
- **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
- **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.

c. В открывшемся окне укажите путь к XML-файлу, созданному по завершении локальной или групповой задачи *Формирование правил контроля запуска программ*.

d. Нажмите на кнопку **Открыть**.

- **На основе событий Kaspersky Security Center с помощью запроса**.

  a. В контекстном меню кнопки выберите **Импортировать → Создать разрешающие правила на основе событий Kaspersky Security Center (запрос)**.

  b. Выберите принцип добавления правил к списку уже созданных правил контроля запуска программ:

  - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
  - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  Откроется окно **Создать правила контроля запуска программ**.

  c. Выберите типы событий, на основе которых приложение будет создавать правила контроля запуска программ:

  - **Запуск приложения запрещен**.
  - **Только статистика: запуск приложения запрещен**.

  d. Выберите период из раскрывающегося списка **Учитывать события, сформированные в течение периода**.

  e. Снимите или установите флажок **Приоритизировать использование контрольной суммы при создании правил**.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует контрольную сумму файла для формирования правила, когда доступны и контрольная сумма, и сертификат файла.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes использует цифровой сертификат файла для формирования правила, когда доступны и контрольная сумма, и сертификат файла.

  f. Нажмите на кнопку **Создать правила**.

  g. Нажмите на кнопку **ОК**.

- **С помощью импорта TXT-файла с выборкой событий Kaspersky Security Center о заблокированных приложениях**.

  1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

  2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

  3. В открывшемся окне свойств политики перейдите в раздел **Журналы и уведомления**.

  4. В блоке **Журналы выполнения задач** нажмите на кнопку **Настройка**.

  Откроется окно **Уведомления**.

  5. Раскройте узел **Контроль активности на компьютерах**.

6. Выберите раздел **Контроль запуска программ**.

7. В списке событий для компонента Контроль запуска программ в столбце **Отправлять события в Kaspersky Security Center** установите флажки напротив *Запуск приложения запрещен* и *Запуск приложения запрещен в тестовом режиме*.

8. Сохраните внесенные изменения.

9. В разделе политики **Настройка событий** убедитесь, что срок хранения выбранных событий, указанный в поле **Хранить в базе данных Сервера администрирования в течение (сут)**, превышает запланированный период для сбора данных о запрещенных запусках приложений (значение по умолчанию – 30 дней).

   По завершении периода хранения журнала компонента Контроль запуска программ, информация о зарегистрированных событиях будет удалена и не попадет в файл отчета.

10. Активируйте политику, которая настроена для сбора данных о запрещенных запусках приложений.

11. При необходимости меняйте режим работы компонента Контроль запуска программ.

12. По истечении периода, отведенного для сбора данных о запрещенных запусках приложений, создайте, запустите и экспортируйте в TXT-файл выборку из событий *Запуск приложения запрещен* и *Запуск приложения запрещен в тестовом режиме*. Подробнее читайте в разделе "Выборки событий" в справке Kaspersky Security Center.

13. Откройте экспортированный TXT-файл.

14. Если нужно, скорректируйте список событий.

Добавленные правила контроля запуска программ отобразятся в списке.

9. Если необходимо, выполните пункт 5 для добавления следующих правил контроля запуска программ.

10. Если необходимо, измените добавленные правила контроля запуска программ с помощью кнопки **Изменить**.

11. Если необходимо, удалите добавленные правила контроля запуска программ с помощью кнопки **Удалить**.

12. Нажмите на кнопку **ОК**.

Как добавить правила контроля запуска программ с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Контроль компьютера → Контроль запуска программ**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

3. Выберите вкладку **Правила**.

4. Добавьте правила контроля запуска программ любым из следующих способов:

- **Вручную**

  a. Нажмите на кнопку **Добавить**.

  Откроется окно **Контроль запуска программ**.

  b. В поле **Название** введите название правила.

  c. Если необходимо, в поле **Описание** введите описание правила.

  d. В раскрывающемся списке **Тип** выберите тип правила:

  - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск приложений, описанных в правиле.
  - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск приложений, описанных в правиле.

  e. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:

  - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.
  - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI. Поддерживаются файлы со следующими расширениями: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

  f. Установите флажок **Доверенные приложения обновления**, если вы хотите, чтобы приложения, удовлетворяющие условиям срабатывания правила, Kaspersky Industrial CyberSecurity for Nodes считало доверенными приложениями обновления. Доверенные приложения обновления – приложения с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

  Если приложение соответствует условиям срабатывания нескольких правил, Kaspersky Industrial CyberSecurity for Nodes устанавливает признак *Доверенные приложения обновления* при выполнении следующих условий:

  - запуск приложения разрешен во всех правилах;
  - хотя бы в одном правиле установлен флажок **Доверенные приложения обновления**.

  g. Добавьте условия срабатывания правила контроля запуска программ.

  h. Добавьте исключения из условий срабатывания правила контроля запуска программ.

  i. Добавьте пользователей и/или группы пользователей, которым будет разрешено или запрещено запускать приложения, удовлетворяющие правилу.

  j. Нажмите на кнопку **ОК**.

- **С помощью импорта XML-файла с правилами контроля запуска программ**

  a. В контекстном меню кнопки выберите **Импортировать → Из XML-файла**.

  b. Выберите принцип добавления правил контроля устройств из XML-файла к списку уже имеющихся в политике правил контроля устройств:

  - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
  - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.

  c. В открывшемся окне укажите путь к XML-файлу, созданному по завершении локальной или групповой задачи *Формирование правил контроля запуска программ*.

  d. Нажмите на кнопку **Открыть**.

Добавленные правила контроля запуска программ отобразятся в списке.

5. Если необходимо, выполните пункт 5 для добавления следующих правил контроля запуска программ.
6. Если необходимо, измените добавленные правила контроля запуска программ с помощью кнопки **Изменить**.
7. Если необходимо, удалите добавленные правила контроля запуска программ с помощью кнопки **Удалить**.
8. Нажмите на кнопку **OK**.

Как добавить правила контроля запуска программ с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Контроль активности на компьютерах**.
5. В блоке **Контроль запуска программ** нажмите на кнопку **Настроить**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.
6. Выберите вкладку **Правила**.

7. С помощью раскрывающегося списка **Применение правил** выберите режим применения правил:

   - **Добавить правила политики к локальным правилам**. Приложение применяет список правил, заданный в политике, совместно с локальными списками правил.

   - **Заменить локальные правила правилами политики**. Приложение применяет список правил, заданных в политике, для контроля запуска программ на группе защищаемых устройств. Формирование, редактирование и применение локальных списков правил недоступно.

8. Если необходимо, включите функцию **Запретить изменение локальных правил пользователями**.

   Если функция включена, приложение запрещает изменение правил контроля запуска программ локально с помощью Консоли приложения. По умолчанию функция выключена.

9. Добавьте правила контроля запуска программ любым из следующих способов:

   - **Вручную**

     a. Нажмите на кнопку **Добавить**.

     Откроется окно **Настройки правила**.

     b. В поле **Название** введите название правила.

     c. В раскрывающемся списке **Тип** выберите тип правила:

     - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск приложений, описанных в правиле.

     - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск приложений, описанных в правиле.

     d. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:

     - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.

     - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.

     e. Установите флажок **Запрещать для остальных пользователей**, если вы хотите, чтобы приложение запрещало запуск приложений, описанных в правиле, всем пользователям, которые не указаны во вкладке **Пользователь или группа**.

     f. Установите флажок **Доверенные приложения обновления**, если вы хотите, чтобы приложения, удовлетворяющие условиям срабатывания правила, Kaspersky Industrial CyberSecurity for Nodes считало доверенными приложениями обновления. Доверенные приложения обновления – приложения с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

     Если приложение соответствует условиям срабатывания нескольких правил, Kaspersky Industrial CyberSecurity for Nodes устанавливает признак *Доверенные приложения обновления* при выполнении следующих условий:

     - запуск приложения разрешен во всех правилах;

     - хотя бы в одном правиле установлен флажок **Доверенные приложения обновления**.

g. Добавьте условия срабатывания правила контроля запуска программ.

h. Добавьте исключения из условий срабатывания правила контроля запуска программ.

i. **Добавьте пользователей и/или группы пользователей, которым будет разрешено или запрещено запускать приложения, удовлетворяющие правилу**.

a. Выберите вкладку **Пользователь или группа**.

b. Нажмите на кнопку **Добавить**.

c. В открывшемся окне выберите из списка или введите вручную имя пользователя или группы пользователей.

d. Нажмите на кнопку **Выбрать**.

e. Выполните пункты b-d для каждого пользователя или группы пользователей.

j. Нажмите на кнопку **ОК**.

Добавленные правила контроля запуска программ отобразятся в списке.

- **С помощью импорта XML-файла с правилами контроля запуска программ**

a. Нажмите на кнопку **Импорт**.

b. В открывшемся окне **Импорт из файла** нажмите на кнопку **Выбрать**.

c. Укажите путь к XML-файлу, созданному по завершении локальной или групповой задачи *Формирование правил контроля запуска программ*.

d. Нажмите на кнопку **Открыть**.

e. Нажмите на кнопку **Импорт**.

Импортированные правила контроля запуска программ будут добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.

- **С помощью импорта XML-файла с правилами контроля запуска программ Kaspersky Industrial CyberSecurity for Nodes версии 4.0**

a. Нажмите на кнопку **Импорт из предыдущей версии**.

b. В открывшемся окне **Импорт из файла** нажмите на кнопку **Выбрать**.

c. Укажите путь к XML-файлу с правилами контроля запуска программ, экспортированному из приложения Kaspersky Industrial CyberSecurity for Nodes версии 4.0.

d. Нажмите на кнопку **Открыть**.

e. Нажмите на кнопку **Импорт**.

Импортированные правила контроля запуска программ будут добавлены в список существующих правил. Правила с одинаковыми параметрами не добавляются. Если хотя бы один параметр правила уникален, правило добавляется.

- **С помощью импорта правил из файла отчета Kaspersky Security Center**

  a. Нажмите на кнопку **Импорт из отчета KSC**.

  b. В открывшемся окне выберите файл формата TXT, в который были экспортированы события из отчета.

  c. Нажмите на кнопку **Открыть.**

  Правила, созданные на основе отчета Kaspersky Security Center, будут добавлены к списку правил в политике.

- **На основе событий Kaspersky Security Center с помощью запроса**

  a. Нажмите на кнопку **Разрешающие правила из событий KSC**.

  Откроется окно **Формирование правил контроля запуска программ**.

  b. Выберите тип событий, на основе которых приложение будет создавать правила контроля запуска программ:

  - **Все события**.
  - **Запуск приложения запрещен**.
  - **Только статистика: запуск приложения запрещен**.

  c. Выберите период из раскрывающегося списка **Использовать события, сформированные за период**.

  d. Снимите или установите флажок **Приоритизировать использование контрольной суммы при создании правил**.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes использует контрольную сумму файла для формирования правила, когда доступны и контрольная сумма, и сертификат файла.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes использует цифровой сертификат файла для формирования правила, когда доступны и контрольная сумма, и сертификат файла.

  e. При необходимости укажите название группы управляемых устройств в поле **Использовать события, сформированные для группы управляемых устройств**.

  f. Нажмите на кнопку **Сформировать правила**.

  g. Выберите из выпадающего списка **Правило добавления в основной список** принцип добавления правил к списку уже созданных правил контроля запуска программ:

  - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

h. Выберите правила, которые вы хотите экспортировать в правила контроля запуска программ политики и нажмите на кнопку **Экспорт**.

i. Сохраните внесенные изменения.

10. Если необходимо, выполните пункт 5 для добавления следующих правил контроля запуска программ.

11. Если необходимо, измените добавленные правила контроля запуска программ с помощью кнопки **Изменить**.

12. Если необходимо, удалите добавленные правила контроля запуска программ с помощью кнопки **Удалить**.

13. Нажмите на кнопку **ОК**.

Добавление условий срабатывания правила контроля запуска программ

Как добавить условия срабатывания правила контроля запуска программ с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности на компьютерах**.

4. В блоке **Контроль запуска программ** нажмите на кнопку **Настройка**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

5. Выберите вкладку **Правила**.

6. Выполните одно из следующих действий:

   a. Нажмите на кнопку **Добавить**, если вы добавляете новое правило контроля запуска программ.

   b. В списке правил контроля запуска программ выберите то, для которого хотите добавить условия срабатывания, и нажмите на кнопку **Изменить**.

   Откроется окно **Контроль запуска программ**.

7. На вкладке **Условия** в контекстном меню кнопки **Добавить** выберите условие срабатывания правила контроля запуска программ:

   - **Информация из файла**. В качестве условия срабатывания правила будет использована **информация из выбранного файла**.

     a. В окне **Информация из файла** нажмите на кнопку **Обзор**.

     Откроется стандартное окно Microsoft Windows **Открыть файл**.

     b. Выберите файл.

c. Нажмите на кнопку **Открыть**.

Данные о выбранном файле отобразятся в окне **Информация из файла**.

d. Выберите хотя бы один пункт:

- **Данные сертификата**. Если флажок установлен, правило не будет контролировать запуск приложений, подписанных цифровым сертификатом, с указанными данными.
- **Метаданные**. Если флажок установлен, правило не будет контролировать запуск приложений с указанными метаданными.
- **Хеш файла**. Если флажок установлен, правило не будет контролировать запуск приложений с указанным SHA256-хешом.
- **Путь к файлу**. Если флажок установлен, правило не будет контролировать запуск приложений, расположенных по указанному пути.

e. Если необходимо, в поле **Командная строка** введите команду для запуска приложения с помощью командной строки. Правило будет контролировать запуск этого приложения. Вы можете использовать символы ? и * для ввода маски.

> Kaspersky Industrial CyberSecurity for Nodes не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\") для ввода пути.

f. Нажмите на кнопку **OK**.

- **Тип носителя**. Правило будет контролировать запуск приложений со всех подключенных в защищаемому компьютеру съемных дисков.
- **KL-категория**. Правило будет контролировать запуск приложений, которые относятся к выбранным KL-категориям.
- **Доверенные в KSN**. Правило будет контролировать запуск приложений, которые являются доверенными в KSN.
- **Недоверенные в KSN**. Правило будет контролировать запуск приложений, которые являются недоверенными в KSN.
- **Доверенные в ОС**. Правило будет контролировать запуск приложений, которые являются доверенными в операционной системе.

Добавленное условие отобразится в списке.

8. Если необходимо, выполните предыдущий пункт инструкции для каждого следующего условия срабатывания правила.
9. Если необходимо, измените условия срабатывания правила с помощью кнопки **Изменить**.
10. Сохраните внесенные изменения.

Как добавить условия срабатывания правила контроля запуска программ с помощью с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Контроль компьютера** → **Контроль запуска программ**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

3. Выберите вкладку **Правила**.

4. Выполните одно из следующих действий:

   a. Нажмите на кнопку **Добавить**, если вы добавляете новое правило контроля запуска программ.

   b. В списке правил контроля запуска программ выберите то, для которого хотите добавить условия срабатывания, и нажмите на кнопку **Изменить**.

   Откроется окно **Контроль запуска программ**.

5. На вкладке **Условия** в контекстном меню кнопки **Добавить** выберите условие срабатывания правила контроля запуска программ:

   - **Информация из файла**. В качестве условия срабатывания правила будет использована **информация из выбранного файла**.

     a. В окне **Информация из файла** нажмите на кнопку **Обзор**.

     Откроется стандартное окно Microsoft Windows **Открыть файл**.

     b. Выберите файл.

     c. Нажмите на кнопку **Открыть**.

     Данные о выбранном файле отобразятся в окне **Информация из файла**.

     d. Выберите хотя бы один пункт:

     - **Данные сертификата**. Если флажок установлен, правило не будет контролировать запуск приложений, подписанных цифровым сертификатом, с указанными данными.

     - **Метаданные**. Если флажок установлен, правило не будет контролировать запуск приложений с указанными метаданными.

     - **Хеш файла**. Если флажок установлен, правило не будет контролировать запуск приложений с указанным SHA256-хешом.

     - **Путь к файлу**. Если флажок установлен, правило не будет контролировать запуск приложений, расположенных по указанному пути.

e. Если необходимо, в поле **Командная строка** введите команду для запуска приложения с помощью командной строки. Правило будет контролировать запуск этого приложения. Вы можете использовать символы ? и * для ввода маски.

> Kaspersky Industrial CyberSecurity for Nodes не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\") для ввода пути.

f. Нажмите на кнопку **OK**.

- **Тип носителя**. Правило будет контролировать запуск приложений со всех подключенных в защищаемому компьютеру съемных дисков.
- **KL-категория**. Правило будет контролировать запуск приложений, которые относятся к выбранным KL-категориям.
- **Доверенные в KSN**. Правило будет контролировать запуск приложений, которые являются доверенными в KSN.
- **Недоверенные в KSN**. Правило будет контролировать запуск приложений, которые являются недоверенными в KSN.
- **Доверенные в ОС**. Правило будет контролировать запуск приложений, которые являются доверенными в операционной системе.

Добавленное условие отобразится в списке.

6. Если необходимо, выполните предыдущий пункт инструкции для каждого следующего условия срабатывания правила.
7. Если необходимо, измените условия срабатывания правила с помощью кнопки **Изменить**.
8. Сохраните внесенные изменения.

Как добавить условия срабатывания правила контроля запуска программ с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Контроль активности на компьютерах**.
5. В блоке **Контроль запуска программ** нажмите на кнопку **Настроить**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.
6. Выберите вкладку **Правила**.
7. Нажмите на кнопку **Добавить**.

   Откроется окно **Настройки правила**.

8. На вкладке **Условия** нажмите на кнопку **Добавить**.

   Откроется окно **Настройки правила**.

9. Выберите условие срабатывания правила контроля запуска программ:

   - **Информация из файла**. В качестве условия срабатывания правила будет использована **информация из файла**.

     a. В блоке **Критерии срабатывания правила** укажите значение хотя бы для одного критерия:

     - **Цифровой сертификат**. Если флажок установлен, правило не будет контролировать запуск приложений, подписанных цифровым сертификатом, с указанными данными.
     - **Метаданные**. Если флажок установлен, правило не будет контролировать запуск приложений с указанными метаданными.
     - **SHA256-хеш**. Если флажок установлен, правило не будет контролировать запуск приложений с указанным SHA256-хешом.
     - **Путь к файлу**. Если флажок установлен, правило не будет контролировать запуск приложений, расположенных по указанному пути.

     b. Нажмите на кнопку **OK**.

   - **Из KL-категории**. Правило будет контролировать запуск приложений, которые относятся к выбранным KL-категориям.
   - **Внешний диск**. Правило будет контролировать запуск приложений со всех подключенных в защищаемому компьютеру съемных дисков.
   - **Доверенные в ОС**. Правило будет контролировать запуск приложений, которые являются доверенными в операционной системе.

   Добавленное условие отобразится в списке.

10. Если необходимо, выполните пункты 4-5 для каждого следующего условия срабатывания правила.
11. Если необходимо, измените условия срабатывания правила с помощью кнопки **Изменить**.
12. Сохраните внесенные изменения.

Добавление исключений из области действия правила контроля запуска программ

Как добавить исключения из области действия правила контроля запуска программ с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности на компьютерах**.

4. В блоке **Контроль запуска программ** нажмите на кнопку **Настройка**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

5. Выберите вкладку **Правила**.

6. Выполните одно из следующих действий:

   a. Нажмите на кнопку **Добавить**, если вы добавляете новое правило контроля запуска программ.

   b. В списке правил контроля запуска программ выберите то, для которого хотите добавить исключения, и нажмите на кнопку **Изменить**.

   Откроется окно **Контроль запуска программ**.

7. На вкладке **Исключения** в контекстном меню кнопки **Добавить** выберите критерий для формирования исключения из области действия правила контроля запуска программ:

   - **Информация из файла**. В качестве критерия будет использована **информация из выбранного файла**.

     a. В окне **Информация из файла** нажмите на кнопку **Обзор**.

     Откроется стандартное окно Microsoft Windows **Открыть файл**.

     b. Выберите файл.

     c. Нажмите на кнопку **Открыть**.

     Данные о выбранном файле отобразятся в окне **Информация из файла**.

     d. Выберите хотя бы один пункт:

     - **Данные сертификата**. Если флажок установлен, правило не будет контролировать запуск приложений, подписанных цифровым сертификатом, с указанными данными.
     - **Метаданные**. Если флажок установлен, правило не будет контролировать запуск приложений с указанными метаданными.
     - **Хеш файла**. Если флажок установлен, правило не будет контролировать запуск приложений с указанным SHA256-хешом.
     - **Путь к файлу**. Если флажок установлен, правило не будет контролировать запуск приложений, расположенных по указанному пути.

     e. Если необходимо, в поле **Командная строка** введите команду для запуска приложения с помощью командной строки. Правило не будет контролировать запуск этого приложения. Вы можете использовать символы ? и * для ввода маски.

     > Kaspersky Industrial CyberSecurity for Nodes не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\") для ввода пути.

     f. Нажмите на кнопку **ОК**.

   - **Тип носителя**. Правило не будет контролировать запуск приложений со всех подключенных в защищаемому компьютеру съемных дисков.

- **KL-категория**. Правило не будет контролировать запуск приложений, которые относятся к выбранным KL-категориям.
- **Доверенные в KSN**. Правило не будет контролировать запуск приложений, которые являются доверенными в KSN.
- **Недоверенные в KSN**. Правило не будет контролировать запуск приложений, которые являются недоверенными в KSN.
- **Доверенные в ОС**. Правило не будет контролировать запуск приложений, которые являются доверенными в операционной системе.

Добавленное исключение отобразится в списке.

8. Если необходимо, выполняйте предыдущий пункт инструкции для добавления каждого следующего исключения из области действия правила контроля запуска программ.
9. Если необходимо, измените исключения с помощью кнопки **Изменить**.
10. Сохраните внесенные изменения.

Как добавить исключения из области действия правила контроля запуска программ с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Контроль компьютера** → **Контроль запуска программ**.
2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.
3. Выберите вкладку **Правила**.
4. Выполните одно из следующих действий:

   a. Нажмите на кнопку **Добавить**, если вы добавляете новое правило контроля запуска программ.

   b. В списке правил контроля запуска программ выберите то, для которого хотите добавить исключения, и нажмите на кнопку **Изменить**.

   Откроется окно **Контроль запуска программ**.
5. На вкладке **Исключения** в контекстном меню кнопки **Добавить** выберите критерий для формирования исключения из области действия правила контроля запуска программ:

   - **Информация из файла**. В качестве критерия будет использована **информация из выбранного файла**.

     a. В окне **Информация из файла** нажмите на кнопку **Обзор**.

     Откроется стандартное окно Microsoft Windows **Открыть файл**.

     b. Выберите файл.

     c. Нажмите на кнопку **Открыть**.

     Данные о выбранном файле отобразятся в окне **Информация из файла**.

d. Выберите хотя бы один пункт:

- **Данные сертификата**. Если флажок установлен, правило не будет контролировать запуск приложений, подписанных цифровым сертификатом, с указанными данными.
- **Метаданные**. Если флажок установлен, правило не будет контролировать запуск приложений с указанными метаданными.
- **Хеш файла**. Если флажок установлен, правило не будет контролировать запуск приложений с указанным SHA256-хешом.
- **Путь к файлу**. Если флажок установлен, правило не будет контролировать запуск приложений, расположенных по указанному пути.

e. Если необходимо, в поле **Командная строка** введите команду для запуска приложения с помощью командной строки. Правило не будет контролировать запуск этого приложения. Вы можете использовать символы ? и * для ввода маски.

> Kaspersky Industrial CyberSecurity for Nodes не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\") для ввода пути.

f. Нажмите на кнопку **OK**.

- **Тип носителя**. Правило не будет контролировать запуск приложений со всех подключенных в защищаемому компьютеру съемных дисков.
- **KL-категория**. Правило не будет контролировать запуск приложений, которые относятся к выбранным KL-категориям.
- **Доверенные в KSN**. Правило не будет контролировать запуск приложений, которые являются доверенными в KSN.
- **Недоверенные в KSN**. Правило не будет контролировать запуск приложений, которые являются недоверенными в KSN.
- **Доверенные в ОС**. Правило не будет контролировать запуск приложений, которые являются доверенными в операционной системе.

Добавленное исключение отобразится в списке.

6. Если необходимо, выполняйте предыдущий пункт инструкции для добавления каждого следующего исключения из области действия правила контроля запуска программ.
7. Если необходимо, измените исключения с помощью кнопки **Изменить**.
8. Сохраните внесенные изменения.

Как добавить исключения из области действия правила контроля запуска программ с помощью Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Контроль активности на компьютерах**.

5. В блоке **Контроль запуска программ** нажмите на кнопку **Настроить**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

6. Выберите вкладку **Правила**.

7. Нажмите на кнопку **Добавить**.

   Откроется окно **Настройки правила**.

8. На вкладке **Исключения** нажмите на кнопку **Добавить**.

   Откроется окно **Настройки правила**.

9. Выберите критерий для формирования исключения из области действия правила контроля запуска программ:

   - **Информация из файла**. Правило не будет контролировать запуск приложений, данные которых соответствуют **данным из файла**.

     a. В блоке **Критерии срабатывания правила** укажите значение хотя бы для одного критерия:

     - **Цифровой сертификат**. Если флажок установлен, правило не будет контролировать запуск приложений, подписанных цифровым сертификатом, с указанными данными.
     - **Метаданные**. Если флажок установлен, правило не будет контролировать запуск приложений с указанными метаданными.
     - **SHA256-хеш**. Если флажок установлен, правило не будет контролировать запуск приложений с указанным SHA256-хешом.
     - **Путь к файлу**. Если флажок установлен, правило не будет контролировать запуск приложений, расположенных по указанному пути.

     b. Нажмите на кнопку **ОК**.

   - **KL-категория**. Правило не будет контролировать запуск приложений, которые относятся к выбранным KL-категориям.
   - **Тип носителя**. Правило не будет контролировать запуск приложений со всех подключенных в защищаемому компьютеру съемных дисков.
   - **Доверенные в ОС**. Правило не будет контролировать запуск приложений, которые являются доверенными в операционной системе.

   Добавленное условие отобразится в списке.

10. Если необходимо, выполняйте пункты 4-5 для каждого следующего исключения из области действия правила контроля запуска программ.

11. Если необходимо, измените исключения с помощью кнопки **Изменить**.

12. Сохраните внесенные изменения.

Разрешение запуска всех приложений

Вы можете разрешить запуск всех приложений с помощью специально настроенных разрешающих правил контроля запуска программ.

Чтобы настроить разрешение запуска всех приложений:

1. Добавьте вручную два разрешающих правила контроля запуска программ со следующими параметрами:
   - тип правила – *разрешающее*, область применения – *исполняемые файлы*, путь к файлу – `?:\`.
   - тип правила – *разрешающее*, область применения – *скрипты и пакеты MSI*, путь к файлу – `?:\`.
2. Если ранее были добавлены запрещающие правила контроля запуска программ, удалите их.
3. Для всех ранее созданных разрешающих правил контроля запуска программ удалите исключения.
4. Сохраните внесенные изменения.

Экспорт правил контроля запуска программ

Вы можете экспортировать список правил контроля запуска программ и список доверенных пакетов контроля пакетов установки в файл формата XML. Вы можете использовать функцию экспорта для резервного копирования списка правил контроля запуска программ или для миграции списка на другой сервер.

Экспорт правил контроля запуска программ с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности на компьютерах**.
4. В блоке **Контроль запуска программ** нажмите на кнопку **Настройка**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.
5. Перейдите на вкладку **Правила** для экспорта правил Контроля запуска программ или **Контроль пакетов установки** для экспорта правил Контроля пакетов установки.
6. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

7. Если вы хотите экспортировать только часть списка, выполните следующие действия:

   a. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A**.

   b. Нажмите на кнопку и выберите **Экспортировать выбранное**.

8. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

Kaspersky Industrial CyberSecurity for Nodes экспортирует список правил в XML-файл.

Экспорт правил контроля запуска программ с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите раздел **Контроль компьютера → Контроль запуска программ**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

3. Перейдите на вкладку **Правила** для экспорта правил Контроля запуска программ или **Контроль пакетов установки** для экспорта правил Контроля пакетов установки.

4. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

5. Если вы хотите экспортировать только часть списка, выполните следующие действия:

   a. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A**.

   b. Нажмите на кнопку и выберите **Экспортировать выбранное**.

6. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

Kaspersky Industrial CyberSecurity for Nodes экспортирует список правил в XML-файл.

Экспорт правил контроля запуска программ с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Контроль активности на компьютерах**.

5. В блоке **Контроль запуска программ** нажмите на кнопку **Настроить**.

   Откроется окно **Контроль запуска программ** на вкладке **Общие**.

6. Перейдите на вкладку **Правила** для экспорта правил Контроля запуска программ или **Контроль пакетов установки** для экспорта правил Контроля пакетов установки.

7. Выберите правила, которые вы хотите экспортировать, с помощью флажков.

8. Нажмите на кнопку **Экспорт.** В открывшемся окне укажите, хотите ли вы экспортировать только выбранные правила или все правила, и нажмите на кнопку **Экспорт**.

   Если вы не выбрали ни одного правила, Kaspersky Industrial CyberSecurity for Nodes экспортирует все правила.

Kaspersky Industrial CyberSecurity for Nodes экспортирует список правил в XML-файл.

Формирование TXT-файла с выборкой событий Kaspersky Security Center о заблокированных приложениях

Вы можете экспортировать выборку событий Kaspersky Security Center о заблокированных приложениях в TXT-файл и далее импортировать эти данные для формирования списка разрешающих правил контроля запуска программ в настраиваемой политике.

Как сформировать TXT-файл с выборкой событий Kaspersky Security Center о заблокированных приложениях с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Журналы и уведомления**.
4. В блоке **Журналы выполнения задач** нажмите на кнопку **Настройка**.

   Откроется окно **Уведомления**.
5. Раскройте узел **Контроль активности на компьютерах**.
6. Выберите раздел **Контроль запуска программ**.
7. В списке событий для компонента Контроль запуска программ в столбце **Отправлять события в Kaspersky Security Center** установите флажки напротив *Запуск приложения запрещен* и *Запуск приложения запрещен в тестовом режиме*.
8. Сохраните внесенные изменения.
9. В разделе политики **Настройка событий** убедитесь, что срок хранения выбранных событий, указанный в поле **Хранить в базе данных Сервера администрирования в течение (сут)**, превышает запланированный период для сбора данных о запрещенных запусках приложений (значение по умолчанию – 30 дней).

   > По завершении периода хранения журнала компонента Контроль запуска программ, информация о зарегистрированных событиях будет удалена и не попадет в файл отчета.
10. Активируйте политику, которая настроена для сбора данных о запрещенных запусках приложений.
11. При необходимости меняйте режим работы компонента Контроль запуска программ.
12. По истечении периода, отведенного для сбора данных о запрещенных запусках приложений, создайте, запустите и экспортируйте в TXT-файл выборку из событий *Запуск приложения запрещен* и *Запуск приложения запрещен в тестовом режиме*. Подробнее читайте в разделе "Выборки событий" в справке Kaspersky Security Center.

13. Откройте экспортированный TXT-файл.

14. Если нужно, скорректируйте список событий.

Как сформировать TXT-файл с выборкой событий Kaspersky Security Center о заблокированных приложениях с помощью Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Журналы и уведомления**.

5. В блоке **Журналы выполнения задач** нажмите на кнопку **Настроить**.

   Откроется окно **Журналы выполнения задач**.

6. Выберите раздел **Контроль запуска программ**.

7. В списке событий для компонента Контроль запуска программ в столбце **Отправлять события в Kaspersky Security Center** установите флажки напротив *Запуск приложения запрещен* и *Запуск приложения запрещен в тестовом режиме*.

8. Сохраните внесенные изменения.

9. На вкладке настраиваемой политики **Настройка событий** убедитесь, что срок хранения выбранных событий, указанный в поле **Хранить в базе данных Сервера администрирования в течение (сут)**, превышает запланированный период для сбора данных о запрещенных запусках приложений (значение по умолчанию – 30 дней).

   По завершении периода хранения журнала компонента Контроль запуска программ, информация о зарегистрированных событиях будет удалена и не попадет в файл отчета.

10. Активируйте политику, которая настроена для сбора данных о запрещенных запусках приложений.

11. При необходимости меняйте режим работы компонента Контроль запуска программ.

12. По истечении периода, отведенного для сбора данных о запрещенных запусках приложений, создайте, запустите и экспортируйте в TXT-файл выборку из событий *Запуск приложения запрещен* и *Запуск приложения запрещен в тестовом режиме*. Подробнее читайте в разделе "Выборки событий" в справке Kaspersky Security Center.

13. Откройте экспортированный TXT-файл.

14. Если нужно, скорректируйте список событий.

Настройка групповой задачи Формирование правил контроля запуска программ

Как настроить групповую задачу Формирование правил контроля запуска программ с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите вкладку **Задачи**.
4. В списке групповых задач откройте задачу *Формирование правил контроля запуска программ* двойным щелчком мыши по названию задачи.

   Откроется окно **Свойства: Формирование правил контроля запуска программ**.
5. Перейдите в раздел **Настройки**.
6. На вкладке **Правила**, если необходимо, укажите префикс для названий правил.
7. В блоке **Область применения разрешающих правил** укажите способ создания разрешающих правил:
   - **Создавать разрешающие правила на основе запущенных приложений**.
   - **Создавать разрешающие правила для приложений из папок**.
8. На вкладке **Настройки** выберите критерий, который будет устанавливать задача при формировании разрешающих правил контроля запуска программ:
   - **Использовать цифровой сертификат**.

     Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. Kaspersky Industrial CyberSecurity for Nodes будет разрешать запуск файлов, у которых есть цифровой сертификат. Рекомендуем этот вариант, если вы хотите разрешать запуск приложений, доверенных в операционной системе. Этот вариант выбран по умолчанию.
   - **Использовать заголовок и отпечаток цифрового сертификата**.
   - **Если сертификат отсутствует, использовать**.
   - **Использовать SHA256-хеш**.

     Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается контрольная сумма файла, на основе которого формируется правило. Kaspersky Industrial CyberSecurity for Nodes будет разрешать запуск приложений, запускаемых с помощью файлов с указанной контрольной суммой. Использование контрольной суммы SHA256 в качестве критерия срабатывания правила сужает область применения правила до одного файла.
9. Настройте параметр **Добавлять путь к файлу для правил, сформированных на основе хеш-сумм**.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes при экспорте правил добавляет в XML-файл полные пути к исполняемым файлам. Наличие полного пути поможет вам определить, к какому ПО относится данный исполняемый файл.

Если флажок снят, в XML-файле будут содержаться только имена и SHA256-хеши исполняемых файлов. По умолчанию флажок снят.

10. Добавьте пользователей и/или группы пользователей, которым будет разрешено запускать приложения, удовлетворяющие правилам, которые будут созданы с помощью задачи:

    a. В контекстном меню кнопки **Добавить** выберите способ добавления пользователей или групп.

    b. В открывшемся окне введите или выберите имя пользователя или группы пользователей.

    c. Нажмите на кнопку **OK**.

    d. Выполните пункты a-c для каждого пользователя или группы пользователей.

11. В блоке **По завершении задачи** настройте следующие параметры:

    - **Добавлять разрешающие правила в список правил контроля запуска программ**.
    - **Принцип добавления**.
    - **Экспортировать разрешающие правила в файл**.
    - **Добавлять информацию о защищаемом устройстве в имя файла**.

12. Если требуется, на вкладке **Исключения** укажите объекты, которые хотите исключить из области действия задачи.

13. В окне **Свойства: Формирование правил контроля запуска программ** нажмите на кнопку **OK**.

Как настроить групповую задачу Формирование правил контроля запуска программ с помощью Web Console

1. В главном окне Web Console выберите **Управление активами → Задачи**.

2. В списке групповых задач откройте задачу Формирование правил контроля запуска программ.

   Откроется окно **Формирование правил контроля запуска программ**.

3. Откройте вкладку **Параметры приложения**.

4. В разделе **Область применения разрешающих правил**, если необходимо, укажите префикс для названий правил.

5. В блоке **Область применения разрешающих правил** укажите способ создания разрешающих правил:

   - **Создавать разрешающие правила на основе запущенных приложений**
   - **Создавать разрешающие правила для приложений из папок**

6. На вкладке **Параметры** выберите критерий, который будет устанавливать задача при формировании разрешающих правил контроля запуска программ:

   - **Использовать цифровой сертификат**.

- **Использовать заголовок и отпечаток цифрового сертификата**.
- **Если сертификат отсутствует, использовать**.
- **Использовать хеш SHA256**.

7. Настройте параметр **Добавлять путь к файлу для правил, сформированных на основе хеш-сумм**.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes при экспорте правил добавляет в XML-файл полные пути к исполняемым файлам. Наличие полного пути поможет вам определить, к какому ПО относится данный исполняемый файл.

   Если флажок снят, в XML-файле будут содержаться только имена и SHA256-хеши исполняемых файлов. По умолчанию флажок снят.

8. Добавьте пользователей и/или группы пользователей, которым будет разрешено запускать приложения, удовлетворяющие правилам, которые будут созданы с помощью задачи:

   a. Нажмите на кнопку **Добавить пользователя или группу**.

   b. В открывшемся окне выберите из списка или введите вручную имя пользователя или группы пользователей.

   c. Нажмите на кнопку **Выбрать**.

   d. Выполните пункты a-c для каждого пользователя или группы пользователей.

9. В блоке **По завершении задачи** настройте следующие параметры:

   - **Добавлять разрешающие правила в список правил контроля запуска программ**.
   - **Принцип добавления**.
   - **Правила будут экспортированы в файл**. В поле **Задайте полный путь к файлу с расширением .xml** вы можете указать путь, по которому по завершении задачи Формирование правил контроля запуска программ Kaspersky Industrial CyberSecurity for Nodes экспортирует разрешающие правила в XML-файл.
   - **Добавлять информацию о защищаемом устройстве в имя файла**.

10. Если требуется, на вкладке **Исключения** укажите объекты, которые хотите исключить из области действия задачи.

11. В окне **Формирование правил контроля запуска программ** нажмите на кнопку **OK**.

Создание правил с помощью групповой задачи Формирование правил контроля запуска программ

Чтобы создать правила с помощью групповой задачи Формирование правил контроля запуска программ:

1. Создайте групповую задачу *Формирование правил контроля запуска программ или выберите уже созданную задачу*.

2. Настройте задачу Формирование правил контроля запуска программ.

3. Запустите задачу Формирование правил контроля запуска программ.

После завершения задачи, в зависимости от настроек задачи:

- если в качестве действия по завершению задачи вы указали **Добавлять разрешающие правила в список правил контроля запуска программ**, то сформированные правила контроля запуска программ будут добавлены в список в настройках Контроля запуска программ в Консоли приложения.

- если в качестве действия по завершению задачи вы указали **Правила будут экспортированы в файл**, то сформированные правила контроля запуска программ будут сохранены в XML-файл, расположенный по указанному в настройках задачи пути.

Списки содержат разрешающие правила для запуска программ, расположение и тип которых соответствует настройкам, указанным в групповой задаче Формирование правил контроля запуска программ.

Контроль устройств

Контроль устройств управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.

Контроль устройств имеет следующие возможности:

- Управление правами доступа пользователей к запоминающим устройствам (например, съемные диски, мобильные телефоны, CD/DVD-приводы и другие).
- Контроль подключения устройств без файловой системы (например, внешние модемы, Bluetooth-адаптеры, USB-клавиатуры и другие).
- Управление подключением компьютера к сети Wi-Fi.

По умолчанию Контроль устройств выключен. При включении компонента Контроль устройств Kaspersky Industrial CyberSecurity for Nodes по умолчанию запрещает доступ к следующим типам устройств:

- съемные диски (включая USB-флешки);
- дискеты;
- CD/DVD-приводы;
- портативные устройства (MTP);
- модемы;
- устройства чтения смарт-карт;
- внешние сетевые адаптеры;
- Bluetooth (за исключением устройств ввода).

Уровни контроля доступа к устройствам

Kaspersky Industrial CyberSecurity for Nodes управляет доступом к устройствам на следующих уровнях:

1. **Тип устройства**.

   При подключении устройства к компьютеру операционная система определяет тип устройства: принтер, съемный диск, CD/DVD-привод и так далее. На этом уровне вы можете разрешить или запретить подключение устройств по их типу.

2. **Шина подключения**.

   Шина подключения – интерфейс, с помощью которого устройства подключаются к компьютеру. Некоторые типы устройств имеют несколько интерфейсов для подключения. Например, вы можете подключить принтер через USB или последовательный порт (COM).

   На этом уровне вы можете разрешить или запретить доступ к устройствам в зависимости от шины подключения.

Например, вы запретили доступ через шину подключения USB. Kaspersky Industrial CyberSecurity for Nodes запретит доступ ко всем типам устройств с режимом **Зависит от шины подключения** при их подключении через USB.

> Если для устройства выбран режим доступа **Разрешать** или **Запрещать**, управление доступом осуществляется вне зависимости шины подключения устройства.

3. **Доверенные устройства**.

   Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Режимы работы Контроля устройств

Контроль устройств может работать в следующих режимах:

- **Активный режим**.

  Kaspersky Industrial CyberSecurity for Nodes запрещает или разрешает использование устройств в соответствии с заданными правилами доступа к устройствам. Также приложение разрешает доступ к доверенным устройствам. Приложение регистрирует события подключения и отключения устройств.

- **Информировать**.

  Kaspersky Industrial CyberSecurity for Nodes разрешает использование всех устройств и регистрирует соответствующие события в журнале. Использование всех устройств разрешено. Этот режим установлен по умолчанию. Вы можете включить этот режим, чтобы провести аудит устройств в вашей организации и на основе этой информации сформировать список доверенных устройств.

О правилах доступа к устройствам

Правило доступа к устройствам – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам: доступ к устройству, расписание доступа, разрешение на чтение или запись и другие. Набор параметров правил доступа отличается в зависимости от типа устройств.

Параметры правила доступа

Устройства	Назначение пользователей / группы пользователей	Расписание доступа к устройству	Разрешение на чтение/запись	Контроль по шине подключения
Жесткие диски	✓	✓	✓	✓
Съемные диски (включая USB-флешки)	✓	✓	✓	✓
Дискеты	✓	✓	✓	✓
CD/DVD-приводы	✓	✓	✓	✓
Портативные устройства (MTP)	✓	✓	✓	✓
Локальные принтеры	✓	–	–	✓
Сетевые принтеры	✓	–	–	–
Модемы	–	–	–	✓
Стримеры	–	–	–	✓

Устройства	Назначение пользователей / группы пользователей	Расписание доступа к устройству	Разрешение на чтение/запись	Контроль по шине подключения
Многофункциональные устройства	–	–	–	✓
Устройства чтения смарт-карт	–	–	–	✓
Windows CE USB ActiveSync устройства	–	–	–	✓
Внешние сетевые адаптеры	–	–	–	✓
Bluetooth	–	–	–	–
Камеры и сканеры	–	–	–	✓
Wi-Fi	–	–	–	–
USB-клавиатуры	–	–	–	✓
USB-мыши	–	–	–	✓

Контроль доступа к устройствам по типу

Контроль устройств позволяет управлять доступом к устройствам по типу. Тип устройства определяет операционная система при подключении устройства. Вы можете узнать тип устройства с помощью встроенного в операционную систему инструмента Менеджер устройств. Для управления доступом к устройствам вам нужно настроить правила. *Правило доступа к устройствам* – набор параметров, которые определяют доступ пользователей к установленным или подключенным к компьютеру устройствам: доступ к устройству, расписание доступа, разрешение на чтение или запись и другие. Набор параметров правил доступа отличается в зависимости от типа устройств.

Вы можете настроить доступ к устройствам следующим образом:

- **Разрешать**.

  Kaspersky Industrial CyberSecurity for Nodes предоставляет полный доступ к устройствам для всех пользователей.

- **Запрещать**.

  Kaspersky Industrial CyberSecurity for Nodes блокирует подключение устройств. Приложение разрешает подключение только доверенных устройств.

- **Зависит от шины подключения**.

  Kaspersky Industrial CyberSecurity for Nodes определяет шину подключения устройства и управляет доступом в соответствии с режимом доступа для шины подключения. Также приложение разрешает подключение доверенных устройств.

- **По правилам**.

  Для некоторых типов устройств вы можете выбрать пользователей или группу пользователей, которым будет разрешено использование устройств, задать расписание для доступа к устройствам и настроить разрешения на чтение и запись. Также приложение разрешает подключение доверенных устройств.

Будьте осторожны при настройке доступа к типу устройств **Жесткие диски**. Если вы запретите доступ к системному диску, приложение может вызвать сбой при загрузке операционной системы (BSOD).

Если устройство выходит за рамки классификации Контроля устройств, ограничить доступ к таким устройствам невозможно.

Как контролировать доступ к устройствам по типу в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Контроль активности на компьютерах**.
4. В разделе **Контроль устройств** нажмите **Настройка**.
5. Установите флажок **Контроль устройств**.
6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.
7. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации Контроля устройств.
8. Настройте правила доступа к устройствам:

   a. Выберите режим доступа: **Разрешать**, **Запрещать**, **Зависит от шины подключения**, **По правилам**.

   Чтобы выбрать режим доступа **По правилам** вам нужно открыть свойства правила доступа двойным щелчком мыши.

   b. Если вы выбрали режим доступа **Зависит от шины подключения**, вам нужно перейти на закладку **Шины подключения** и настроить правила доступа для интерфейсов подключения.

   c. Для запоминающих устройств (например, съемных дисков) вы можете настроить права доступа для отдельных пользователей. Также вы можете задать расписание для доступа к устройствам и настроить разрешения на чтение и запись.

   d. Если требуется, настройте правила печати.

   e. Если требуется, настройте правила подключения компьютера к Wi-Fi.
9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как контролировать доступ к устройствам по типу в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.
5. Установите флажок **Включить контроль устройств**.
6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

7. В блоке **Настройки Контроля устройств** нажмите **Правила доступа для устройств и сетей Wi-Fi**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

8. Настройте правила доступа к устройствам:

   a. Выберите режим доступа: **Разрешать**, **Запрещать**, **Зависит от шины подключения**, **По правилам**.

      Если режим доступа недоступен в раскрывающемся меню, вам нужно открыть свойства правила доступа двойным щелчком мыши по типу устройств.

   b. Если вы выбрали режим доступа **Зависит от шины подключения**, вам нужно вернуться в окно с общими настройками Контроля устройств, нажать **Шины подключения** и настроить правила доступа для интерфейсов подключения.

   c. Для запоминающих устройств (например, съемных дисков) вы можете настроить права доступа для отдельных пользователей. Также вы можете задать расписание для доступа к устройствам и настроить разрешения на чтение и запись.

   d. Если требуется, настройте правила печати.

   e. Если требуется, настройте правила подключения компьютера к Wi-Fi.

9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как контролировать доступ к устройствам по типу в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. Установите флажок **Контроль устройств**.

4. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

5. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Настройте правила доступа к устройствам:

   a. Выберите режим доступа: **Разрешать**, **Запрещать**, **Зависит от шины подключения**, **По правилам**.

      Чтобы выбрать режим доступа **По правилам** вам нужно открыть свойства правила доступа двойным щелчком мыши.

   b. Если вы выбрали режим доступа **Зависит от шины подключения**, вам нужно перейти на вкладку **Шины подключения** и настроить правила доступа для интерфейсов подключения.

   c. Для запоминающих устройств (например, съемных дисков) вы можете настроить права доступа для отдельных пользователей. Также вы можете задать расписание для доступа к устройствам и настроить разрешения на чтение и запись.

d. Если требуется, настройте правила печати.

e. Если требуется, настройте правила подключения компьютера к Wi-Fi.

7. Сохраните внесенные изменения.

В результате при попытке пользователя получить доступ к устройству приложение заблокирует доступ в соответствии с правилами. Также Kaspersky Industrial CyberSecurity for Nodes зарегистрирует соответствующее событие. Если вы хотите предоставить доступ к отдельным устройствам, вы можете добавить эти устройства в список доверенных.

Контроль подключения к Wi-Fi

Контроль устройств позволяет управлять подключением компьютера (терминала) к сетям Wi-Fi. Публичные сети Wi-Fi могут быть не защищены, и использование таких сетей может привести к потере данных. С помощью компонента Контроль устройств вы можете запретить пользователю подключение к Wi-Fi или разрешить подключение только к доверенным сетям. Например, вы можете разрешить подключение только к корпоративной сети Wi-Fi, которая достаточно защищена. Контроль устройств будет блокировать доступ ко всем сетям Wi-Fi, кроме тех, которые указаны в списке доверенных.

На компьютерах под управлением Windows 11 для контроля подключения к Wi-Fi нужно включить службы определения местоположения. Для этого вам нужно включить переключатель **Службы определения местоположения** в параметрах операционной системы (**Настройки** → **Конфиденциальность и защита** → **Расположение**). Если службы определения местоположения выключены, Kaspersky Industrial CyberSecurity for Nodes не контролирует подключение к сетям Wi-Fi.

Как ограничить подключение к Wi-Fi в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Контроль активности на компьютерах**.
4. В разделе **Контроль устройств** нажмите **Настройка**.
5. Установите флажок **Контроль устройств**.
6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.
7. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации Контроля устройств.

8. Для типа устройств **Wi-Fi** настройте правило доступа:

   a. Выберите режим доступа: **Разрешать**, **Запрещать**, **Запрещать с исключениями**.

   b. Если вы выбрали режим доступа **Запрещать с исключениями**, вам нужно сформировать список доверенных сетей Wi-Fi:

      1. Откройте список доверенных сетей Wi-Fi двойным щелчком мыши по типу устройств **Wi-Fi**.

      2. В открывшемся окне нажмите на кнопку **Добавить**.

      3. В открывшемся окне задайте параметры доверенной сети Wi-Fi:

         - **Имя сети**. Имя сети Wi-Fi или SSID (Service Set Identifier).
         - **Тип аутентификации**. Тип аутентификации при подключении к сети Wi-Fi.
         - **Тип шифрования**. Тип шифрования, используемый для защиты трафика сети Wi-Fi.
         - **Комментарий**. Дополнительная информация о добавленной сети Wi-Fi.

   Вы можете посмотреть параметры доверенной сети Wi-Fi в параметрах роутера.

   > Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.

9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как ограничить подключение к Wi-Fi в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.

5. Установите флажок **Включить контроль устройств**.

6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

7. В блоке **Настройки Контроля устройств** нажмите **Правила доступа для устройств и сетей Wi-Fi**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

8. Откройте свойства правила доступа двойным щелчком мыши по типу устройств **Wi-Fi**.

9. Выберите режим доступа: **Разрешать**, **Запрещать**, **Запрещать с исключениями**.

10. Если вы выбрали режим доступа **Запрещать с исключениями**, вам нужно сформировать список доверенных сетей Wi-Fi:

    1. В блоке **Доверенные сети Wi-Fi** нажмите на кнопку **Добавить**.

    2. В открывшемся окне задайте параметры доверенной сети Wi-Fi:

        - **Имя сети**. Имя сети Wi-Fi или SSID (Service Set Identifier).
        - **Тип аутентификации**. Тип аутентификации при подключении к сети Wi-Fi.
        - **Тип шифрования**. Тип шифрования, используемый для защиты трафика сети Wi-Fi.
        - **Комментарий**. Дополнительная информация о добавленной сети Wi-Fi.

    Вы можете посмотреть параметры доверенной сети Wi-Fi в параметрах роутера.

    > Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.

11. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как ограничить подключение к Wi-Fi в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. Установите флажок **Контроль устройств**.

4. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

5. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Для типа устройств **Wi-Fi** настройте правило доступа:

    a. Выберите режим доступа: **Разрешать**, **Запрещать**, **Запрещать с исключениями**.

    b. Если вы выбрали режим доступа **Запрещать с исключениями**, вам нужно сформировать список доверенных сетей Wi-Fi:

        1. Откройте список доверенных сетей Wi-Fi двойным щелчком мыши по типу устройств **Wi-Fi**.

        2. В открывшемся окне нажмите на кнопку **Добавить**.

        3. В открывшемся окне задайте параметры доверенной сети Wi-Fi:

            - **Имя сети**. Имя сети Wi-Fi или SSID (Service Set Identifier).
            - **Тип аутентификации**. Тип аутентификации при подключении к сети Wi-Fi.

- **Тип шифрования**. Тип шифрования, используемый для защиты трафика сети Wi-Fi.
- **Комментарий**. Дополнительная информация о добавленной сети Wi-Fi.

Вы можете посмотреть параметры доверенной сети Wi-Fi в параметрах роутера.

Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.

7. Сохраните внесенные изменения.

В результате при попытке пользователя подключиться к сети Wi-Fi, которая не указана в списке доверенных, приложение заблокирует подключение.

Контроль печати

Контроль устройств позволяет настроить доступ пользователей к локальным и сетевым принтерам.

Контроль локальных принтеров

Kaspersky Industrial CyberSecurity for Nodes управляет подключением локальных принтеров по следующим шинам: USB, Последовательный порт (COM), Параллельный порт (LPT).

Kaspersky Industrial CyberSecurity for Nodes контролирует подключение локальных принтеров через COM и LPT только на уровне шины. То есть, чтобы запретить подключение принтеров через COM и LPT вам нужно для типа устройств **Локальные принтеры** выбрать режим **Зависит от шины подключения** и запретить подключение устройств к шинам COM и LPT.

Принтеры, подключенные через USB, приложение контролирует на двух уровнях: тип устройств (локальные принтеры) и шина подключения (USB).

Вы можете выбрать один следующих режимов доступа к локальным принтерам через USB:

- **Разрешать**. Kaspersky Industrial CyberSecurity for Nodes предоставляет полный доступ к локальным принтерам для всех пользователей. Пользователи могут подключать принтеры и печатать документы средствами операционной системы.
- **Запрещать**. Kaspersky Industrial CyberSecurity for Nodes блокирует подключение локальных принтеров. Приложение разрешает подключать только доверенные принтеры.
- **Зависит от шины подключения**. Kaspersky Industrial CyberSecurity for Nodes ограничивает доступ к локальным принтерам в соответствии со статусом подключения к шине USB (**Разрешать** ✓ или **Запрещать** ⊘).
- **По правилам**. Для контроля печати вам нужно добавить *правила печати*. В правилах вы можете выбрать пользователей или группу пользователей, которым будет разрешено или запрещено печатать документы на локальных принтерах.

Контроль сетевых принтеров

Kaspersky Industrial CyberSecurity for Nodes позволяет настроить доступ к печати на сетевых принтерах. Вы можете выбрать один следующих режимов доступа к сетевым принтерам:

- **Разрешать и не записывать в отчет** . Kaspersky Industrial CyberSecurity for Nodes не контролирует печать на сетевых принтерах. Приложение предоставляет доступ к печати на сетевых принтерах для всех пользователей и не сохраняет информацию о печати в журнал событий.
- **Разрешать** . Kaspersky Industrial CyberSecurity for Nodes предоставляет доступ к печати на сетевых принтерах для всех пользователей.
- **Запрещать** . Kaspersky Industrial CyberSecurity for Nodes ограничивает доступ к печати на сетевых принтерах для всех пользователей. Приложение разрешает доступ только к доверенным принтерам.
- **По правилам**. Для контроля печати вам нужно добавить *правила печати*. В правилах вы можете выбрать пользователей или группу пользователей, которым будет разрешено или запрещено печатать документы на сетевых принтерах.

Добавление правил печати для принтеров

Как добавить правила печати в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Контроль активности на компьютерах**.
4. В разделе **Контроль устройств** нажмите **Настройка**.
5. Установите флажок **Контроль устройств**.
6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.
7. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации Контроля устройств.
8. Настройте правила доступа к принтерам:

   a. Для типов устройств **Локальные принтеры** и **Сетевые принтеры** настройте правила доступа: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет** (только для сетевых принтеров), **Зависит от шины подключения** (только для локальных принтеров), **По правилам**.

   b. Если вы выбрали режим доступа **Зависит от шины подключения**, вам нужно перейти на закладку **Шины подключения** и настроить правила доступа для интерфейсов подключения.

c. Если вы выбрали режим доступа **По правилам**, вам нужно настроить правила печати:

1. Откройте список правил печати двойным щелчком мыши по типу устройств **Локальные принтеры** и **Сетевые принтеры**.

2. Выберите пользователей или группы пользователей, к которым вы хотите применить правило печати. Для этого нажмите на кнопку **Добавить**.

   Откроется окно добавления нового правила печати.

3. Назначьте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, действие (разрешено/запрещено) и приоритет.

   Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

   Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

   Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи запрещающей доступ к устройству.

4. В блоке **Действие** настройте доступ пользователя к печати на принтере.

5. Нажмите на кнопку **Пользователи и группы** и выберите пользователей или группы пользователей для доступа к печати. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

6. Нажмите на кнопку **OK**.

9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как добавить правила печати в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.

5. Установите флажок **Включить контроль устройств**.

6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

7. В блоке **Настройки Контроля устройств** нажмите **Правила доступа для устройств и сетей Wi-Fi**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

8. Настройте правила доступа к принтерам:

   a. Для типов устройств **Локальные принтеры** и **Сетевые принтеры** выберите режим доступа: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет** (только для сетевых принтеров), **Зависит от шины подключения** (только для локальных принтеров), **По правилам**.

   Если режим доступа недоступен в раскрывающемся меню, вам нужно открыть свойства правила доступа двойным щелчком мыши по типу устройств.

   b. Если вы выбрали режим доступа **Зависит от шины подключения**, вам нужно вернуться в окно с общими настройками компонента Контроль устройств, нажать **Шины подключения** и настроить правила доступа для интерфейсов подключения.

   c. Если вам нужно настроить печать, выполните следующие действия:

      1. Откройте свойства правила доступа двойным щелчком мыши по типу устройств **Локальные принтеры** или **Сетевые принтеры**.

      2. Выберите режим доступа **По правилам**.

      3. Выберите пользователей или группы пользователей, к которым вы хотите применить правило печати. Для этого нажмите на кнопку **Добавить**.

         Откроется окно добавления нового правила печати.

      4. Назначьте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, действие (разрешено/запрещено) и приоритет.

         Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

         Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

         Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи запрещающей доступ к устройству.

      5. В блоке **Действие** настройте доступ пользователя к печати на принтере.

      6. В блоке **Пользователи и группы** нажмите на кнопку **Добавить** и выберите пользователей или группы пользователей для доступа к печати. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

      7. Нажмите на кнопку **ОК**.

9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки 🔒.

Как добавить правила печати в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. Установите флажок **Контроль устройств**.

4. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

5. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Настройте правила доступа к принтерам:

   a. Для типов устройств **Локальные принтеры** и **Сетевые принтеры** настройте правила доступа: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет** (только для сетевых принтеров), **Зависит от шины подключения** (только для локальных принтеров), **По правилам**.

   b. Если вы выбрали режим доступа **Зависит от шины подключения**, вам нужно перейти на закладку **Шины подключения** и настроить правила доступа для интерфейсов подключения.

   c. Если вы выбрали режим доступа **По правилам**, вам нужно настроить правила печати:

      1. Откройте список правил печати двойным щелчком мыши по типу устройств **Локальные принтеры** и **Сетевые принтеры**.

      2. Выберите пользователей или группы пользователей, к которым вы хотите применить правило печати. Для этого нажмите на кнопку **Добавить**.

         Откроется окно добавления нового правила печати.

      3. Назначьте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, действие (разрешено/запрещено) и приоритет.

         Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

         Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

         Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи запрещающей доступ к устройству.

      4. В блоке **Действие** настройте доступ пользователя к печати на принтере.

5. Нажмите на кнопку **Пользователи и группы** и выберите пользователей или группы пользователей для доступа к печати. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

6. Нажмите на кнопку **OK**.

7. Сохраните внесенные изменения.

Контроль устройств ввода (HID)

К устройствам ввода относятся клавиатуры, мыши, трекболы, тачпады и другие устройства. Вы можете подключать устройства ввода с помощью следующих интерфейсов: USB, Bluetooth, порт PS/2, последовательный порт RS-232 (COM), ИК-порт и другие.

Kaspersky Industrial CyberSecurity for Nodes позволяет контролировать мыши и клавиатуры, подключенные через USB и Bluetooth. Контроль устройств регистрирует события подключения и отключения устройств ввода.

При подключении или отключении Bluetooth-устройств приложение может создавать несколько событий о действиях с устройством. Это связано с тем, что операционная система может определять Bluetooth-устройство как несколько устройств разных типов. Также Kaspersky Industrial CyberSecurity for Nodes контролирует Bluetooth-адаптер, через который подключено устройство, как отдельное устройство. Поэтому приложение создает событие для всех обнаруженных устройств.

Kaspersky Industrial CyberSecurity for Nodes позволяет разрешить, запретить использование устройств ввода, а также сформировать список доверенных устройств.

Как настроить контроль устройств ввода в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне свойств политики выберите **Контроль активности на компьютерах**.

4. В разделе **Контроль устройств** нажмите **Настройка**.

5. Установите флажок **Контроль устройств**.

6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

7. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации Контроля устройств.

8. Для типа устройств **Bluetooth** выберите режим доступа: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.

   Вы можете запретить или разрешить все Bluetooth-устройства или вы можете разрешить подключение только устройств ввода по Bluetooth (класс HID-устройств – Human Interface Devices).

Вы можете разрешить подключение устройств ввода только в Web Console. Разрешить подключение устройств ввода в Консоли администрирования (MMC) и Консоли Kaspersky Industrial CyberSecurity for Nodes невозможно.

9. Для типов устройств **USB-клавиатуры** и **USB-мыши** выберите правила доступа: **Разрешать**, **Запрещать**, **Зависит от шины подключения**.

10. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как настроить контроль устройств ввода в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.

5. Установите флажок **Включить контроль устройств**.

6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

7. В блоке **Настройки Контроля устройств** нажмите **Правила доступа для устройств и сетей Wi-Fi**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

8. Откройте свойства правила доступа щелчком мыши по типу устройств **Bluetooth**

9. Выберите режим доступа: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.

   Вы можете запретить или разрешить все Bluetooth-устройства или вы можете разрешить подключение только устройств ввода по Bluetooth (класс HID-устройств – Human Interface Devices).

10. Для типов устройств **USB-клавиатуры** и **USB-мыши** выберите правила доступа: **Разрешать**, **Запрещать**, **Зависит от шины подключения**.

11. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как настроить контроль устройств ввода в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. Установите флажок **Контроль устройств**.

4. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

5. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Для типа устройств **Bluetooth** выберите режим доступа: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.

   Вы можете запретить или разрешить все Bluetooth-устройства или вы можете разрешить подключение только устройств ввода по Bluetooth (класс HID-устройств – Human Interface Devices).

   > Вы можете разрешить подключение устройств ввода только в Web Console. Разрешить подключение устройств ввода в Консоли администрирования (MMC) и Консоли Kaspersky Industrial CyberSecurity for Nodes невозможно.

7. Для типов устройств **USB-клавиатуры** и **USB-мыши** выберите правила доступа: **Разрешать**, **Запрещать**, **Зависит от шины подключения**.

8. Сохраните внесенные изменения.

Контроль доступа к мобильным устройствам

Kaspersky Industrial CyberSecurity for Nodes позволяет управлять доступом к данным на мобильных устройствах под управлением Android и iOS. Мобильные устройства относятся к портативным устройствам (MTP). Поэтому, чтобы настроить доступ к данным на мобильных устройствах вам нужно перейти в настройки доступа к портативным устройствам (MTP).

При подключении мобильного устройства к компьютеру операционная система определяет тип устройства. Если на компьютере установлены приложения Android Debug Bridge (подробнее о приложении ADB см. в Базе знаний и на сайте Службы технической поддержки Android), iTunes или их аналоги, операционная система определяет мобильные устройства как ADB- или iTunes-устройства. В остальных случаях операционная система может определить тип мобильного устройства как портативное устройство (MTP) для передачи файлов, PTP-устройство (камера) для передачи изображений или другое устройство. Тип устройства зависит от модели мобильного устройства и выбранного режима подключения по USB. Kaspersky Industrial CyberSecurity for Nodes позволяет настроить отдельные права доступа к данным на мобильных устройствах в приложениях ADB, iTunes или файловом менеджере. В остальных случаях Контроль устройств предоставляет доступ к мобильным устройствам согласно правилам доступа к портативным устройствам (MTP).

Доступ к мобильным устройствам

Так как мобильные устройства относятся к портативным устройствам (MTP), настройки доступа у этих устройств общие. Вы можете выбрать один из следующих режимов доступа к мобильным устройствам:

- **Разрешать**. Kaspersky Industrial CyberSecurity for Nodes предоставляет полный доступ к мобильным устройствам. Вы можете открывать, создавать, изменять, копировать или удалять файлы на мобильных устройствах с помощью файлового менеджера или приложений ADB и iTunes. Также вы можете заряжать батарею устройства, подключив мобильное устройство через USB к компьютеру.

- **Запрещать**. Kaspersky Industrial CyberSecurity for Nodes ограничивает доступ к мобильным устройствам в файловом менеджере и приложениях ADB и iTunes. Приложение разрешает доступ только к доверенным мобильным устройствам. Также вы можете заряжать батарею устройства, подключив мобильное устройство через USB к компьютеру.

- **Зависит от шины подключения**. Kaspersky Industrial CyberSecurity for Nodes ограничивает доступ к мобильным устройствам в соответствии со статусом подключения к шине USB (**Разрешать** или **Запрещать**).

- **По правилам**. Kaspersky Industrial CyberSecurity for Nodes ограничивает доступ к мобильным устройствам в соответствии с правилами. В правилах вы можете настроить права доступа (чтение/запись), выбрать пользователей или группу пользователей, которые имеют доступ к мобильным устройствам и задать расписание доступа к мобильным устройствам. Также вы можете ограничить доступ к данным на мобильных устройствах через приложения ADB и iTunes.

Настройка правил доступа к мобильным устройствам

Настройка правил доступа для портативных устройств (MTP), ADB- и iTunes-устройств отличается. Для портативных устройств (MTP) и ADB-устройств вы можете назначать правила для отдельных пользователей или групп пользователей и составлять расписание работы правил. Для iTunes-устройств таких возможностей нет. Вы можете только разрешить или запретить доступ к данным через приложение iTunes для всех пользователей.

Как настроить правила доступа к мобильным устройствам в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Контроль активности на компьютерах**.
4. В разделе **Контроль устройств** нажмите **Настройка**.
5. В блоке **Настройки Контроля устройств** выберите вкладку **Типы устройств**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.
6. В контекстном меню для типа устройств **Портативные устройства (MTP)** настройте режим доступа к мобильным устройствам: **Разрешать**, **Запрещать** или **Зависит от шины подключения**.
7. Для настройки правил доступа к мобильным устройствам откройте список правил двойным щелчком мыши.
8. Настройте правило доступа к мобильным устройствам:

   a. В блоке **Правила доступа** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к мобильным устройствам.

   b. В поле **Приоритет** задайте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись / доступ через ADB) и приоритет.

      Запись правила имеет приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи, запрещающей доступ к устройству.

c. В блоке **Правило для пользователей и групп** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

d. Нажмите на кнопку **OK**.

9. В блоке **Расписания для выбранного правила доступа** настройте расписание доступа к мобильным устройствам для пользователей.

   Настроить отдельное расписание доступа к ADB-устройствам невозможно. Вы можете настроить общее расписание для ADB-устройств и портативных устройств (MTP).

10. Настройте разрешения пользователей для доступа к мобильным устройствам в файловом менеджере (**Чтение** / **Запись**).

11. Настройте доступ к данным мобильного устройства через приложение ADB с помощью флажка **Доступ через ADB**.

    Если флажок снят, при подключении мобильного устройства приложение ADB не сможет обнаружить устройство.

12. В блоке **Доступ через iTunes** настройте доступ к данным мобильного устройства через приложение iTunes.

    Kaspersky Industrial CyberSecurity for Nodes применяет настройки доступа к мобильным устройствам через приложение iTunes для всех пользователей. Настроить отдельное расписание доступа к iTunes-устройствам невозможно.

13. Сохраните внесенные изменения.

Как настроить правила доступа к мобильным устройствам в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.

5. В блоке **Настройки Контроля устройств** перейдите по ссылке **Правила доступа для устройств и сетей Wi-Fi**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Выберите тип устройств **Портативные устройства (MTP)**.

   Откроются правила доступа к портативным устройствам (MTP).

7. Настройте режим доступа к мобильным устройствам: **Разрешать**, **Запрещать**, **Зависит от шины подключения** или **По правилам**.

8. В блоке **Доступ через iTunes** настройте доступ к данным мобильного устройства через приложение iTunes.

   Kaspersky Endpoint Security применяет настройки доступа к мобильным устройствам через приложение iTunes для всех пользователей. Настроить отдельное расписание доступа к iTunes-устройствам невозможно.

9. Если вы выбрали режим **По правилам**, вам нужно добавить правила доступа к устройствам. Для этого в блоке **Пользователи** нажмите на кнопку **Добавить** и настройте правило доступа к мобильным устройствам:

   a. В поле **Приоритет** задайте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись / доступ через ADB) и приоритет.

      Запись правила имеет приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи, запрещающей доступ к устройству.

   b. В блоке **Пользователи** выберите пользователей или группы пользователей для доступа к мобильным устройствам. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   c. В блоке **Расписание доступа к устройствам** настройте расписание доступа к мобильным устройствам для пользователей.

      Настроить отдельное расписание доступа к ADB-устройствам невозможно. Вы можете настроить общее расписание для ADB-устройств и портативных устройств (MTP).

   d. Настройте разрешения пользователей для доступа к мобильным устройствам в файловом менеджере (**Чтение** / **Запись**).

   e. Настройте доступ к данным мобильного устройства через приложение ADB с помощью флажка **Доступ через ADB**.

      Если флажок снят, при подключении мобильного устройства приложение ADB не сможет обнаружить устройство.

10. Сохраните внесенные изменения.

Как настроить правила доступа к мобильным устройствам в консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. Выберите вкладку **Типы устройств**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. В контекстном меню для типа устройств **Портативные устройства (MTP)** настройте режим доступа к мобильным устройствам: **Разрешать**, **Запрещать** или **Зависит от шины подключения**.

5. Для настройки правил доступа к мобильным устройствам откройте список правил двойным щелчком мыши.

6. Настройте правило доступа к мобильным устройствам:

   a. В блоке **Правила доступа** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к мобильным устройствам.

   b. В поле **Приоритет** задайте приоритет записи правила. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтения / запись / доступ через ADB) и приоритет.

      Запись правила имеет приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи, запрещающей доступ к устройству.

   c. В блоке **Правило для пользователей и групп** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   d. Нажмите на кнопку **OK**.

7. В блоке **Расписания для выбранного правила доступа** настройте расписание доступа к мобильным устройствам для пользователей.

   > Настроить отдельное расписание доступа к ADB-устройствам невозможно. Вы можете настроить общее расписание для ADB-устройств и портативных устройств (MTP).

8. Настройте разрешения пользователей для доступа к мобильным устройствам в файловом менеджере (**Чтение** / **Запись**).

9. Настройте доступ к данным мобильного устройства через приложение ADB с помощью флажка **Доступ через ADB**.

   Если флажок снят, при подключении мобильного устройства приложение ADB не сможет обнаружить устройство.

10. В блоке **Доступ через iTunes** настройте доступ к данным мобильного устройства через приложение iTunes.

    Kaspersky Industrial CyberSecurity for Nodes применяет настройки доступа к мобильным устройствам через приложение iTunes для всех пользователей. Настроить отдельное расписание доступа к iTunes-устройствам невозможно.

11. Сохраните внесенные изменения.

В результате пользователям будет ограничен доступ к мобильным устройствам согласно правилам. Если вы запретили доступ к мобильным устройствам в приложениях ADB и iTunes, при подключении мобильного устройства приложения ADB и iTunes не смогут обнаружить мобильное устройство.

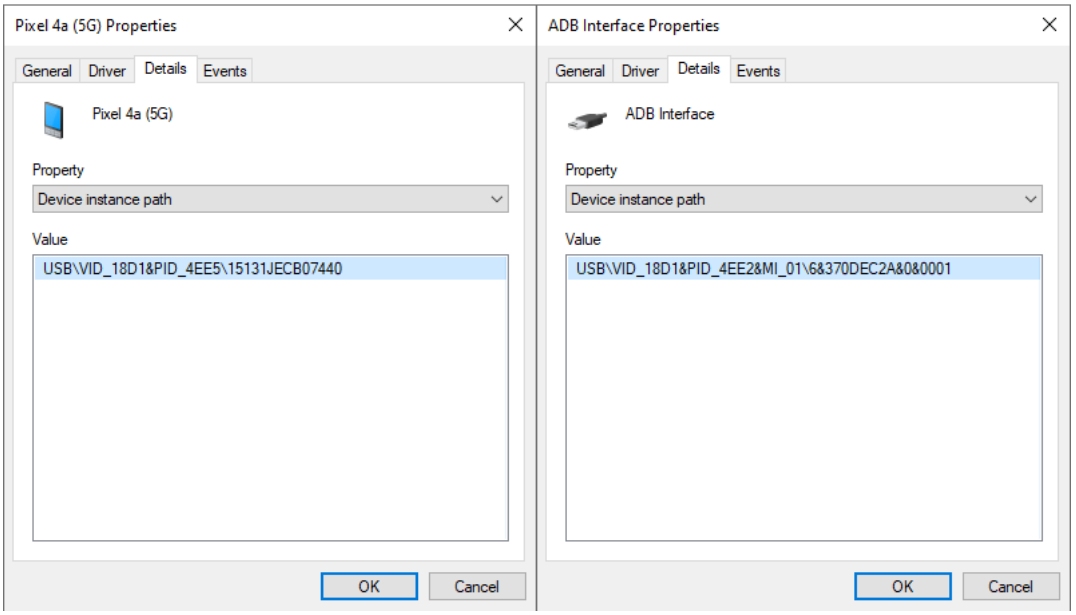
Доверенные мобильные устройства

Добавление доверенного мобильного устройства ничем не отличается от добавления других типов доверенных устройств. Вы можете добавить мобильное устройство по идентификатору или модели устройства.

Для добавления доверенного мобильного устройства по идентификатору, вам понадобится уникальный идентификатор (англ. Hardware ID, HWID). Вы можете просмотреть идентификатор в свойствах устройства средствами операционной системы (см. рис. ниже). Для этого предназначен инструмент Диспетчер устройств (англ. Device Manager). Идентификаторы для портативных устройств (MTP) и ADB-, iTunes-устройств отличаются, даже если это одно мобильное устройство. Пример идентификатора портативного устройства (MTP): `15131JECB07440`. Пример идентификатора ADB-устройства: `6&370DEC2A&0&0001`. Добавлять устройства по идентификатору удобно, если вы хотите добавить несколько определенных устройств. Также вы можете использовать маски.

Если вы установили приложение ADB или iTunes после подключения устройства к компьютеру, уникальный идентификатор устройства может быть сброшен. То есть, Kaspersky Industrial CyberSecurity for Nodes определит это устройство как новое. Если устройство доверенное, добавьте устройство в список доверенных повторно.

Для добавления доверенного мобильного устройства по модели, вам понадобятся идентификатор производителя (англ. Vendor ID, VID) и идентификатор продукта (англ. Product ID, PID). Вы можете просмотреть идентификаторы в свойствах устройства средствами операционной системы (см. рис. ниже). Шаблон для ввода VID и PID: `VID_18D1&PID_4EE5`. Добавлять устройства по модели удобно, если вы используете в вашей организации устройства определенной модели. Таким образом, вы можете добавить все устройства этой модели.



Идентификатор устройства в Диспетчере устройств

Мониторинг использования съемных дисков

Мониторинг использования съемных дисков включает в себя следующие инструменты:

- Контроль операций с файлами на съемных дисках.
- Контроль подключения и отключения доверенных съемных дисков.

  Kaspersky Industrial CyberSecurity for Nodes позволяет контролировать подключение и отключение всех доверенных устройств, не только съемных дисков. Вы можете включить запись событий в параметрах уведомлений для компонента Контроль устройств. События имеют уровень важности *Информационное*.

Как включить контроль операций с файлами на съемных дисках в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Контроль активности на компьютерах**.
4. В разделе **Контроль устройств** нажмите **Настройка**.
5. Установите флажок **Контроль устройств**.
6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

7. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации Контроля устройств.

8. Выберите тип устройств **Съемные диски** и нажмите на кнопку **Запись событий в журнал**.

   Откроется окно настройки записи событий в журнал.

9. Установите флажок **Включить запись событий в журнал**.

10. В блоке **Операции с файлами** выберите операции, которые вы хотите контролировать: **Запись**, **Удаление**.

11. В блоке **Фильтр по форматам файлов** выберите форматы файлов, информацию об операциях с которыми Контроль устройств должен записывать в журнал.

12. Выберите пользователей или группы пользователей, использование съемных дисков которых вы хотите контролировать.

13. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как включить контроль операций с файлами на съемных дисках в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.

5. Установите флажок **Включить контроль устройств**.

6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

7. В блоке **Настройки Контроля устройств** нажмите **Правила доступа для устройств и сетей Wi-Fi**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

8. Откройте свойства правила доступа двойным щелчком мыши по типу устройств **Съемные диски**.

9. В открывшемся окне перейдите на закладку **Запись событий в журнал**.

10. Переведите переключатель в положение **Запись событий в журнал ВКЛЮЧЕНА**.

11. В блоке **Операции с файлами** выберите операции, которые вы хотите контролировать: **Запись**, **Удаление**.

12. В блоке **Фильтр по форматам файлов** выберите форматы файлов, информацию об операциях с которыми Контроль устройств должен записывать в журнал.

13. Выберите пользователей или группы пользователей, использование съемных дисков которых вы хотите контролировать.

14. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как включить контроль операций с файлами на съемных дисках в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. Установите флажок **Контроль устройств**.

4. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

5. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Выберите тип устройств **Съемные диски** и нажмите на кнопку **Запись событий в журнал**.

   Откроется окно настройки записи событий в журнал.

7. Установите флажок **Включить запись событий в журнал**.

8. В блоке **Операции с файлами** выберите операции, которые вы хотите контролировать: **Запись**, **Удаление**.

9. В блоке **Фильтр по форматам файлов** выберите форматы файлов, информацию об операциях с которыми Контроль устройств должен записывать в журнал.

10. Выберите пользователей или группы пользователей, использование съемных дисков которых вы хотите контролировать.

11. Сохраните внесенные изменения.

В результате, когда пользователи будут производить запись в файлы, расположенные на съемных дисках, или удалять файлы со съемных дисков, Kaspersky Industrial CyberSecurity for Nodes будет сохранять информацию о совершенной операции в журнал событий и отправлять события в Kaspersky Security Center. Вы можете просмотреть события, связанные с файлами на съемных дисках, в консоли Kaspersky Security Center в рабочей области для узла **Сервер администрирования** на закладке **События**. Чтобы события отображались в локальном журнале событий Kaspersky Industrial CyberSecurity for Nodes, требуется установить флажок **Выполнена операция с файлом** в параметрах уведомлений для компонента Контроль устройств.

Контроль доступа к Bluetooth-устройствам

Kaspersky Industrial CyberSecurity for Nodes позволяет управлять доступом к устройствам, подключенным по Bluetooth. К Bluetooth-устройствам относятся беспроводные клавиатуры, мыши, гарнитуры, принтеры и т.д. Также вы можете использовать Bluetooth для обмена данными, например, с мобильным устройством.

При подключении или отключении Bluetooth-устройств приложение может создавать несколько событий о действиях с устройством. Это связано с тем, что операционная система может определять Bluetooth-устройство как несколько устройств разных типов. Также Kaspersky Industrial CyberSecurity for Nodes контролирует Bluetooth-адаптер, через который подключено устройство, как отдельное устройство. Поэтому приложение создает событие для всех обнаруженных устройств.

Вы можете выбрать один из следующих режимов доступа к Bluetooth-устройствам:

- **Разрешать и не записывать в отчет** . Kaspersky Industrial CyberSecurity for Nodes позволяет подключать любые Bluetooth-устройства и не сохраняет информацию о подключении в журнал событий. Вы можете подключать устройства ввода по Bluetooth (клавиатуры, мыши и т.п.), передавать данные по Bluetooth, управлять другими устройствами по Bluetooth (гарнитура, наушники и т.п.).
- **Разрешать** . Kaspersky Industrial CyberSecurity for Nodes позволяет подключать любые Bluetooth-устройства. Вы можете подключать устройства ввода по Bluetooth (клавиатуры, мыши и т.п.), передавать данные по Bluetooth, управлять другими устройствами по Bluetooth (гарнитура, наушники и т.п.).
- **Запрещать** . Kaspersky Industrial CyberSecurity for Nodes ограничивает доступ к Bluetooth-устройствам. Вы можете разрешить подключение только устройств ввода по Bluetooth (класс HID-устройств – Human Interface Devices). К этим устройствам относятся клавиатуры, мыши, джойстики и т.п.

Сформировать список доверенных Bluetooth-устройств невозможно. Если вы ограничили доступ к Bluetooth-устройствам, вы можете разрешить подключение только устройств ввода по Bluetooth.

Вы можете разрешить подключение устройств ввода только в Консоли приложения или в Web Console. Разрешить подключение устройств ввода в Консоли администрирования Kaspersky Security Center невозможно.

Как настроить правила доступа к Bluetooth-устройствам в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль активности на компьютерах** → **Контроль устройств** и нажмите **Настройка**.
4. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

5. В контекстном меню для типа устройств **Bluetooth** настройте режим доступа к Bluetooth-устройствам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.

   Если вы запретили доступ к Bluetooth-устройствам, вы можете разрешить подключение только устройств ввода (клавиатуры, мыши и т.п.) в Консоли приложения или в Web Console. Разрешить подключение устройств ввода в Консоли администрирования Kaspersky Security Center невозможно.

6. Сохраните внесенные изменения.

Как настроить правила доступа к Bluetooth-устройствам в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.
4. В окне политики выберите **Контроль активности на компьютерах** → **Контроль устройств** и нажмите **Настройка**.
5. В блоке **Настройки Контроля устройств** перейдите по ссылке **Правила доступа для устройств и сетей Wi-Fi**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Выберите тип устройств **Bluetooth**.

   Откроются настройки доступа к Bluetooth-устройствам.

7. Настройте режим доступа к Bluetooth-устройствам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.
8. Если вы выбрали режим **Запрещать**, вы можете разрешить подключение только устройств ввода по Bluetooth (клавиатуры, мыши и т.п.). Для этого в блоке **Исключения** установите флажок **Устройства ввода (мыши и клавиатуры)**.
9. Сохраните внесенные изменения.

Как настроить правила доступа к Bluetooth-устройствам в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.
2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   В таблице находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. В блоке **Доступ** настройте режим доступа к Bluetooth-устройствам: **Разрешать**, **Запрещать**, **Разрешать и не записывать в отчет**.

5. Если вы выбрали режим **Запрещать**, вы можете разрешить подключение только устройств ввода по Bluetooth (клавиатуры, мыши и т.п.). Для этого в блоке **Исключения** установите флажок **Устройства ввода (мыши и клавиатуры)**.

6. Сохраните внесенные изменения.

Разграничение прав доступа пользователей к устройствам

Вы можете настроить права доступа пользователей по типу устройств или к доверенным устройствам.

Разграничение прав доступа пользователей по типу устройств

Контроль устройств позволяет настроить права доступа пользователей к данным на *запоминающих устройствах*. Для этих устройств вы можете настроить разрешения на запись и чтение. Контроль устройств поддерживает следующие типы запоминающих устройств:

- Жесткие диски.
- Съемные диски.
- Дискеты.
- CD/DVD-приводы.
- Портативные устройства (MTP). К портативным устройствам (MTP) относятся, например, мобильные устройства, фотокамеры, медиаплееры и другие.

Таким образом, вы можете, например, разрешить использование съемных дисков только группе администраторов. Для других типов устройств вы можете или запретить, или разрешить доступ для всех пользователей. Также вы можете настроить права доступа пользователей при работе с принтерами.

Как настроить права доступа пользователей к данным на запоминающих устройствах в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Контроль активности на компьютерах**.
4. В разделе **Контроль устройств** нажмите **Настройка**.
5. Установите флажок **Контроль устройств**.
6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.
7. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации Контроля устройств.

8. Для настройки правил доступа к запоминающим устройствам откройте список правил двойным щелчком мыши.

9. Настройте правило доступа к запоминающим устройствам:

   a. В блоке **Правила доступа** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к запоминающим устройствам.

   b. В поле **Приоритет** задайте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтение/запись) и приоритет.

      Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи запрещающей доступ к устройству.

   c. В блоке **Правило для пользователей и групп** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   d. Нажмите на кнопку **OK**.

10. В блоке **Расписания для выбранного правила доступа** настройте расписание доступа к запоминающим устройствам для пользователей.

    Например, вы можете разрешить пользователям работать с запоминающими устройствами только в рабочее время.

11. Настройте разрешения пользователей для доступа к запоминающим устройствам в файловом менеджере (**Чтение/Запись**).

12. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как настроить права доступа пользователей к данным на запоминающих устройствах в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль активности на компьютерах → Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.

5. Установите флажок **Включить контроль устройств**.

6. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

7. В блоке **Настройки Контроля устройств** нажмите **Правила доступа для устройств и сетей Wi-Fi**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

8. В блоке **Доступ к запоминающим устройствам** откройте свойства правила доступа к запоминающим устройствам.

9. Настройте правило доступа к запоминающим устройствам:

   a. В блоке **Пользователи** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к запоминающим устройствам.

   b. В поле **Приоритет** задайте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтение/запись) и приоритет.

      Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи запрещающей доступ к устройству.

   c. В блоке **Пользователи** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   d. В блоке **Расписание доступа к устройствам** настройте расписание доступа к запоминающим устройствам для пользователей.

      Например, вы можете разрешить пользователям работать с запоминающими устройствами только в рабочее время.

   e. Настройте разрешения пользователей для доступа к запоминающим устройствам в файловом менеджере (**Чтение**/**Запись**).

   f. Нажмите на кнопку **OK**.

10. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как настроить права доступа пользователей к данным на запоминающих устройствах в Консоли Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. Установите флажок **Контроль устройств**.

4. В блоке **Режим работы для блокирующих правил** выберите **Блокировать** или **Информировать**.

5. В блоке **Настройки Контроля устройств** выберите закладку **Типы устройств**.

   Откроется окно с правилами доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

6. Для настройки правил доступа к запоминающим устройствам откройте список правил двойным щелчком мыши.

7. Настройте правило доступа к запоминающим устройствам:

   a. В блоке **Правила доступа** нажмите на кнопку **Добавить**.

      Откроется окно добавления нового правила доступа к запоминающим устройствам.

   b. В поле **Приоритет правила** задайте приоритет *записи правила*. Запись правила включает в себя следующие атрибуты: учетная запись, расписание, разрешения (чтение/запись) и приоритет.

      Запись правила имеют приоритет. Если пользователь добавлен в несколько групп, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ к устройству по записи правила с высшим приоритетом. Kaspersky Industrial CyberSecurity for Nodes позволяет назначить приоритет от 0 до 10 000. Чем больше значение, тем выше приоритет. То есть, запись со значением 0 имеет наименьший приоритет.

      Например, вы можете предоставить разрешение только на чтение для группы "Все" и разрешение на чтение и запись для группы администраторов. Для этого назначьте записи для группы администраторов приоритет 1, а группе "Все" приоритет 0.

      Приоритет запрещающей записи правила выше приоритета разрешающей записи. То есть, если пользователь добавлен в несколько групп и приоритет записей правила одинаковый, Kaspersky Industrial CyberSecurity for Nodes регулирует доступ по записи запрещающей доступ к устройству.

   c. В блоке **Правило для пользователей и групп** выберите пользователей или группы пользователей. Вы можете выбрать пользователей в Active Directory или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно.

   d. Нажмите на кнопку **OK**.

8. В блоке **Расписания для выбранного правила доступа** настройте расписание доступа к запоминающим устройствам для пользователей.

   Например, вы можете разрешить пользователям работать с запоминающими устройствами только в рабочее время.

9. Настройте разрешения пользователей для доступа к запоминающим устройствам в файловом менеджере (**Чтение**/**Запись**).

10. Сохраните внесенные изменения.

Разграничение прав доступа пользователей к доверенным устройствам

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства. Для работы с доверенными устройствами вы можете предоставить доступ отдельному пользователю, группе пользователей или всем пользователям организации. Вы можете настроить права доступа пользователей в свойствах доверенного устройства.

О формировании правил контроля устройств

Вы можете сформировать правила контроля устройств с помощью задач и политик Kaspersky Security Center одновременно для всех защищаемых устройств и групп защищаемых устройств в сети организации. Для создания списка доверенных устройств вам нужно выполнить аудит внешних устройств в вашей организации.

Для создания списка правил на основе перечня устройств, подключенных к отдельному защищаемому устройству, вы можете запустить задачу *Формирование правил контроля устройств* локально с помощью Консоли приложения.

Вы можете сформировать правила контроля устройств с помощью Kaspersky Security Center следующими способами:

- С помощью задачи *Формирование правил контроля устройств*.

  Задача *Формирование правил контроля устройств* в зависимости от заданных настроек может собирать данные обо всех устройствах, которые когда-либо были подключены к компьютеру, и информация о которых хранится в операционной системе, или об устройствах, которые подключены во время запуска задачи. На основании собранных данных задача формирует список разрешающих правил для компонента Контроль устройств. Вы можете настроить автоматический импорт сформированных правил в список правил компонента Контроль устройств или импортировать сформированные правила вручную.

  Этот сценарий может быть использован, например, если требуется быстро сформировать разрешающие правила для уже использовавшихся доверенных устройств перед первым запуском компонента Контроль устройств.

  Как запустить задачу Формирование правил контроля устройств в Консоли администрирования Kaspersky Security Center

  1. Откройте Консоль администрирования Kaspersky Security Center.
  2. В дереве консоли выберите папку **Задачи**.
  3. Выберите задачу *Формирование правил контроля устройств* и откройте свойства задачи двойным щелчком мыши.

     Если требуется, создайте новую задачу.
  4. В блоке **Режим** выберите режим работы задачи:

     - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**.

       Приложение получает данные обо всех устройствах, которые были подключены к компьютеру, из памяти операционной системы.

     - **Учитывать данные только об устройствах, подключенных в текущий момент**.

       Приложение получает данные об устройствах, которые подключены во время запуска задачи.
  5. Введите путь для сохранения файла с данными.
  6. Если задача будет запущена на нескольких компьютерах, рекомендуется установить флажок **Добавлять информацию о защищаемом устройстве в имя файла.**

7. Сохраните внесенные изменения.

8. Запустите задачу.

Как запустить задачу Формирование правил контроля устройств в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Выберите задачу *Формирование правил контроля устройств* и откройте свойства задачи двойным щелчком мыши.

   Если требуется, создайте новую задачу.

3. В блоке **Режим** выберите режим работы задачи:

   - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**.

     Приложение получает данные обо всех устройствах, которые были подключены к компьютеру, из памяти операционной системы.

   - **Учитывать данные только об устройствах, подключенных в текущий момент**.

     Приложение получает данные об устройствах, которые подключены во время запуска задачи.

4. Введите путь для сохранения файла с данными.

5. Если задача будет запущена на нескольких компьютерах, рекомендуется установить флажок **Добавлять информацию о защищаемом устройстве в имя файла**.

6. Сохраните внесенные изменения.

7. Запустите задачу.

Как запустить задачу Формирование правил контроля устройств в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Автоматическое формирование правил** → **Формирование правил контроля устройств**.

2. В панели результатов узла **Формирование правил контроля устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Формирование правил контроля устройств**.

3. В блоке **Режим** выберите режим работы задачи:

   - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**.

     Приложение получает данные обо всех устройствах, которые были подключены к компьютеру, из памяти операционной системы.

   - **Учитывать данные только об устройствах, подключенных в текущий момент**.

     Приложение получает данные об устройствах, которые подключены во время запуска задачи.

4. В разделе **После завершения задачи** выберите действия приложения после завершения задачи:

   - **Добавлять разрешающие правила в список правил контроля устройств**. Список правил контроля устройств доступен в параметрах компонента Контроль устройств.

     Если флажок установлен, приложение добавляет правила, сформированные в ходе выполнения задачи, в список правил контроля устройств согласно выбранному принципу добавления правил.

Если флажок снят, не добавляет новые сформированные разрешающие правила в список правил контроля устройств. Приложение только экспортирует правила в файл.

- **Принцип добавления**. Способ добавления сформированных разрешающих правил в список правил контроля устройств:
  - **Добавить к существующим правилам**. Приложение добавляет правило в список существующих правил. При этом приложение дублирует одинаковые правила.
  - **Заменить существующие правила**. Приложение добавляет новые правила вместо существующих правил.
  - **Объединить правила с существующими**. Приложение добавляет правило в список существующих правил. При приложение объединяет одинаковые правила.
- **Экспортировать разрешающие правила в файл**. Приложение экспортирует разрешающие правила в файл, указанный в поле ниже. Далее вы можете импортировать файл в параметрах приложения на других компьютерах для распространения разрешающих правил. Также файл можно использовать для резервного копирования разрешающих правил.
- **Добавлять информацию о защищаемом устройстве в имя файла**. Приложение кроме даты и времени добавляет к имени экспортируемого файла имя компьютера. Это удобно, если вы собираете разрешающие правила с нескольких компьютеров.

5. Сохраните внесенные изменения.

В результате Kaspersky Industrial CyberSecurity for Nodes выполнит аудит внешних устройств и сохранит данные в реестре Kaspersky Security Center. Список внешних устройств доступен при добавлении доверенных устройств.

> Задача *Формирование правил контроля устройств* не собирает данные о подключенных к устройствам сетевых принтерах и сетях Wi-Fi. Для данных типов устройств вам необходимо сформировать правила вручную.

- На основе отчета о событиях компонента Контроль устройств, работающего в режиме **Информировать**, сформированного в Kaspersky Security Center.

  В рамках этого сценария Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к устройствам. Когда компонент Контроль устройств работает в режиме **Информировать**, приложение разрешает использование всех устройств и регистрирует события подключения и отключения внешних устройств в журнале.

  Как включить Контроль устройств в режиме Информировать в Консоли администрирования Kaspersky Security Center

  1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
  2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
  3. В окне свойств политики выберите **Контроль активности на компьютерах**.
  4. В разделе **Контроль устройств** нажмите **Настройка**.
  5. Установите флажок **Контроль устройств**.

6. В блоке **Режим работы для блокирующих правил** выберите **Информировать**.
7. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как включить Контроль устройств в режиме Информировать в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.
5. Установите флажок **Включить контроль устройств**.
6. В блоке **Режим работы для блокирующих правил** выберите **Информировать**.
7. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как включить Контроль устройств в режиме Информировать в Консоли приложения

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.
2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.
3. Установите флажок **Контроль устройств**.
4. В блоке **Режим работы для блокирующих правил** выберите **Информировать**.
5. Сохраните внесенные изменения.

Вам нужно, чтобы за время работы компонента выполнились все возможные сценарии работы защищаемых устройств и групп защищаемых устройств. Далее вы можете импортировать данные отчета о событиях Kaspersky Security Center в файл формата TXT и, проанализировав данные отчета, добавить доверенные устройства.

Рекомендуем использовать этот сценарий, если в сети организации имеется большое количество защищаемых устройств разных типов с различным набором внешних устройств.

Добавление доверенных устройств

Доверенные устройства – это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Для работы с доверенными устройствами вы можете предоставить доступ отдельному пользователю, группе пользователей или всем пользователям организации.

Например, если в вашей организации запрещено использование съемных дисков, но администраторы используют съемные диски в своей работе, вы можете разрешить использование съемных дисков только для группы администраторов. Для этого необходимо добавить съемные диски в список доверенных и настроить права доступа пользователей.

Не рекомендуется добавлять более 1000 доверенных устройств, поскольку это может привести к нестабильности системы.

Как добавить доверенное устройство в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Контроль активности на компьютерах**.
4. В разделе **Контроль устройств** нажмите **Настройка**.
5. В блоке **Настройки контроля устройств** выберите закладку **Доверенные устройства**.

   Откроется список доверенных устройств.
6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных устройств для всех компьютеров организации.

   Списки доверенных устройств родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные устройства родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных устройств родительской политики невозможно.
7. Нажмите на кнопку **Добавить** и выберите способ добавления устройства в список доверенных:

   - **Сформировать правила для устройств, подключенных в текущий момент**.
   - **Сформировать правила на основе данных системы**.
   - **Сформировать правила на основе реестра Kaspersky Security Center**.

   Если список устройств пуст, вам нужно выполнить аудит внешних устройств. Для этого запустите задачу *Формирование правил контроля устройств*.

   Kaspersky Industrial CyberSecurity for Nodes не поддерживает добавление устройств типа **Дискеты** в список доверенных.
8. Нажмите кнопку **Добавить правила для выбранных устройств**.
9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как добавить доверенное устройство в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

   Откроется окно **Контроль устройств**.

5. В блоке **Настройки Контроля устройств** нажмите **Доверенные устройства**.

   Откроется список доверенных устройств.

6. Установите флажок **Объединять значения при наследовании**, если вы хотите создать общий список доверенных устройств для всех компьютеров организации.

   Списки доверенных устройств родительских и дочерних политик будут объединены. Для объединения списков должно быть включено наследование параметров родительской политики. Доверенные устройства родительской политики отображаются в дочерних политиках и доступны только для просмотра. Изменение или удаление доверенных устройств родительской политики невозможно.

7. Нажмите на кнопку **Из реестра KSC**.

   Если список устройств пуст, вам нужно выполнить аудит внешних устройств. Для этого запустите задачу *Формирование правил контроля устройств*.

   > Kaspersky Industrial CyberSecurity for Nodes не поддерживает добавление устройств типа **Дискеты** в список доверенных.

8. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как добавить доверенное устройство в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. В блоке **Настройки Контроля устройств** выберите закладку **Доверенные устройства**.

   Откроется список доверенных устройств.

4. Нажмите на кнопку **Добавить** и выберите способ добавления устройства в список доверенных:

   - **Сформировать правила для устройств, подключенных в текущий момент**.
   - **Сформировать правила на основе данных системы**.
   - **Сформировать правила на основе реестра Kaspersky Security Center**.

   Если список устройств пуст, вам нужно выполнить аудит внешних устройств. Для этого запустите задачу *Формирование правил контроля устройств*.

   > Kaspersky Industrial CyberSecurity for Nodes не поддерживает добавление устройств типа **Дискеты** в список доверенных.

5. Нажмите кнопку **Добавить правила для выбранных устройств**.

6. Сохраните внесенные изменения.

Экспорт и импорт списка доверенных устройств

Для распространения списка доверенных устройств на компьютеры организации вы можете использовать процедуру экспорта/импорта. Вы можете экспортировать список доверенных устройств в файл формата XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных устройств. Вы можете использовать функцию экспорта/импорта для резервного копирования списка доверенных устройств или для миграции списка на другой сервер.

Kaspersky Industrial CyberSecurity for Nodes позволяет импортировать список доверенных устройств из приложения Kaspersky Endpoint Security для Windows. Формат файлов XML для этих приложений совпадает.

Как экспортировать/импортировать список доверенных устройств в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне свойств политики выберите **Контроль активности на компьютерах**.

4. В разделе **Контроль устройств** нажмите **Настройка**.

5. В блоке **Настройки Контроля устройств** выберите вкладку **Доверенные устройства**.

   Откроется список доверенных устройств.

6. Для экспорта списка доверенных устройств выполните следующие действия:

   a. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

   b. Если вы хотите экспортировать только часть списка, выполните следующие действия:

      1. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A.**

      2. Нажмите на кнопку и выберите **Экспортировать выбранное**.

   c. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список доверенных устройств в XML-файл.

7. Для импорта списка доверенных устройств выполните следующие действия:

   a. Нажмите на кнопку **Добавить** → **Импортировать правила из файла формата XML** и выберите режим импорта: объединить, добавить или заменить правила.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список доверенных устройств.

В режиме объединения списков доверенных устройств приложение проверяет списки и удаляет повторяющиеся записи. В режиме добавления списка доверенных устройств приложение добавляет записи без проверки на наличие повторяющихся записей.

b. Откройте файл.

Kaspersky Industrial CyberSecurity for Nodes импортирует доверенные устройства в соответствии с выбранным режимом.

8. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как экспортировать/импортировать список доверенных устройств в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль активности на компьютерах** → **Контроль устройств** и нажмите на кнопку **Настроить**.

Откроется окно **Контроль устройств**.

5. В блоке **Настройки Контроля устройств** нажмите **Доверенные устройства**.

Откроется список доверенных устройств.

6. Для экспорта списка доверенных устройств выполните следующие действия:

a. Если требуется, выберите доверенные устройства, которые вы хотите экспортировать.

b. Нажмите на кнопку **Экспорт** и выберите режим экспорта: экспортировать весь список доверенных устройств или только выбранные доверенные устройства.

c. Сохраните файл.

Kaspersky Industrial CyberSecurity for Nodes экспортирует список адресов веб-ресурсов в XML-файл.

7. Для импорта списка доверенных устройств выполните следующие действия:

a. Нажмите на кнопку **Импорт** и выберите режим импорта: добавить или заменить правила.

b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список веб-ресурсов.

c. Откройте файл.

Kaspersky Industrial CyberSecurity for Nodes импортирует доверенные устройства в соответствии с выбранным режимом.

8. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как экспортировать/импортировать список доверенных устройств в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Контроль устройств**.

2. В панели результатов узла **Контроль устройств** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль устройств**.

3. В блоке **Настройки Контроля устройств** выберите закладку **Доверенные устройства**.

   Откроется список доверенных устройств.

4. Для экспорта списка доверенных устройств выполните следующие действия:

   a. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

   b. Если вы хотите экспортировать только часть списка, выполните следующие действия:

      1. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A.**

      2. Нажмите на кнопку и выберите **Экспортировать выбранное**.

   c. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список доверенных устройств в XML-файл.

5. Для импорта списка доверенных устройств выполните следующие действия:

   a. Нажмите на кнопку **Добавить** → **Импортировать правила из файла формата XML** и выберите режим импорта: объединить, добавить или заменить правила.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список веб-ресурсов.

      В режиме объединения списков доверенных устройств приложение проверяет списки и удаляет повторяющиеся записи. В режиме добавления списка доверенных устройств приложение добавляет записи без проверки на наличие повторяющихся записей.

   b. Откройте файл.

      Kaspersky Industrial CyberSecurity for Nodes импортирует доверенные устройства в соответствии с выбранным режимом.

6. Сохраните внесенные изменения.

Сетевой экран

Компонент Сетевой экран работает в следующих режимах:

- **Отслеживать статус работы брандмауэра Windows**. Режим предназначен для плавного перехода от логики работы задачи Управление сетевым экраном в приложении версии 4.0 и ниже к полноценному Сетевому экрану приложения версии 4.5 и выше. После обновления приложения версии 4.0 и ниже правила задачи Управление сетевым экраном, интегрированные в брандмауэр Windows, сохраняются. Однако компонент Сетевой экран уже не взаимодействует с брандмауэром Windows, а только отслеживает фильтрацию трафика брандмауэром Windows и записывает соответствующие события в журнал работы компонента. Далее вы можете создать правила Сетевого экрана и/или импортировать правила брандмауэра Windows и изменить режим работы Сетевого экрана на **Информировать**.

- **Информировать**. Приложение только отслеживает работу правил Сетевого экрана и фиксирует соответствующие события в журнал работы компонента. Режим предназначен для тестирования правил Сетевого экрана. С помощью журнала работы Сетевого экрана вы можете оценить их применимость. Далее, при необходимости, вы можете скорректировать правила Сетевого экрана и изменить режим работы Сетевого экрана на **Блокировать**.

- **Блокировать**. Приложение фильтрует сетевой трафик в соответствии с настройками компонента и фиксирует соответствующие события в журнал работы компонента.

О правилах сетевого экрана

Компонент Сетевой экран фильтрует сетевой трафик с помощью правил сетевого экрана, если установлен режим **Блокировать**.

Правила сетевого экрана для приложений контролируют сетевые соединения для указанных приложений. Критерием срабатывания таких правил является путь к исполняемому файлу приложения.

Правила сетевого экрана для портов контролируют сетевые соединения для указанных портов и протоколов (TCP/UDP). Критериями срабатывания таких правил являются тип протокола и порт или диапазон портов.

Правила для портов предполагают более широкую область действия, чем правила для приложений. Разрешая сетевые соединения с помощью правил для портов, вы снижаете уровень безопасности защищаемого компьютера.

Настройка Сетевого экрана

В этом разделе приведены инструкции по настройке общих параметров компонента Сетевой экран и созданию и настройке правил сетевого экрана.

Настройка общих параметров Сетевого экрана

Настройка общих параметров компонента Сетевой экран в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В разделе **Контроль активности в сети** в блоке **Сетевой экран** нажмите на кнопку **Настройка**.

   Откроется окно **Сетевой экран**.
4. На вкладке **Общие** в блоке **Режим работы для блокирующих правил** выберите режим работы компонента Сетевой экран:

   - **Отслеживать статус работы брандмауэра Windows**. Режим предназначен для плавного перехода от логики работы задачи Управление сетевым экраном в приложении версии 4.0 и ниже к полноценному Сетевому экрану приложения версии 4.5 и выше. После обновления приложения версии 4.0 и ниже правила задачи Управление сетевым экраном, интегрированные в брандмауэр Windows, сохраняются. Однако компонент Сетевой экран уже не взаимодействует с брандмауэром Windows, а только отслеживает фильтрацию трафика брандмауэром Windows и записывает соответствующие события в журнал работы компонента. Далее вы можете создать правила Сетевого экрана и/или импортировать правила брандмауэра Windows и изменить режим работы Сетевого экрана на **Информировать**.

   - **Информировать**. Приложение только отслеживает работу правил Сетевого экрана и фиксирует соответствующие события в журнал работы компонента. Режим предназначен для тестирования правил Сетевого экрана. С помощью журнала работы Сетевого экрана вы можете оценить их применимость. Далее, при необходимости, вы можете скорректировать правила Сетевого экрана и изменить режим работы Сетевого экрана на **Блокировать**.

   - **Блокировать**. Приложение фильтрует сетевой трафик в соответствии с настройками компонента и фиксирует соответствующие события в журнал работы компонента.
5. В блоке **Входящие соединения** настройте параметры для входящих сетевых соединений:

   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет приложение для всех входящих сетевых соединений, если иное не определено в правилах Сетевого экрана для входящих соединений.

   - При необходимости добавьте правила Сетевого экрана для входящих соединений.

     Правила Сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то приложение разрешает входящие сетевые соединения, подпадающие под критерии правила.

6. В блоке **Исходящие соединения** настройте параметры для исходящих сетевых соединений:

   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет приложение для всех исходящих сетевых соединений, если иное не определено в правилах Сетевого экрана для исходящих соединений.

   - При необходимости добавьте правила Сетевого экрана для исходящих соединений.

     Правила Сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешать**, то приложение блокирует исходящие сетевые соединения, подпадающие под критерии правила.

7. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Настройка общих параметров компонента Сетевой экран в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. В разделе **Контроль активности в сети** в блоке **Сетевой экран** нажмите на кнопку **Настроить**.

   Откроется окно **Сетевой экран**.

5. Установите переключатель в положение **Сетевой экран ВКЛЮЧЕН**.

6. В блоке **Режим работы для блокирующих правил** выберите режим работы компонента Сетевой экран:

   - **Отслеживать статус работы брандмауэра Windows**. Режим предназначен для плавного перехода от логики работы задачи Управление сетевым экраном в приложении версии 4.0 и ниже к полноценному Сетевому экрану приложения версии 4.5 и выше. После обновления приложения версии 4.0 и ниже правила задачи Управление сетевым экраном, интегрированные в брандмауэр Windows, сохраняются. Однако компонент Сетевой экран уже не взаимодействует с брандмауэром Windows, а только отслеживает фильтрацию трафика брандмауэром Windows и записывает соответствующие события в журнал работы компонента. Далее вы можете создать правила Сетевого экрана и/или импортировать правила брандмауэра Windows и изменить режим работы Сетевого экрана на **Информировать**.

   - **Информировать**. Приложение только отслеживает работу правил Сетевого экрана и фиксирует соответствующие события в журнал работы компонента. Режим предназначен для тестирования правил Сетевого экрана. С помощью журнала работы Сетевого экрана вы можете оценить их применимость. Далее, при необходимости, вы можете скорректировать правила Сетевого экрана и изменить режим работы Сетевого экрана на **Блокировать**.

   - **Блокировать**. Приложение фильтрует сетевой трафик в соответствии с настройками компонента и фиксирует соответствующие события в журнал работы компонента.

7. В блоке **Входящие соединения** настройте параметры для входящих сетевых соединений:

   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет приложение для всех входящих сетевых соединений, если иное не определено в правилах Сетевого экрана для входящих соединений.

   - При необходимости добавьте правила Сетевого экрана для входящих соединений.

     Правила Сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то приложение разрешает входящие сетевые соединения, подпадающие под критерии правила.

8. В блоке **Исходящее соединение** настройте параметры для исходящих сетевых соединений:

   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет приложение для всех исходящих сетевых соединений, если иное не определено в правилах Сетевого экрана для исходящих соединений.

   - При необходимости добавьте правила Сетевого экрана для исходящих соединений.

     Правила Сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешить**, то приложение блокирует исходящие сетевые соединения, подпадающие под критерии правила.

9. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Настройка общих параметров компонента Сетевой экран в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Сетевой экран**.

2. В панели результатов узла **Сетевой экран** нажмите **Свойства**.

   Откроется окно **Свойства: Сетевой экран**.

3. Установите флажок **Сетевой экран**.

4. В блоке **Режим работы для блокирующих правил** выберите режим работы компонента Сетевой экран:

   - **Отслеживать статус работы брандмауэра Windows**. Режим предназначен для плавного перехода от логики работы задачи Управление сетевым экраном в приложении версии 4.0 и ниже к полноценному Сетевому экрану приложения версии 4.5 и выше. После обновления приложения версии 4.0 и ниже правила задачи Управление сетевым экраном, интегрированные в брандмауэр Windows, сохраняются. Однако компонент Сетевой экран уже не взаимодействует с брандмауэром Windows, а только отслеживает фильтрацию трафика брандмауэром Windows и записывает соответствующие события в журнал работы компонента. Далее вы можете создать правила Сетевого экрана и/или импортировать правила брандмауэра Windows и изменить режим работы Сетевого экрана на **Информировать**.

   - **Информировать**. Приложение только отслеживает работу правил Сетевого экрана и фиксирует соответствующие события в журнал работы компонента. Режим предназначен для тестирования правил Сетевого экрана. С помощью журнала работы Сетевого экрана вы можете оценить их применимость. Далее, при необходимости, вы можете скорректировать правила Сетевого экрана и изменить режим работы Сетевого экрана на **Блокировать**.

   - **Блокировать**. Приложение фильтрует сетевой трафик в соответствии с настройками компонента и фиксирует соответствующие события в журнал работы компонента.

5. В блоке **Входящие соединения** настройте параметры для входящих сетевых соединений:

   - С помощью раскрывающегося списка **Действие для входящих соединений** определите действие, которое выполняет приложение для всех входящих сетевых соединений, если иное не определено в правилах Сетевого экрана для входящих соединений.

   - При необходимости добавьте правила Сетевого экрана для входящих соединений.

     Правила Сетевого экрана для входящих соединений выполняют роль исключений. Например, если вы настроили правило для входящих сетевых соединений как разрешающее, а в раскрывающемся списке **Действие для входящих соединений** выбрали **Блокировать**, то приложение разрешает входящие сетевые соединения, подпадающие под критерии правила.

6. В блоке **Исходящие соединения** настройте параметры для исходящих сетевых соединений:

   - С помощью раскрывающегося списка **Действие для исходящих соединений** определите действие, которое выполняет приложение для всех исходящих сетевых соединений, если иное не определено в правилах Сетевого экрана для исходящих соединений.

   - При необходимости добавьте правила Сетевого экрана для исходящих соединений.

     Правила Сетевого экрана для исходящих соединений выполняют роль исключений. Например, если вы настроили правило для исходящих сетевых соединений как блокирующее, а в раскрывающемся списке **Действие для исходящих соединений** выбрали **Разрешать**, то приложение блокирует исходящие сетевые соединения, подпадающие под критерии правила.

7. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Создание и настройка правил Сетевого экрана

Создание и настройка правил Сетевого экрана в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В разделе **Контроль активности в сети** в блоке **Сетевой экран** нажмите на кнопку **Настройка**.

   Откроется окно **Сетевой экран**.
4. В блоке **Входящие соединения** нажмите на кнопку **Список правил**.

   Откроется окно **Правила для входящих соединений**.
5. **Создайте и настройте правила Сетевого экрана для входящих соединений**.

   1. На вкладке **Приложения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для приложения**.
   2. Настройте параметры правила:

      a. В поле **Имя правила** введите название правила.

      > Название правила, независимо от регистра символов, не должно совпадать с зарезервированными названиями All, ICMPv4 и ICMPv6; должно быть уникальным в списке всех правил для входящих сетевых соединений.

      b. В раскрывающемся списке **Действие** выберите один из вариантов:

      - **Разрешать**. Если выбран этот вариант, приложение разрешает входящие сетевые соединения для приложения.
      - **Блокировать**. Если выбран этот вариант, приложение блокирует входящие сетевые соединения для приложения.

      c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

      d. В блоках **Порты** и **Порты** укажите порт или диапазон портов.

      e. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

      f. В поле **Имя сервиса** при необходимости укажите названия сервиса, для которого должно применяться правило.

g. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

h. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

i. Нажмите на кнопку **OK**, чтобы сохранить правило.

3. На вкладке **Порты** нажмите на кнопку **Добавить**.

   Откроется окно **Правило для портов**.

4. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

   b. В раскрывающемся списке **Действие** выберите один из вариантов:

   - **Разрешать**. Если выбран этот вариант, приложение разрешает входящие сетевые соединения для портов.
   - **Блокировать**. Если выбран этот вариант, приложение блокирует входящие сетевые соединения для портов.

   c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

   d. В блоках **Порты** и **Порты** укажите порт или диапазон портов.

   e. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

   > Для IP-адресов поддерживается только формат IPv4.

   f. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

   g. Нажмите на кнопку **OK**, чтобы сохранить правило.

5. В окне **Правила для входящих соединений** нажмите на кнопку **OK**.

6. В блоке **Исходящие соединения** нажмите на кнопку **Список правил**.

   Откроется окно **Правила для исходящих соединений**.

7. **Создайте и настройте правила Сетевого экрана для исходящих соединений**.

   1. На вкладке **Приложения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для приложения**.

2. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

      Название правила, независимо от регистра символов, не должно совпадать с зарезервированными названиями All, ICMPv4 и ICMPv6; должно быть уникальным в списке всех правил для исходящих сетевых соединений.

   b. В раскрывающемся списке **Действие** выберите один из вариантов:

      - **Разрешать**. Если выбран этот вариант, приложение разрешает исходящие сетевые соединения для приложения.
      - **Блокировать**. Если выбран этот вариант, приложение блокирует исходящие сетевые соединения для приложения.

   c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

   d. В блоках **Порты** и **Порты** укажите порт или диапазон портов.

   e. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

   f. В поле **Имя сервиса** при необходимости укажите названия сервиса, для которого должно применяться правило.

   g. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует исходящие соединения на указанные сетевые адреса в соответствии с параметрами правила.

      Для IP-адресов поддерживается только формат IPv4.

   h. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

   i. Нажмите на кнопку **OK**, чтобы сохранить правило.

3. На вкладке **Порты** нажмите на кнопку **Добавить**.

   Откроется окно **Правило для портов**.

4. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

   b. В раскрывающемся списке **Действие** выберите один из вариантов:

      - **Разрешать**. Если выбран этот вариант, приложение разрешает исходящие сетевые соединения для портов.
      - **Блокировать**. Если выбран этот вариант, приложение блокирует исходящие сетевые соединения для портов.

   c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

d. В блоках **Порты** и **Порты** укажите порт или диапазон портов.

e. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует исходящие соединения на указанные сетевые адреса в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

f. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

g. Нажмите на кнопку **OK**, чтобы сохранить правило.

5. В окне **Правила для исходящих соединений** нажмите на кнопку **OK**.

8. Если вы хотите импортировать или экспортировать пользовательские правила из файла формата XML, используйте кнопки **Импортировать** или **Экспортировать** в блоке **Импорт и экспорт правил**.

9. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Создание и настройка правил Сетевого экрана в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. В разделе **Контроль активности в сети** в блоке **Сетевой экран** нажмите на кнопку **Настроить**.

   Откроется окно **Сетевой экран**.

5. Установите переключатель в положение **Сетевой экран ВКЛЮЧЕН**.

6. В блоке **Входящие соединения** нажмите на кнопку **Настроить**.

   Откроется окно **Правила для входящих соединений**.

7. **Создайте и настройте правила Сетевого экрана для входящих соединений**.

   1. На вкладке **Порты** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для портов**.

2. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

   b. В раскрывающемся списке **Действие** выберите один из вариантов:

      - **Разрешить**. Если выбран этот вариант, приложение разрешает входящие сетевые соединения для портов.
      - **Запретить**. Если выбран этот вариант, приложение блокирует входящие сетевые соединения для портов.

   c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

   d. В блоках **Локальные порты** и **Удаленные порты** укажите порт или диапазон портов.

   e. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует входящие соединения на указанные сетевые адреса в соответствии с параметрами правила.

      Для IP-адресов поддерживается только формат IPv4.

   f. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

   g. Нажмите на кнопку **OK**, чтобы сохранить правило.

3. На вкладке **Приложения** нажмите на кнопку **Добавить**.

   Откроется окно **Правило для приложений**.

4. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

      Название правила, независимо от регистра символов, не должно совпадать с зарезервированными названиями All, ICMPv4 и ICMPv6; должно быть уникальным в списке всех правил для входящих сетевых соединений.

   b. В раскрывающемся списке **Действие** выберите один из вариантов:

      - **Разрешить**. Если выбран этот вариант, приложение разрешает входящие сетевые соединения для приложения.
      - **Запретить**. Если выбран этот вариант, приложение блокирует входящие сетевые соединения для приложения.

   c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

   d. В блоках **Локальные порты** и **Удаленные порты** укажите порт или диапазон портов.

   e. В поле **Путь к приложению** вручную укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

f. В поле **Имя сервиса** при необходимости укажите названия сервиса, для которого должно применяться правило.

g. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

h. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

i. Нажмите на кнопку **OK**, чтобы сохранить правило.

5. В окне **Правила для входящих соединений** нажмите на кнопку **OK**.

8. В блоке **Исходящее соединение** нажмите на кнопку **Настроить**.

   Откроется окно **Правила для исходящих соединений**.

9. **Создайте и настройте правила Сетевого экрана для исходящих соединений**.

   1. На вкладке **Порты** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для портов**.

   2. Настройте параметры правила:

      a. В поле **Имя правила** введите название правила.

      b. В раскрывающемся списке **Действие** выберите один из вариантов:

      - **Разрешить**. Если выбран этот вариант, приложение разрешает исходящие сетевые соединения для портов.
      - **Запретить**. Если выбран этот вариант, приложение блокирует исходящие сетевые соединения для портов.

      c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

      d. В блоках **Локальные порты** и **Удаленные порты** укажите порт или диапазон портов.

      e. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует исходящие соединения на указанные сетевые адреса в соответствии с параметрами правила.

      > Для IP-адресов поддерживается только формат IPv4.

      f. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

      g. Нажмите на кнопку **OK**, чтобы сохранить правило.

   3. На вкладке **Приложения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для приложений**.

4. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

   > Название правила, независимо от регистра символов, не должно совпадать с зарезервированными названиями All, ICMPv4 и ICMPv6; должно быть уникальным в списке всех правил для исходящих сетевых соединений.

   b. В раскрывающемся списке **Действие** выберите один из вариантов:

   - **Разрешить**. Если выбран этот вариант, приложение разрешает исходящие сетевые соединения для приложения.
   - **Запретить**. Если выбран этот вариант, приложение блокирует исходящие сетевые соединения для приложения.

   c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

   d. В блоках **Локальные порты** и **Удаленные порты** укажите порт или диапазон портов.

   e. В поле **Путь к приложению** вручную укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

   f. В поле **Имя сервиса** при необходимости укажите названия сервиса, для которого должно применяться правило.

   g. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует исходящие соединения на указанные сетевые адреса в соответствии с параметрами правила.

   > Для IP-адресов поддерживается только формат IPv4.

   h. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

   i. Нажмите на кнопку **OK**, чтобы сохранить правило.

5. В окне **Правила для исходящих соединений** нажмите на кнопку **OK**.

10. Если вы хотите импортировать или экспортировать пользовательские правила из файла формата XML, используйте кнопки **Импорт правил** или **Экспорт правил** в блоке **Импорт и экспорт правил**.

11. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Создание и настройка правил Сетевого экрана в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Сетевой экран**.

2. В панели результатов узла **Сетевой экран** нажмите **Свойства**.

   Откроется окно **Свойства: Сетевой экран**.

3. В блоке **Входящие соединения** нажмите на кнопку **Список правил**.

   Откроется окно **Правила для входящих соединений**.

4. **Создайте и настройте правила Сетевого экрана для входящих соединений**.

   1. На вкладке **Приложения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для приложения**.

   2. Настройте параметры правила:

      a. В поле **Имя правила** введите название правила.

      > Название правила, независимо от регистра символов, не должно совпадать с зарезервированными названиями All, ICMPv4 и ICMPv6; должно быть уникальным в списке всех правил для входящих сетевых соединений.

      b. В раскрывающемся списке **Действие** выберите один из вариантов:

      - **Разрешать**. Если выбран этот вариант, приложение разрешает входящие сетевые соединения для приложения.
      - **Блокировать**. Если выбран этот вариант, приложение блокирует входящие сетевые соединения для приложения.

      c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

      d. В блоках **Порты** и **Порты** укажите порт или диапазон портов.

      e. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

      f. В поле **Имя сервиса** при необходимости укажите названия сервиса, для которого должно применяться правило.

      g. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

      > Для IP-адресов поддерживается только формат IPv4.

      h. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

      i. Нажмите на кнопку **ОК**, чтобы сохранить правило.

   3. На вкладке **Порты** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для портов**.

4. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

   b. В раскрывающемся списке **Действие** выберите один из вариантов:

   - **Разрешать**. Если выбран этот вариант, приложение разрешает входящие сетевые соединения для портов.
   - **Блокировать**. Если выбран этот вариант, приложение блокирует входящие сетевые соединения для портов.

   c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

   d. В блоках **Порты** и **Порты** укажите порт или диапазон портов.

   e. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует входящие соединения с указанных сетевых адресов в соответствии с параметрами правила.

   > Для IP-адресов поддерживается только формат IPv4.

   f. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

   g. Нажмите на кнопку **OK**, чтобы сохранить правило.

5. В окне **Правила для входящих соединений** нажмите на кнопку **OK**.

5. В блоке **Исходящие соединения** нажмите на кнопку **Список правил**.

   Откроется окно **Правила для исходящих соединений**.

6. **Создайте и настройте правила Сетевого экрана для исходящих соединений**.

   1. На вкладке **Приложения** нажмите на кнопку **Добавить**.

      Откроется окно **Правило для приложения**.

   2. Настройте параметры правила:

      a. В поле **Имя правила** введите название правила.

      > Название правила, независимо от регистра символов, не должно совпадать с зарезервированными названиями All, ICMPv4 и ICMPv6; должно быть уникальным в списке всех правил для исходящих сетевых соединений.

      b. В раскрывающемся списке **Действие** выберите один из вариантов:

      - **Разрешать**. Если выбран этот вариант, приложение разрешает исходящие сетевые соединения для приложения.
      - **Блокировать**. Если выбран этот вариант, приложение блокирует исходящие сетевые соединения для приложения.

c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

d. В блоках **Порты** и **Порты** укажите порт или диапазон портов.

e. В поле **Путь к приложению** вручную или с помощью кнопки **Обзор** укажите путь к исполняемому файлу приложения, для которого вы настраиваете правило.

f. В поле **Имя сервиса** при необходимости укажите названия сервиса, для которого должно применяться правило.

g. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует исходящие соединения на указанные сетевые адреса в соответствии с параметрами правила.

> Для IP-адресов поддерживается только формат IPv4.

h. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

i. Нажмите на кнопку **OK**, чтобы сохранить правило.

3. На вкладке **Порты** нажмите на кнопку **Добавить**.

   Откроется окно **Правило для портов**.

4. Настройте параметры правила:

   a. В поле **Имя правила** введите название правила.

   b. В раскрывающемся списке **Действие** выберите один из вариантов:

   - **Разрешать**. Если выбран этот вариант, приложение разрешает исходящие сетевые соединения для портов.
   - **Блокировать**. Если выбран этот вариант, приложение блокирует исходящие сетевые соединения для портов.

   c. Установите флажок **Протокол**, чтобы выбрать тип протокола, для которого приложение контролирует входящие сетевые соединения.

   d. В блоках **Порты** и **Порты** укажите порт или диапазон портов.

   e. В поле **Область применения правила** укажите сетевые адреса. Приложение контролирует исходящие соединения на указанные сетевые адреса в соответствии с параметрами правила.

   > Для IP-адресов поддерживается только формат IPv4.

   f. В блоке **Сетевые адаптеры** укажите список сетевых адаптеров.

   g. Нажмите на кнопку **OK**, чтобы сохранить правило.

5. В окне **Правила для исходящих соединений** нажмите на кнопку **OK**.

7. Если вы хотите импортировать или экспортировать пользовательские правила из файла формата XML, используйте кнопки **Импортировать** или **Экспортировать** в блоке **Импорт и экспорт правил**.

8. Чтобы импортировать правила брандмауэра Windows, нажмите на кнопку **Импортировать правила брандмауэра Windows**.

   На компьютерах под управлением операционной системы Windows 11 24H2 приложение может пропускать некоторые правила брандмауэра Windows. Из-за особенностей работы этой версии операционной системы Kaspersky Industrial CyberSecurity for Nodes не может распознать параметры некоторых правил для пакетов приложений.

9. Сохраните внесенные изменения.

Kaspersky Industrial CyberSecurity for Nodes применит новые значения параметров. Информация о дате и времени изменения параметров сохранится в журнале системного аудита.

Включение и выключение правил Сетевого экрана

Включение и выключение правил Сетевого экрана в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В разделе **Контроль активности в сети** в блоке **Сетевой экран** нажмите на кнопку **Настройка**.

   Откроется окно **Сетевой экран**.

4. В открывшемся окне нажмите на кнопку **Список правил** в разделе **Входящие соединения** или **Исходящие соединения** в зависимости от типа правила, статус которого вы хотите изменить.

5. В открывшемся окне выберите закладку **Приложения** или **Порты**.

   В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:

   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.

   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.

6. Для удаления правил из списка выберите правила и нажмите на кнопку **Удалить**.

7. Сохраните внесенные изменения.

Включение и выключение правил Сетевого экрана в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. В разделе **Контроль активности в сети** в блоке **Сетевой экран** нажмите на кнопку **Настроить**.

   Откроется окно **Сетевой экран**.

5. В открывшемся окне нажмите на кнопку **Настроить** в разделе **Входящие соединения** или **Исходящее соединение** в зависимости от типа правила, статус которого вы хотите изменить.

6. В открывшемся окне выберите закладку **Порты** или **Приложения**.

   В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:

   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.

   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.

7. Для удаления правил из списка выберите правила и нажмите на кнопку **Удалить**.

8. Сохраните внесенные изменения.

Включение и выключение правил Сетевого экрана в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Контроль компьютера** → **Сетевой экран**.

2. В панели результатов узла **Сетевой экран** нажмите **Свойства**.

   Откроется окно **Свойства: Сетевой экран**.

3. В открывшемся окне нажмите на кнопку **Список правил** в разделе **Входящие соединения** или **Исходящие соединения** в зависимости от типа правила, статус которого вы хотите изменить.

4. В открывшемся окне выберите закладку **Приложения** или **Порты**.

   В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:

   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.

   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.

5. Для удаления правил из списка выберите правила и нажмите на кнопку **Удалить**.

6. Сохраните внесенные изменения.

Защита от атак BadUSB

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Вы можете добавить компонент во время установки приложения или изменить состав компонентов приложения после установки приложения.

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру. В результате вирус может выполнять команды под вашей учетной записью, например, загрузить вредоносное приложение.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, приложение предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный приложением. Эта процедура называется авторизацией клавиатуры.

Если код введен правильно, приложение сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

При подключении авторизованной клавиатуры через другой USB-порт компьютера приложение снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, приложение формирует новый. Вы можете настроить число попыток для ввода цифрового кода. Если цифровой код введен неправильно несколько раз или закрыто окно авторизации клавиатуры, приложение блокирует ввод с этой клавиатуры. По истечении времени блокировки USB-устройства или перезагрузке операционной системы приложение снова предлагает пройти авторизацию клавиатуры.

Приложение разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

USB-устройства, определенные операционной системой как клавиатуры и подключенные к компьютеру до установки компонента Защита от атак BadUSB, считаются авторизованными после его установки.

Как включить и настроить компонент Защита от атак BadUSB в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Контроль активности на компьютерах**.
4. В блоке **Защита от атак BadUSB** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от атак BadUSB**.

5. Используйте флажок **Защита от атак BadUSB**, чтобы включить или выключить компонент.

6. В блоке **Авторизация USB-устройств** настройте параметры:

   - **Максимальное количество попыток авторизации USB-устройства**. Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Industrial CyberSecurity for Nodes покажет время блокировки USB-устройства. По истечении указанного времени, вам будет доступно 5 попыток ввода кода авторизации.

   - **Тайм-аут при достижении максимального количества попыток (минут)**. Время блокировки USB-устройства после достижения заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

7. В блоке **Авторизация USB-устройств при подключении** настройте параметры:

   - **Запретить использование экранной клавиатуры для авторизации USB-устройств**. Если флажок установлен, приложение запрещает использование экранной клавиатуры для авторизации USB-устройств, с которых невозможно ввести код авторизации (например, сканеров штрихкодов).

   - **Запретить использование штрихкода для авторизации USB-устройств**. Если флажок установлен, приложение не отображает штрихкод в уведомлении для авторизации сканеров штрихкодов.

8. Закройте замки для применения политики на компьютерах.

9. Нажмите на кнопку **ОК** для сохранения внесенных изменений.

Как включить и настроить компонент Защита от атак BadUSB в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Контроль активности на компьютерах**.

5. В блоке **Защита от атак BadUSB** нажмите на кнопку **Настроить**.

   Откроется окно **Защита от атак BadUSB**.

6. Используйте переключатель **Защита от атак BadUSB**, чтобы включить или выключить компонент.

7. Используйте переключатель **Запрет на использование экранной клавиатуры для авторизации USB-устройств ВКЛЮЧЕН**, чтобы запретить или разрешить использование экранной клавиатуры для авторизации USB-устройств, с которых невозможно ввести код авторизации (например, сканеров штрихкодов).

8. Используйте переключатель **Запрет на использование штрихкода для авторизации USB-устройств ВКЛЮЧЕН**, чтобы запретить или разрешить отображение штрихкода в уведомлении для авторизации сканеров штрихкодов.

9. В блоке **Авторизация USB-устройств** настройте параметры:

   - **Максимальное количество попыток авторизации USB-устройства (1-10)**. Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Industrial CyberSecurity for Nodes покажет время блокировки USB-устройства. По истечении указанного времени, вам будет доступно 5 попыток ввода кода авторизации.

   - **Тайм-аут при достижении максимального количества попыток в минутах (1-180)**. Время блокировки USB-устройства после достижения заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

10. Закройте замки для применения политики на компьютерах.

11. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как включить и настроить компонент Защита от атак BadUSB в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Контроль компьютера → Защита от атак BadUSB**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Защита от атак BadUSB**.

3. Используйте флажок **Защита от атак BadUSB**, чтобы включить или выключить компонент.

4. В блоке **Авторизация USB-устройств** настройте параметры:

   - **Максимальное количество попыток авторизации USB-устройства**. Автоматическое блокирование USB-устройства, если код авторизации введен неверно заданное количество раз. Доступны значения от 1 до 10. Например, если вы разрешили 5 попыток ввода кода авторизации, после пятой неудачной попытки приложение заблокирует USB-устройство. Kaspersky Industrial CyberSecurity for Nodes покажет время блокировки USB-устройства. По истечении указанного времени, вам будет доступно 5 попыток ввода кода авторизации.

   - **Тайм-аут при достижении максимального количества попыток (минут)**. Время блокировки USB-устройства после достижения заданного количества неудачных попыток ввода кода авторизации. Доступны значения от 1 до 180 (минут).

5. В блоке **Авторизация USB-устройств при подключении** настройте параметры:

   - **Запретить использование экранной клавиатуры для авторизации USB-устройств**. Если флажок установлен, приложение запрещает использование экранной клавиатуры для авторизации USB-устройств, с которых невозможно ввести код авторизации (например, сканеров штрихкодов).

   - **Запретить использование штрихкода для авторизации USB-устройств**. Если флажок установлен, приложение не отображает штрихкод в уведомлении для авторизации сканеров штрихкодов.

6. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Контроль целостности системы

В Kaspersky Industrial CyberSecurity for Nodes 4.5 вместо компонентов Мониторинг файловых операций и Мониторинг доступа к реестру добавлен компонент Контроль целостности системы. Контроль целостности системы включает в себя все функции Мониторинга файловых операций, а также позволяет контролировать изменения в реестре и подключение внешних устройств.

Контроль целостности системы отслеживает изменения в операционной системе, которые могут указывать на нарушения безопасности компьютера. Обнаружив такие изменения, Kaspersky Industrial CyberSecurity for Nodes формирует соответствующие события и предупреждает администратора. Контроль целостности системы может работать в режиме реального времени, а также выполнять проверку целостности системы по запросу.

Контроль целостности системы в режиме реального времени

При работе в режиме реального времени компонент Контроль целостности системы отслеживает изменения в объектах, которые вы включили в область действия компонента (область мониторинга). Также Контроль целостности системы позволяет блокировать несанкционированный доступ к этим объектам в режиме реального времени.

Проверка целостности системы по запросу

Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Для выполнения задачи *Мониторинг целостности системы на основе эталона* требуется настроить область действия компонента (область мониторинга) и создать снимок состояния системы. Снимок состояния системы – зафиксированное состояние объектов системы, с которым приложение сравнивает текущее состояние. Снимок состояния системы создается при первом запуске задачи.

Миграция параметров Мониторинга файловых операций

При обновлении Kaspersky Industrial CyberSecurity for Nodes версии 4.0 и ниже до версии 5.0 миграция параметров Мониторинга файловых операций и Мониторинга доступа к реестру будет выполнена автоматически. Во время миграции приложение переносит правила мониторинга в Контроль целостности системы.

О правилах Контроля целостности системы

Для работы компонента Контроль целостности системы требуется добавить хотя бы одно правило. *Правило Контроля целостности системы* – набор критериев, которые определяют доступ пользователей к файлам или реестру. Компонент Контроль целостности системы обнаруживает изменения в файлах или реестре в заданной *области мониторинга*. Область мониторинга является одним из критериев правила Контроля целостности системы.

Контроль целостности системы позволяет контролировать следующие объекты:

- файлы;
- реестр;
- внешние устройства.

Особенности мониторинга файлов

Контроль целостности системы осуществляет мониторинг изменений в файлах и папках, а также добавление и удаление файлов в области мониторинга. Эти изменения могут указывать на нарушение безопасности компьютера. Рекомендуем добавлять в область мониторинга объекты, изменения в которых происходят редко, или, доступ к которым имеет только администратор. Это позволит уменьшить количество событий Контроля целостности системы.

Kaspersky Industrial CyberSecurity for Nodes отслеживает изменения файлов и папок только на тех дисках, которые подключены в момент начала работы Контроля целостности системы в режиме реального времени. Если диск отключен в момент начала работы Контроля целостности системы в режиме реального времени, приложение не отслеживает изменения файлов и папок на этом диске, даже если эти файлы и папки добавлены в область мониторинга.

Приложение формирует событие Создание объекта в случае, если было зарегистрировано одно из следующих действий: создание файла, увеличения размера файла, перезапись данных в файле, усечение файла. Соответственно, если в процессе работы блокирующих правил Контроля запуска программ для файла было сформировано событие Создание объекта, это может быть следствием как запрета создания файла, так и запрета изменения данного файла, включающего операции увеличения размера, перезаписи данных, усечения.

Особенности мониторинга реестра

Контроль целостности системы осуществляет мониторинг реестра. Эти изменения могут указывать на нарушение безопасности компьютера.

Контроль целостности системы осуществляет мониторинг следующих корневых разделов реестра:

- `HKCR`;
- `HKLM`;
- `HKU`;
- `HKCC`;
- `HKEY_CLASSES_ROOT`;
- `HKEY_LOCAL_MACHINE`;

- HKEY_USERS;
- HKEY_CURRENT_CONFIG.

Контроль целостности системы не поддерживает ключ HKEY_CURRENT_USER. Вы можете указывать путь к ключу в реестре через раздел HKEY_USERS в виде HKEY_USERS\<user profile ID>\<key>.

Особенности мониторинга внешних устройств

Контроль целостности системы осуществляет мониторинг подключения и отключения внешних устройств. Это нужно для защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с этими устройствами. Контроль целостности системы не контролирует доступ к внешним устройствам и не запрещает обмен файлами. Вы можете настроить доступ к устройствам с помощью другого компонента приложения – Контроль устройств.

При выполнении задачи *Мониторинг целостности системы на основе эталона* приложение пропускает переключение внешних устройств, если устройства имеют одинаковую букву диска в операционной системе. Для регистрации переключения внешних устройств необходимо, чтобы эти устройства имели разные буквы диска.

Контроль целостности системы осуществляет мониторинг подключения следующих типов внешних устройств:

- Съемный диск (включая USB-флешки).
- Жесткий диск.
- Внешний сетевой адаптер.
- Привод CD/DVD/Blu-ray.
- Сканер / камера.

Контроль целостности системы в режиме реального времени

Контроль целостности системы позволяет отслеживать изменения в операционной системе в режиме реального времени. Вы можете отслеживать изменения, которые могут указывать на нарушения безопасности на компьютере. Компонент позволяет или блокировать эти изменения, или только регистрировать события об изменениях.

Для работы Контроля целостности системы требуется добавить хотя бы одно правило. Правило Контроля целостности системы – набор критериев, которые определяют доступ пользователей к файлам и реестру. Контроль целостности системы обнаруживает изменения в файлах и реестре в заданной области мониторинга. Область мониторинга является одним из критериев правила Контроля целостности системы.

Как включить и настроить Контроль целостности системы в режиме реального времени в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне свойств политики выберите **Диагностика системы**.

4. В разделе **Контроль целостности системы** нажмите **Настройка**.

5. Установите флажок **Контроль целостности системы**.

6. Настройте мониторинг файловых операций:

   a. Установите флажок **Следить за файлами** на вкладке **Файлы**.

   b. В блоке **Режим работы для блокирующих правил** выберите режим мониторинга файловых операций:

      - **Блокировать**. В этом режиме приложение выполняет действия с файлами в соответствии с правилами мониторинга файловых операций и формирует в журнале работы Контроля целостности системы соответствующие события.

      - **Информировать**. В этом режиме приложение только формирует в журнале работы Контроля целостности системы события о срабатывании правил мониторинга файловых операций.

   c. Добавьте правила мониторинга файловых операций вручную с помощью кнопки **Добавить** или с помощью импорта из XML-файла. Настройки правил мониторинга файловых операций описаны в таблице ниже.

   d. В списке правил мониторинга файловых операций с помощью флажков оставьте включенными нужные правила.

7. Настройте мониторинг доступа к реестру:

   a. Установите флажок **Следить за реестром** на вкладке **Реестр**.

   b. В блоке **Режим работы для блокирующих правил** выберите режим мониторинга доступа к реестру:

      - **Блокировать**. В этом режиме приложение блокирует действия с реестром в соответствии с правилами мониторинга доступа к реестру и формирует в журнале работы Контроля целостности системы соответствующие события.

      - **Информировать**. В этом режиме приложение только формирует в журнале работы Контроля целостности системы события о срабатывании правил мониторинга доступа к реестру.

   c. Добавьте правила мониторинга доступа к реестру вручную с помощью кнопки **Добавить** или с помощью импорта из XML-файла. Настройки правил мониторинга доступа к реестру описаны в таблице ниже.

   d. В списке правил мониторинга доступа к реестру с помощью флажков оставьте включенными нужные правила.

8. Настройте мониторинг внешних устройств:

    a. Установите флажок **Следить за устройствами** на вкладке **Устройства**.

    b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

    После применения настроек мониторинга внешних устройств приложение фиксирует текущие подключения внешних устройств. Далее при подключении или отключении внешних устройств приложение формирует соответствующие события в журнале работы Контроля целостности системы.

9. Сохраните внесенные изменения.

Как включить и настроить Контроль целостности системы в режиме реального времени в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

    Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Диагностика системы** → **Контроль целостности системы** и нажмите на кнопку **Настроить**.

5. Установите флажок **Контроль целостности системы**.

6. Настройте мониторинг файловых операций:

    a. Установите флажок **Следить за файлами** на вкладке **Файлы**.

    b. В блоке **Режим работы для блокирующих правил** выберите режим мониторинга файловых операций:

    - **Блокировать**. В этом режиме приложение выполняет действия с файлами в соответствии с правилами мониторинга файловых операций и формирует в журнале работы Контроля целостности системы соответствующие события.

    - **Информировать**. В этом режиме приложение только формирует в журнале работы Контроля целостности системы события о срабатывании правил мониторинга файловых операций.

    c. Добавьте правила мониторинга файловых операций вручную с помощью кнопки **Добавить** или с помощью импорта из XML-файла. Настройки правил мониторинга файловых операций описаны в таблице ниже.

    d. В списке правил мониторинга файловых операций с помощью переключателя в графе **Статус** оставьте включенными нужные правила.

7. Настройте мониторинг доступа к реестру:

   a. Установите флажок **Следить за реестром** на вкладке **Реестр**.

   b. В блоке **Режим работы для блокирующих правил** выберите режим мониторинга доступа к реестру:

      - **Блокировать**. В этом режиме приложение блокирует действия с реестром в соответствии с правилами мониторинга доступа к реестру и формирует в журнале работы Контроля целостности системы соответствующие события.

      - **Информировать**. В этом режиме приложение только формирует в журнале работы Контроля целостности системы события о срабатывании правил мониторинга доступа к реестру.

   c. Добавьте правила мониторинга доступа к реестру вручную с помощью кнопки **Добавить** или с помощью импорта из XML-файла. Настройки правил мониторинга доступа к реестру описаны в таблице ниже.

   d. В списке правил мониторинга доступа к реестру с помощью переключателя в графе **Статус** оставьте включенными нужные правила.

8. Настройте мониторинг внешних устройств:

   a. Установите флажок **Следить за устройствами** на закладке **Устройства**.

   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

      Контроль целостности системы фиксирует текущее подключение внешних устройств. Приложение начинает контролировать подключение и отключение внешних устройств после включения компонента в параметрах приложения. Далее при подключении или отключении внешних устройств приложение формирует соответствующее событие.

9. Сохраните внесенные изменения.

Как включить и настроить Контроль целостности системы в режиме реального времени в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Мониторинг целостности системы → Контроль целостности системы**.

2. В панели результатов узла **Контроль целостности системы** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль целостности системы**.

3. Установите флажок **Контроль целостности системы**.

4. Настройте мониторинг файловых операций:

   a. Установите флажок **Следить за файлами** на вкладке **Файлы**.

   b. В блоке **Режим работы для блокирующих правил** выберите режим мониторинга файловых операций:

      - **Блокировать**. В этом режиме приложение выполняет действия с файлами в соответствии с правилами мониторинга файловых операций и формирует в журнале работы Контроля целостности системы соответствующие события.

      - **Информировать**. В этом режиме приложение только формирует в журнале работы Контроля целостности системы события о срабатывании правил мониторинга файловых операций.

c. Добавьте правила мониторинга файловых операций вручную с помощью кнопки **Добавить** или с помощью импорта из XML-файла. Настройки правил мониторинга файловых операций описаны в таблице ниже.

d. В списке правил мониторинга файловых операций с помощью флажков оставьте включенными нужные правила.

5. Настройте мониторинг доступа к реестру:

a. Установите флажок **Следить за реестром** на вкладке **Реестр**.

b. В блоке **Режим работы для блокирующих правил** выберите режим мониторинга доступа к реестру:

- **Блокировать**. В этом режиме приложение блокирует действия с реестром в соответствии с правилами мониторинга доступа к реестру и формирует в журнале работы Контроля целостности системы соответствующие события.
- **Информировать**. В этом режиме приложение только формирует в журнале работы Контроля целостности системы события о срабатывании правил мониторинга доступа к реестру.

c. Добавьте правила мониторинга доступа к реестру вручную с помощью кнопки **Добавить** или с помощью импорта из XML-файла. Настройки правил мониторинга доступа к реестру описаны в таблице ниже.

d. В списке правил мониторинга доступа к реестру с помощью флажков оставьте включенными нужные правила.

6. Настройте мониторинг внешних устройств:

a. Установите флажок **Следить за устройствами** на вкладке **Устройства**.

b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

После применения настроек мониторинга внешних устройств приложение фиксирует текущие подключения внешних устройств. Далее при подключении или отключении внешних устройств приложение формирует соответствующие события в журнале работы Контроля целостности системы.

7. Сохраните внесенные изменения.

Параметры правил Контроля целостности системы

Параметр	Описание
Выполнять мониторинг файловых операций для области	Область, для которой будет производиться мониторинг файловых операций. Данное поле является обязательным. Используйте маски: Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. Символ `?`, который заменяет любой один символ, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Параметр	Описание
Объекты мониторинга	Здесь вы можете указать имя или значение ключа реестра. Используйте маски: Kaspersky Industrial CyberSecurity for Nodes поддерживает символы `*` и `?` для ввода маски.
Действия с файлами	• **Обнаруживать**. Приложение разрешает действия с файлами в области мониторинга. • **Обнаруживать и блокировать**. Действие приложения зависит от выбранного режима работы мониторинга файловых операций. Если вы выбрали режим *Блокировать*, Контроль целостности системы блокирует действия с файлами из области мониторинга. Если вы выбрали *Информировать*, Контроль целостности системы разрешает действия с файлами в области мониторинга.
Доверенные пользователи и / или группы пользователей	Доверенный пользователь – пользователь, которому разрешено выполнение действий с файлами и реестром в области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes обнаруживает действие, выполненное доверенным пользователем, Контроль целостности системы формирует событие с уровнем важности Информационные. Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную.
Маркеры файловых операций / **Действия**	Маркеры, характеризующие действие над файлами или реестром, которые будет контролировать приложение.
Обнаруживать файловые операции по всем распознаваемым маркерам / **Обнаруживать операции с реестром по всем распознаваемым маркерам**	По умолчанию Kaspersky Industrial CyberSecurity for Nodes обнаруживает все маркеры файловых операций / операций с реестром.
Обнаруживать файловые операции по следующим маркерам / **Обнаруживать операции с реестром по следующим маркерам**	В списке доступных файловых операций / операций с реестром установите флажки напротив тех операций, которые вы хотите контролировать.
Рассчитывать контрольную сумму файла после файловой операции, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции. Если файловая операция обнаружена сразу по нескольким маркерам, рассчитывается только окончательная контрольная сумма файла после всех изменений. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не рассчитывает контрольную сумму измененных файлов. Расчет контрольной суммы не выполняется в следующих случаях: • если файл стал недоступен (например, в результате изменения прав доступа к файлу); • если файловая операция обнаружена в файле, который впоследствии был удален. По умолчанию флажок снят.
Алгоритм вычисления контрольной суммы	В раскрывающемся списке выберите один из алгоритмов вычисления контрольной суммы: • Хеш MD5; • Хеш SHA256.

Параметр	Описание
Исключения	На закладке **Исключения** вы можете добавить объекты, которые вы хотите исключить из области мониторинга: • для правила мониторинга файловых операций вы можете указать список папок; • для правила мониторинга доступа к реестру, вы можете указать ключи реестра или значения ключей реестра. Используйте маски: **Файлы** Список файлов и папок, которые контролирует компонент. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов. **Реестр** Kaspersky Industrial CyberSecurity for Nodes поддерживает символы `*` и `?` для ввода маски. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга.
Уровень важности событий	Kaspersky Industrial CyberSecurity for Nodes регистрирует события изменения файлов и реестра в области мониторинга. Доступны следующие уровни важности событий: **Информационные**, **Предупреждение**, **Критические**.

Проверка целостности системы по запросу

Проверка целостности системы по запросу представляет собой задачу, которую вы можете запускать вручную или по расписанию. Во время выполнения задачи *Мониторинг целостности системы на основе эталона* приложение сравнивает текущее состояние объектов, включенных в область мониторинга, с состоянием этих объектов, зафиксированных в *снимке состояния системы*. Снимок состояния системы создается при первом запуске задачи.

Для работы Контроля целостности системы требуется добавить хотя бы одно правило. Правило Контроля целостности системы – набор критериев, которые определяют доступ пользователей к файлам и реестру. Контроль целостности системы обнаруживает изменения в файлах и реестре в заданной области мониторинга. Область мониторинга является одним из критериев правила Контроля целостности системы.

Настройка области мониторинга для задачи Мониторинг целостности системы на основе эталона

По умолчанию область мониторинга для задачи *Мониторинг целостности системы на основе эталона* совпадает с областью мониторинга Контроля целостности системы. Вы можете задать отдельную область мониторинга для задачи.

Контроль целостности системы не поддерживает импорт ключей `HKEY_CURRENT_USER` и `HKEY_CURRENT_CONFIG` для задачи *Проверка целостности системы*. Если область мониторинга задачи содержит эти ключи, приложение формирует событие *Область мониторинга содержит некорректные объекты*.

Как задать отдельную область мониторинга для задачи Мониторинг целостности системы на основе эталона в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.
2. Выберите нужную задачу *Мониторинг целостности системы на основе эталона* и откройте свойства задачи двойным щелчком мыши.
3. В открывшемся окне выберите **Настройки**.
4. Настройте мониторинг файлов:
   a. Установите флажок **Следить за файлами** на закладке **Файлы**.
   b. Установите флажки напротив нужных правил из списка.
   c. Если нужно, добавьте новое правило нажав на кнопку **Добавить**. Настройки правил Мониторинга целостности системы на основе эталона описаны в таблице ниже.
   d. Вы также можете импортировать правила из другого источника.
5. Настройте мониторинг реестра:
   a. Установите флажок **Следить за реестром** на закладке **Реестр**.
   b. Установите флажки напротив нужных правил из списка.
   c. Если нужно, добавьте новое правило нажав на кнопку **Добавить**. Настройки правил Мониторинга целостности системы на основе эталона описаны в таблице ниже.
   d. Вы также можете импортировать правила из другого источника.
6. Настройте мониторинг внешних устройств:
   a. Установите флажок **Следить за устройствами** на закладке **Устройства**.
   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

      Задача Мониторинга целостности системы на основе эталона фиксирует подключенные внешние устройства на момент создания снимка состояния системы. Далее при подключении внешних устройств приложение формирует соответствующее событие. При выполнении задачи приложение не отслеживает отключение внешних устройств.
7. Сохраните внесенные изменения.

Как задать отдельную область мониторинга для задачи Мониторинг целостности системы на основе эталона в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.
2. Выберите нужную задачу *Мониторинг целостности системы на основе эталона* и откройте свойства задачи двойным щелчком мыши.
3. В открывшемся окне выберите **Параметры приложения**.

4. Настройте мониторинг файлов:

   a. Установите флажок **Следить за файлами**.

   b. Установите флажки напротив нужных правил из списка.

   c. Если нужно, добавьте новое правило нажав на кнопку **Добавить**. Настройки правил мониторинга целостности системы на основе эталона описаны в таблице ниже.

   d. Вы также можете импортировать правила из другого источника.

5. Настройте мониторинг реестра:

   a. Установите флажок **Следить за реестром**.

   b. Установите флажки напротив нужных правил из списка.

   c. Если нужно, добавьте новое правило нажав на кнопку **Добавить**. Настройки правил мониторинга целостности системы на основе эталона описаны в таблице ниже.

   d. Вы также можете импортировать правила из другого источника.

6. Настройте мониторинг внешних устройств:

   a. Установите флажок **Следить за устройствами**.

   b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационные*, *Предупреждение*, *Критические*.

   Задача *Мониторинг целостности системы на основе эталона* фиксирует подключенные внешние устройства на момент создания снимка состояния системы. Далее при подключении внешних устройств приложение формирует соответствующее событие. При выполнении задачи приложение не отслеживает отключение внешних устройств.

7. Сохраните внесенные изменения.

Как задать отдельную область мониторинга для задачи Мониторинг целостности системы на основе эталона в Консоли приложения

Свойства задачи **Мониторинг целостности системы на основе эталона** будут доступны для редактирования в Консоли Kaspersky Industrial CyberSecurity for Nodes, если задача создана локально, либо если в свойствах политики будет установлен флажок **Разрешить использование локальных задач** в разделе **Настройки приложения → Запуск локальных системных задач.**

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Мониторинг целостности системы → Мониторинг целостности системы на основе эталона**.

2. В панели результатов узла **Мониторинг целостности системы на основе эталона** нажмите **Свойства**.

   Откроется окно **Свойства: Мониторинг целостности системы на основе эталона**.

3. Настройте мониторинг файлов:

   a. Установите флажок **Следить за файлами** на закладке **Файлы**.

   b. Установите флажки напротив нужных правил из списка.

c. Если нужно, добавьте новое правило нажав на кнопку **Добавить**. Настройки правил Мониторинга целостности системы на основе эталона описаны в таблице ниже.

d. Вы также можете импортировать правила из другого источника.

4. Настройте мониторинг реестра:

a. Установите флажок **Следить за реестром** на закладке **Реестр**.

b. Установите флажки напротив нужных правил из списка.

c. Если нужно, добавьте новое правило нажав на кнопку **Добавить**. Настройки правил Мониторинга целостности системы на основе эталона описаны в таблице ниже.

d. Вы также можете импортировать правила из другого источника.

5. Настройте мониторинг внешних устройств:

a. Установите флажок **Следить за устройствами** на закладке **Устройства**.

b. В раскрывающемся списке **Уровень важности событий** выберите уровень важности событий мониторинга внешних устройств: *Информационное*, *Предупреждение*, *Критическое*.

Задача Мониторинга целостности системы на основе эталона фиксирует подключенные внешние устройства на момент создания снимка состояния системы. Далее при подключении внешних устройств приложение формирует соответствующее событие. При выполнении задачи приложение не отслеживает отключение внешних устройств.

6. Сохраните внесенные изменения.

Параметры правила задачи Мониторинг целостности системы на основе эталона

Параметр	Описание
Выполнять мониторинг файловых операций для области	Область, для которой будет выполняться мониторинг файловых операций. Данное поле является обязательным. Используйте маски: Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. Символ `?`, который заменяет любой один символ, кроме символов \ и / (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.
Объекты мониторинга	Здесь вы можете указать имя или значение ключа реестра. Используйте маски: Kaspersky Industrial CyberSecurity for Nodes поддерживает символы `*` и `?` для ввода маски.

Параметр	Описание
Исключения	На закладке **Исключения** вы можете добавить объекты, которые вы хотите исключить из области мониторинга: • для правила мониторинга файловых операций вы можете указать список папок; • для правила мониторинга доступа к реестру, вы можете указать ключи реестра или значения ключей реестра. Используйте маски: **Файлы** Список файлов и папок, которые контролирует компонент. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках. Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папках, вложенных в папку `Folder`, кроме самой папки `Folder`. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает. Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов. **Реестр** Kaspersky Industrial CyberSecurity for Nodes поддерживает символы `*` и `?` для ввода маски. Записи исключений имеют более высокий приоритет, чем записи в области мониторинга.
Уровень важности событий	Kaspersky Industrial CyberSecurity for Nodes регистрирует события изменения файлов и реестра в области мониторинга. Доступны следующие уровни важности событий: **Информационные**, **Предупреждение**, **Критические**.

Запуск задачи Мониторинг целостности системы на основе эталона

Задача **Мониторинг целостности системы на основе эталона** позволяет проверять изменения в файлах, реестре, а также контролировать подключение внешних устройств. Для контроля изменений файлов вы можете запустить задачу **Мониторинг целостности системы на основе эталона** в следующих режимах:

- **Полная проверка**. В этом режиме приложение проверяет все атрибуты и хеши файлов.
- **Быстрая проверка**. В этом режиме приложение проверяет только атрибуты файлов.

Режим запуска задачи не влияет на контроль приложением реестра или внешних устройств.

Как запустить задачу Мониторинг целостности системы на основе эталона в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи. Следуйте его указаниям.

3. Выберите **Kaspersky Industrial CyberSecurity for Nodes → Мониторинг целостности системы на основе эталона**. Выберите режим мониторинга целостности системы:

   - **Полная проверка**. В этом режиме приложение проверяет все атрибуты и хеши файлов.
   - **Быстрая проверка**. В этом режиме приложение проверяет только атрибуты файлов.

4. Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

   - Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – нераспределенные устройства. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
   - Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
   - Задать выборку устройств, для которой требуется запускать задачу.
   - Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.

5. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу с правами учетной записи локального пользователя.

6. Настройте расписание запуска задачи, например, вручную или в определенный день недели.

7. Введите название задачи.

8. Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как запустить задачу Мониторинг целостности системы на основе эталона в Web Console

1. В главном окне Web Console выберите **Управление активами → Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите Kaspersky Industrial CyberSecurity for Nodes.

   b. В раскрывающемся списке **Тип задачи** выберите **Мониторинг целостности системы на основе эталона**.

   c. В поле **Название задачи** введите короткое описание, например, *Еженедельная проверка целостности системы*.

4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

5. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Перейдите к следующему шагу.

6. Выберите алгоритм расчета контрольной суммы.

7. Выберите учетную запись для запуска задачи. По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу с правами учетной записи локального пользователя.

8. Завершите работу мастера.

   В списке задач отобразится новая задача.

9. Нажмите на новую задачу.

   Откроется окно свойств задачи.

10. Выберите закладку **Параметры приложения**.

11. Выберите режим проверки целостности системы:

    - **Полная проверка**. В этом режиме приложение проверяет все атрибуты и хеши файлов.
    - **Быстрая проверка**. В этом режиме приложение проверяет только атрибуты файлов.

12. Сохраните внесенные изменения.

13. Установите флажок напротив задачи.

14. Нажмите на кнопку **Запустить**.

Экспорт и импорт правил Контроля целостности системы

Вы можете экспортировать список правил Контроля целостности системы в файл формата XML. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество однотипных записей. Вы можете использовать функцию экспорта/импорта для резервного копирования списка правил Контроля целостности системы или для миграции списка на другой сервер.

Контроль целостности системы не поддерживает импорт ключей `HKEY_CURRENT_USER` и `HKEY_CURRENT_CONFIG` для задачи *Проверка целостности системы*. Если область мониторинга задачи содержит эти ключи, приложение формирует событие *Область мониторинга содержит некорректные объекты*.

Как экспортировать/импортировать список правил Контроля целостности системы в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне свойств политики выберите **Диагностика системы**.

4. В разделе **Контроль целостности системы** нажмите **Настройка**.

5. В зависимости от того, какие правила вы хотите экспортировать/импортировать, перейдите на вкладку **Файлы** или **Реестр**.

6. Для экспорта списка правил действий с файлами / действий с реестром списка выполните следующие действия:

   a. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

   b. Если вы хотите экспортировать только часть списка, выполните следующие действия:

      1. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A.**

      2. Нажмите на кнопку и выберите **Экспортировать выбранное**.

   c. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список правил в XML-файл.

7. Для импорта правил действий с файлами / действий с реестром выполните следующие шаги:

   a. Нажмите на кнопку **Импорт**.

      В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Откройте файл.

      Если на компьютере уже есть список правил, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

8. Сохраните внесенные изменения.

Как экспортировать/импортировать список правил Контроля целостности системы в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Диагностика системы → Контроль целостности системы** и нажмите на кнопку **Настроить**.

   Откроется окно **Настройки Контроля целостности системы**.

5. Для экспорта правил действий с файлами / действий с реестром выполните следующие шаги:

   a. На вкладке **Файл** или **Реестр** выберите правила, которые вы хотите экспортировать.

   b. Нажмите на кнопку **Экспорт.** В открывшемся окне укажите, хотите ли вы экспортировать только выбранные правила или все правила и нажмите на кнопку **Экспорт**.

      Если вы не выбрали ни одного правила, Kaspersky Industrial CyberSecurity for Nodes экспортирует все правила.

      Kaspersky Industrial CyberSecurity for Nodes экспортирует список правил в XML-файл.

6. Для импорта правил действий с файлами / действий с реестром выполните следующие шаги:

   a. На вкладке **Файл** или **Реестр** нажмите на кнопку **Импорт из предыдущей версии**, если хотите импортировать правила из XML-файла, созданного в приложении версии 4.0 или ранее.

   При импорте правил из XML-файла, созданного в приложении версии 4.5 и выше, нажмите на кнопку **Импорт**.

   b. Если на компьютере уже есть список правил, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

   c. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   d. Нажмите на кнопку **Импорт**.

7. Сохраните внесенные изменения.

Как экспортировать/импортировать список правил Контроля целостности системы в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Мониторинг целостности системы → Контроль целостности системы**.

2. В панели результатов узла **Контроль целостности системы** нажмите **Свойства**.

   Откроется окно **Свойства: Контроль целостности системы**.

3. В зависимости от того, какие правила вы хотите экспортировать/импортировать, перейдите на вкладку **Файлы** или **Реестр**.

4. Для экспорта списка правил действий с файлами / действий с реестром списка выполните следующие действия:

   a. Если вы хотите экспортировать список целиком, нажмите на кнопку и выберите **Экспортировать**.

   b. Если вы хотите экспортировать только часть списка, выполните следующие действия:

      1. Выделите элементы списка, которые вы хотите экспортировать, используя клавиши **Ctrl** или **Shift**. Для выбора всех элементов нажмите комбинацию клавиш **Ctrl+A.**

      2. Нажмите на кнопку и выберите **Экспортировать выбранное**.

   c. В открывшемся окне укажите имя файла формата XML, в который вы хотите выполнить экспорт, и выберите папку для сохранения файла. Нажмите на кнопку **Сохранить**.

   Kaspersky Industrial CyberSecurity for Nodes экспортирует список правил в XML-файл.

5. Для импорта правил действий с файлами / действий с реестром выполните следующие шаги:

   a. Нажмите на кнопку **Импортировать**.

   В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список правил.

   b. Откройте файл.

   Если на компьютере уже есть список правил, Kaspersky Industrial CyberSecurity for Nodes предложит удалить действующий список или добавить в него новые записи из XML-файла.

6. Сохраните внесенные изменения.

Просмотр отчетов о работе Контроля целостности системы

Для анализа работы правил Контроля целостности системы вы можете изучать отчеты, а также просматривать события, сформированные приложением. Kaspersky Industrial CyberSecurity for Nodes формирует следующие отчеты о работе компонента:

- Отчет о компьютерах, на которых произошло максимальное количество срабатываний правил мониторинга.
- Отчет о наиболее часто срабатывающих правилах мониторинга.

  Для формирования отчета о наиболее часто срабатывающих правилах мониторинга приложение регистрирует следующие события:

  - *Обнаружено изменение файла или папки;*
  - *Только статистика: запрещенная файловая операция в контролируемой области*;
  - *Разрешенная файловая операция в контролируемой области, выполненная доверенным пользователем*;
  - *Подозрительная файловая операция в контролируемой области*.

  > Для настройки времени хранения этих событий следует в разделе политики **Настройка событий** задать срок для общего события Контроля целостности системы – *Обнаружено изменение файла или папки.*

По умолчанию отчет создается за последние 30 дней, включая дату создания отчета.

Как просмотреть отчеты о работе Контроля целостности системы в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите вкладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. На шаге **Выбор типа шаблона отчета** выберите отчет о работе Контроля целостности системы (раздел **Другое**):

   - **Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего**.
   - **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах**.

После завершения работы мастера создания шаблона отчета в таблице на вкладке **Отчеты** появится новый шаблон отчета.

5. Откройте отчет двойным щелчком мыши.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Как просмотреть отчеты о работе Контроля целостности системы в Web Console

1. В главном окне Web Console выберите **Мониторинг → Отчеты**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания шаблона отчета.
3. В блоке **Шаблон** в разделе **Другое** выберите отчет о работе Контроля целостности системы:

   - **Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего**.
   - **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах**.

   После завершения работы мастера создания шаблона отчета в таблице появится новый шаблон отчета.
4. Выберите и запустите отчет.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Также вы можете просматривать события, сформированные приложением, в консоли Kaspersky Security Center с помощью выборок событий.

Анализ журналов

Компонент Анализ журналов контролирует целостность защищаемой среды на основе журналов событий Windows. При обнаружении признаков нетипичного поведения в системе приложение информирует администратора, так как это поведение может указывать на попытки кибератак.

Kaspersky Industrial CyberSecurity for Nodes анализирует журналы событий Windows и выявляет нарушения в соответствии с правилами. В компонент включены предустановленные правила. Для работы предустановленных правил приложение использует эвристический анализ. Также вы можете добавить собственные правила (пользовательские правила). При срабатывании правила приложение создает событие со статусом *Критическое*.

Для работы Анализа журналов убедитесь, что политика аудита безопасности настроена и система регистрирует нужные события (подробнее см. на сайте Службы технической поддержки Microsoft).

Параметр	Описание
Предустановленные правила	Список правил Анализа журналов. Предустановленные правила включают шаблоны аномальной активности на защищаемом компьютере. Аномальная активность может являться признаком попытки атаки.
Пользовательские правила	Список правил Анализа журналов, которые добавил пользователь. Вы можете задать собственные критерии срабатывания правила Анализа журналов. Для этого вам нужно ввести идентификатор события и выбрать источник событий. Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*. Также вы можете указать журнал стороннего приложения.

Добавление пользовательских правил

Вы можете задать собственные критерии срабатывания правила Анализа журналов. Для этого вам нужно ввести идентификатор события и выбрать источник событий. Вы можете узнать идентификатор события на сайте Службы технической поддержки Microsoft . Для выбора источника событий доступны стандартные журналы: *Application*, *Security* или *System*. Также вы можете указать журнал стороннего приложения. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал *Windows PowerShell*).

Приложение не выполняет проверок на фактическое наличие заданного журнала в журнале событий Windows. Если название журнала введено с ошибкой, приложение не будет контролировать события из этого журнала.

В список пользовательских правил уже добавлено несколько правил, которые созданы специалистами "Лаборатории Касперского".

Как добавить пользовательское правило в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Диагностика системы**.

4. В разделе **Анализ журналов** нажмите **Настройка**.

5. Установите флажок **Анализ журналов**.

6. На закладке **Пользовательские правила** установите флажок **Применять пользовательские правила для анализа журналов**.

7. Установите флажки напротив тех пользовательских правил, которые вы хотите включить.

8. Если требуется, создайте собственные пользовательские правила по кнопке **Добавить**.

9. В открывшемся окне настройте параметры пользовательского правила:

   - **Имя правила**.
   - **Имя журнала**. Журналы событий Windows. Доступны следующие журналы: *Application*, *Security*, *System*.
   - **Источник**. Журналы событий сторонних приложений. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал Windows PowerShell).
   - **Идентификаторы событий**. Идентификаторы событий в журнале событий Windows. Вы можете узнать идентификатор события в справке Microsoft.

10. Сохраните внесенные изменения.

Как добавить пользовательское правило в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Диагностика системы** → **Анализ журналов** и нажмите на кнопку **Настроить**.

5. Установите флажок **Включить Анализ журналов**.

6. На закладке **Пользовательские правила** установите флажок **Применять пользовательские правила для анализа журналов**.

7. Настройте работу пользовательских правил с помощью переключателей.

8. Если требуется, создайте собственные пользовательские правила по кнопке **Добавить**.

9. В открывшемся окне настройте параметры пользовательского правила:

   - **Имя правила**.
   - **Имя журнала событий Windows**. Журналы событий Windows. Доступны следующие журналы: *Application*, *Security*, *System*.

- **Источник**. Журналы событий сторонних приложений. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал Windows PowerShell).

- **Идентификатор события**. Идентификаторы событий в журнале событий Windows. Вы можете узнать идентификатор события в справке Microsoft.

10. Сохраните внесенные изменения.

Как добавить пользовательское правило в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Мониторинг целостности системы → Анализ журналов**.

2. В панели результатов узла **Анализ журналов** нажмите **Свойства**.

   Откроется окно **Свойства: Анализ журналов**.

3. Установите флажок **Анализ журналов**.

4. На закладке **Пользовательские правила** установите флажок **Применять пользовательские правила для анализа журналов**.

5. Установите флажки напротив тех пользовательских правил, которые вы хотите включить.

6. Если требуется, создайте собственные пользовательские правила по кнопке **Добавить**.

7. В открывшемся окне настройте параметры пользовательского правила:

   - **Имя правила**.

   - **Имя журнала**. Журналы событий Windows. Доступны следующие журналы: *Application*, *Security*, *System*.

   - **Источник**. Журналы событий сторонних приложений. Название журнала стороннего приложения вы можете узнать с помощью инструмента Просмотр событий. Журналы сторонних приложений расположены в папке Журналы приложений и служб (например, журнал Windows PowerShell).

   - **Идентификаторы событий**. Идентификаторы событий в журнале событий Windows. Вы можете узнать идентификатор события в справке Microsoft.

8. Сохраните внесенные изменения.

В результате Kaspersky Industrial CyberSecurity for Nodes при срабатывании правила будет создавать события со статусом *Критическое*.

Настройка предустановленных правил

Предустановленные правила включают шаблоны аномальной активности на защищаемом компьютере. Аномальная активность может являться признаком попытки атаки. Для работы предустановленных правил приложение использует эвристический анализ. Для Анализа журналов доступно семь предустановленных правил. Вы можете включать и выключать любые правила. Удалить предустановленные правила невозможно.

Вы можете настроить критерии срабатывания правил, которые контролируют события для следующих операций:

- обработка подбора пароля;
- обработка сетевого входа.

Как настроить предустановленные правила в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Диагностика системы**.
4. В разделе **Анализ журналов** нажмите **Настройка**.
5. Установите флажок **Анализ журналов**.
6. На закладке **Предустановленные правила** установите флажок **Применить предустановленные правила для анализа журналов**.
7. Настройте работу предустановленных правил с помощью флажков:
   - **Обнаружена возможная попытка взлома пароля с помощью подбора**.
   - **Обнаружена подозрительная активность во время сетевого сеанса входа**.
   - **Обнаружены признаки компрометации журналов Windows**.
   - **Обнаружена подозрительная активность со стороны новой установленной службы**.
   - **Обнаружена подозрительная аутентификация с явным указанием учетных данных**.
   - **Обнаружены признаки атаки Kerberos forged PAC (MS14-068)**.
   - **Обнаружены подозрительные изменения привилегированной группы Администраторы**.
8. Если требуется, настройте параметры правила **Обнаружена возможная попытка взлома пароля с помощью подбора**:
   a. Нажмите на кнопку **Настройка** напротив правила.
   b. В открывшемся окне укажите количество попыток и промежуток времени, в течение которого выполнялись попытки ввода пароля, для срабатывания правила.
   c. Нажмите на кнопку **ОК**.
9. Если вы выбрали правило **Обнаружена подозрительная активность во время сетевого сеанса входа**, вам нужно настроить параметры правила:
   a. Нажмите на кнопку **Настройка** напротив правила.
   b. В открывшемся окне в блоке **Обработка атипичной аутентификации** укажите начало и конец временного интервала.

Kaspersky Industrial CyberSecurity for Nodes будет считать аномальной активностью выполненные попытки входа в течение заданного интервала.

По умолчанию интервал не задан и приложение не контролирует попытки входа. Чтобы приложение постоянно контролировало попытки входа, задайте интервал 12:00 AM – 11:59 PM. Начало и конец интервала не должны совпадать. Если они совпадают, приложение не контролирует попытки входа.

c. Сформируйте списки доверенных пользователей и доверенных IP-адресов компьютеров (IPv4 и IPv6).

Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Kaspersky Industrial CyberSecurity for Nodes не будет контролировать попытки входа для этих пользователей и компьютеров.

> Исключение доверенных компьютеров по IP-адресу не работает в приложении под управлением операционной системы Windows XP.

d. Нажмите на кнопку **OK**.

10. Сохраните внесенные изменения.

Как настроить предустановленные правила в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Диагностика системы** → **Анализ журналов** и нажмите на кнопку **Настроить**.
5. Установите флажок **Включить Анализ журналов**.
6. На закладке **Предустановленные правила** установите флажок **Использовать предустановленные правила для анализа журналов**.
7. Настройте работу предустановленных правил с помощью переключателей:
   - **Обнаружена возможная попытка взлома пароля с помощью подбора**.
   - **Обнаружена подозрительная активность во время сетевого сеанса входа**.
   - **Обнаружены признаки компрометации журналов Windows**.
   - **Обнаружена подозрительная активность со стороны новой установленной службы**.
   - **Обнаружена подозрительная аутентификация с явным указанием учетных данных**.
   - **Обнаружены признаки атаки Kerberos forged PAC (MS14-068)**.
   - **Обнаружены подозрительные изменения привилегированной группы Администраторы**.

8. На закладке **Расширенные** укажите следующие параметры:

   - Количество попыток и промежуток времени, в течение которого выполнялись попытки ввода пароля для срабатывания правила **Обнаружена возможная попытка взлома пароля с помощью подбора**.

   - Для срабатывания правила **Обнаружена подозрительная активность во время сетевого сеанса входа** укажите начало и конец временного интервала, в течение которого все попытки входа расцениваются приложением как аномальная активность.

     По умолчанию интервал не задан, и приложение не контролирует попытки входа. Чтобы приложение постоянно контролировало попытки входа, задайте интервал 12:00 AM – 11:59 PM. Начало и конец интервала не должны совпадать. Если они совпадают, приложение не контролирует попытки входа.

9. Сформируйте списки доверенных пользователей и доверенных IP-адресов компьютеров (IPv4 и IPv6) на соответствующих закладках.

   Вы можете выбрать пользователей из списка учетных записей или ввести имя локального пользователя вручную.

   > Исключение доверенных компьютеров по IP-адресу не работает в приложении под управлением операционной системы Windows XP.

10. Сохраните внесенные изменения.

Как настроить предустановленные правила в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Мониторинг целостности системы → Анализ журналов**.

2. В панели результатов узла **Анализ журналов** нажмите **Свойства**.

   Откроется окно **Свойства: Анализ журналов**.

3. Установите флажок **Анализ журналов**.

4. На закладке **Предустановленные правила** установите флажок **Применить предустановленные правила для анализа журналов**.

5. Настройте работу предустановленных правил с помощью флажков:

   - **Обнаружена возможная попытка взлома пароля с помощью подбора**.
   - **Обнаружена подозрительная активность во время сетевого сеанса входа**.
   - **Обнаружены признаки компрометации журналов Windows**.
   - **Обнаружена подозрительная активность со стороны новой установленной службы**.
   - **Обнаружена подозрительная аутентификация с явным указанием учетных данных**.
   - **Обнаружены признаки атаки Kerberos forged PAC (MS14-068)**.
   - **Обнаружены подозрительные изменения привилегированной группы Администраторы**.

6. Если требуется, настройте параметры правила **Обнаружена возможная попытка взлома пароля с помощью подбора**:

   a. Нажмите на кнопку **Настройка** напротив правила.

   b. В открывшемся окне укажите количество попыток и промежуток времени, в течение которого выполнялись попытки ввода пароля, для срабатывания правила.

   c. Нажмите на кнопку **OK**.

7. Если вы выбрали правило **Обнаружена подозрительная активность во время сетевого сеанса входа**, вам нужно настроить параметры правила:

   a. Нажмите на кнопку **Настройка** напротив правила.

   b. В открывшемся окне в блоке **Обработка атипичной аутентификации** укажите начало и конец временного интервала.

   Kaspersky Industrial CyberSecurity for Nodes будет считать аномальной активностью выполненные попытки входа в течение заданного интервала.

   По умолчанию интервал не задан и приложение не контролирует попытки входа. Чтобы приложение постоянно контролировало попытки входа, задайте интервал 12:00 AM – 11:59 PM. Начало и конец интервала не должны совпадать. Если они совпадают, приложение не контролирует попытки входа.

   c. Сформируйте списки доверенных пользователей и доверенных IP-адресов компьютеров (IPv4 и IPv6).

   Вы можете выбрать пользователей в Active Directory, из списка учетных записей в Kaspersky Security Center или ввести имя локального пользователя вручную. Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Сформируйте список пользователей из Active Directory. Kaspersky Industrial CyberSecurity for Nodes не будет контролировать попытки входа для этих пользователей и компьютеров.

   > Исключение доверенных компьютеров по IP-адресу не работает в приложении под управлением операционной системы Windows XP.

   d. Нажмите на кнопку **OK**.

8. Сохраните внесенные изменения.

В результате Kaspersky Industrial CyberSecurity for Nodes при срабатывании правила будет создавать события со статусом *Критическое*.

Анализатор производительности

Задача *Анализатор производительности* позволяет сформировать перечень наиболее активных приложений и файлов, к которым происходит наибольшее количество обращений. Вы можете использовать полученную информацию для формирования доверенной зоны, чтобы минимизировать влияние работы приложения на промышленное ПО.

Для корректной работы задачи *Анализатор производительности* компьютер, на котором запускается задача, должен быть под управлением ОС Windows Vista или выше.

Управление задачей доступно только из Web Console и Консоли приложения.

Настройка параметров и запуск задачи Анализатор производительности в Web Console

1. Запустите мастер создания задачи.
2. В раскрывающемся списке **Тип задачи** выберите **Анализатор производительности**.
3. Введите название задачи или оставьте название по умолчанию.
4. Выберите устройства, для которых будет назначена задача и нажмите на кнопку **Далее**.
5. В окне **Область действия задачи** укажите область действия задачи и нажмите на кнопку **Далее**.
6. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись и нажмите на кнопку **Далее**.
7. В окне **Завершение создания задачи** установите флажок **Открыть окно свойств задачи после ее создания** и нажмите на кнопку **Готово**.
8. В открывшемся окне выберите вкладку **Параметры приложения**.
9. Перейдите в раздел **Настройки Анализатора производительности**.
10. В поле **Автоматически остановить задачу через** задайте период времени в часах (1–168 часов) или днях (1–7 дней), по прошествии которого Kaspersky Industrial CyberSecurity for Nodes остановит выполнение анализа.
11. Если требуется, в блоке **Ограничение области формирования правил** сформируйте список папок, в рамках которого Kaspersky Industrial CyberSecurity for Nodes будет проводить анализ и формировать правила исключений:

    Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. Также вы можете добавлять в область анализа сетевые папки, указывая пути к ним в формате UNC (Universal Naming Convention).

    По умолчанию Kaspersky Industrial CyberSecurity for Nodes выполняет задачу без ограничения области анализа.
12. Перейдите на вкладку **Расписание** и настройте расписание задачи.
13. Сохраните внесенные изменения.
14. Установите флажок напротив названия созданной задачи и нажмите на кнопку **Запустить**.

Настройка параметров и запуск задачи Анализатор производительности в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Мониторинг целостности системы → Анализатор производительности**.
2. В панели результатов нажмите на ссылку **Свойства**.
3. В открывшемся окне на вкладке **Настройки задачи** задайте в поле **Остановить задачу через** период времени в часах (1–168 часов) или днях (1–7 дней), по прошествии которого Kaspersky Industrial CyberSecurity for Nodes остановит выполнение анализа.
4. Если требуется, в блоке **Область формирования правил** сформируйте список папок, в рамках которого Kaspersky Industrial CyberSecurity for Nodes будет проводить анализ и формировать правила исключений:

   Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. Также вы можете добавлять в область анализа сетевые папки, указывая пути к ним в формате UNC (Universal Naming Convention).

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes выполняет задачу без ограничения области анализа.
5. Перейдите на вкладку **Режим запуска**.
6. Выберите вариант **Вручную** или настройте режим запуска задачи.
7. При необходимости в блоке **Пользователь** укажите учетную запись для запуска задачи.
8. Нажмите на кнопку **ОК** для сохранения внесенных изменений.
9. В блоке **Управление** нажмите на ссылку **Запустить**.

Вы можете экспортировать результаты выполнения задачи *Анализатор производительности* напрямую в настройки доверенной зоны политики Kaspersky Industrial CyberSecurity for Nodes или локальные настройки доверенной зоны приложения, либо сохранить данные об объектах из отчетов в XML-файл, который далее может быть импортирован в настройки.

Kaspersky Industrial CyberSecurity for Nodes добавит файлы из отчета в список исключений из проверки, а приложения – в список доверенных приложений доверенной зоны.

Экспорт результатов выполнения задачи Анализатор производительности в Web Console

1. Для экспорта результатов локальной задачи выполните следующие действия:
   a. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
   b. Нажмите на название устройства, для которого вы хотите настроить параметры задачи.
   c. В открывшемся окне **<Имя устройства>** выберите вкладку **Задачи**.
   d. Нажмите на нужную задачу Анализатор производительности.
2. Для экспорта результатов групповой задачи выполните следующие действия:
   a. В главном окне Web Console выберите **Управление активами → Задачи**.
   b. Нажмите на нужную задачу Анализатор производительности.

3. В открывшемся окне выберите вкладку **Параметры приложения**.

   Откроется окно свойств задачи.

4. Перейдите в раздел **Результаты Анализатора производительности**.

5. Установите флажок **Учитывать хеши файлов**, чтобы включить хеши в отчет. По умолчанию флажок снят.

6. При необходимости снимите флажок **Учитывать пути файлов**, чтобы исключить из отчета пути файлов. По умолчанию флажок установлен.

   > Должен быть установлен хотя бы один из флажков **Учитывать хеши файлов**, **Учитывать пути файлов**.

7. Выберите объекты для экспорта на вкладках **Файлы** и **Приложения**.

   Вы можете экспортировать отчет целиком или раскрыть отчет и выбрать отдельные объекты для экспорта.

8. Для экспорта результатов выполнения задачи в настройки доверенной зоны политики выполните следующие действия:

   a. Нажмите на кнопку **Экспортировать в настройки**.

   b. В открывшемся окне установите флажок рядом с названием политики, в которую будут экспортированы настройки и нажмите на кнопку **Экспортировать**.

      Если в политике уже есть список исключений, Kaspersky Industrial CyberSecurity for Nodes добавит в него новые записи.

9. Для экспорта результатов выполнения задачи в XML-файл:

   a. Нажмите на кнопку **Экспортировать в файл**.

   b. Нажмите на кнопку **Экспорт**. В открывшемся окне укажите, хотите ли вы экспортировать только выбранные объекты или все объекты и нажмите на кнопку **Экспорт**.

Экспорт результатов выполнения задачи Анализатор производительности в Консоли приложения

> Экспорт результатов задачи Анализатор производительности в локальные настройки доверенной зоны приложения Kaspersky Industrial CyberSecurity for Nodes будет доступен в Консоли Kaspersky Industrial CyberSecurity for Nodes, если установлены флажки **Разрешить использование локальных исключений** и **Разрешать редактирование локальных доверенных приложений** на закладках **Исключения из проверки** и **Доверенные приложения** в разделе политики **Дополнительные возможности → Доверенная зона**.

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Мониторинг целостности системы → Анализатор производительности**.

2. В панели результатов нажмите на ссылку **Результаты**.

   Откроется окно **Результаты Анализатора производительности**.

3. Установите флажок **Учитывать хеши файлов**, чтобы включить хеши в отчет. По умолчанию флажок снят.

4. При необходимости снимите флажок **Учитывать пути файлов**, чтобы исключить из отчета пути файлов. По умолчанию флажок установлен.

   Должен быть установлен хотя бы один из флажков **Учитывать хеши файлов**, **Учитывать пути файлов**.

5. Выберите объекты для экспорта на вкладках **Файлы** и **Приложения**.

   Вы можете экспортировать отчет целиком или раскрыть отчет и выбрать отдельные объекты для экспорта.

6. Для экспорта результатов выполнения задачи в настройки доверенной зоны приложения выполните следующие действия:

   a. Нажмите на кнопку **Экспорт в настройки**.

   b. Подтвердите, что вы хотите экспортировать выбранные объекты в настройки доверенной зоны.

      Если в настройках уже есть список исключений, Kaspersky Industrial CyberSecurity for Nodes добавит в него новые записи.

7. Для экспорта результатов выполнения задачи в XML-файл:

   a. Нажмите на кнопку **Экспорт в файл**.

   b. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список объектов, а также выберите папку, в которую вы хотите сохранить этот файл.

Проверка по требованию

Этот раздел содержит информацию о задачах проверки по требованию, а также инструкции по настройке задач проверки по требованию и по настройке параметров безопасности защищаемого устройства.

О задачах проверки по требованию

Kaspersky Industrial CyberSecurity for Nodes проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Industrial CyberSecurity for Nodes проверяет файлы и оперативную память защищаемого устройства, а также объекты автозапуска.

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие задачи проверки по требованию:

- Задача *Проверка при старте операционной системы* выполняется каждый раз при запуске Kaspersky Industrial CyberSecurity for Nodes. Приложение проверяет загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Industrial CyberSecurity for Nodes создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, приложение заменяет их резервными копиями.

  Задача *Проверка при старте операционной системы* создается автоматически после установки. По умолчанию применяется режим **Информировать**. В этом случае после развертывания Kaspersky Industrial CyberSecurity for Nodes на устройствах можно включить задачу *Проверка при старте операционной системы*, если во время проверки не было обнаружено проблем со службами операционной системы. Если приложение определяет, что критические службы операционной системы являются зараженными или возможно зараженными, режим **Информировать** позволяет выяснить причину и решить проблему. Лечение или удаление системных файлов могут привести к критическим проблемам при запуске операционной системы. Если приложение применяет режим **Рекомендуемый**, выполняется действие **Выполнять рекомендуемое действие**.

  > Задача *Проверка при старте операционной системы* может не выполняться, если защищаемое устройство выходит из спящего режима или режима гибернации. Задача выполняется только при перезагрузке защищаемого устройства или при его запуске после полного выключения.

- По умолчанию задача *Проверка важных областей* выполняется еженедельно по расписанию. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Kaspersky Industrial CyberSecurity for Nodes применяет параметры безопасности, соответствующие уровню **Информировать**. Вы можете изменять параметры задачи *Проверка важных областей*.

- Задача *Проверка целостности приложения* выполняется ежедневно. Она обеспечивает проверку модулей Kaspersky Industrial CyberSecurity for Nodes на предмет наличия повреждений или изменений. Проверяется папка установки программы. Статистика выполнения задачи содержит сведения о количестве проверенных и поврежденных модулей. Значения параметров задачи устанавливаются по умолчанию и не доступны для изменения. Вы можете настраивать расписание запуска задачи.

- Задача *Проверка съемных дисков* проверяет все файлы, которые вы запускаете или копируете, даже если файл расположен на съемном диске. Для предотвращения распространения вирусов и других приложений, представляющих угрозу, вы можете настроить автоматическую проверку съемных дисков при подключении к компьютеру.

- Задача *Полная проверка* выполняется еженедельно. Задача обеспечивает тщательную проверку защищаемого устройства, включая проверку системного резервного хранилища, загрузочных секторов и почты.

Кроме того, вы можете создать пользовательскую задачу проверки по требованию, например, задачу проверки папок общего доступа на защищаемом устройстве.

Kaspersky Industrial CyberSecurity for Nodes может одновременно выполнять несколько задач проверки по требованию.

Об области проверки и параметрах безопасности задачи

В Консоли приложения область проверки выбранной задачи проверки по требованию представляет собой список файловых ресурсов защищаемого устройства, которые может контролировать Kaspersky Industrial CyberSecurity for Nodes.

Элементы и узлы в списке файловых ресурсов защищаемого устройства отображаются следующим образом:

☑ Узел включен в область проверки.

☐ Узел исключен из области проверки.

Параметры безопасности

В выбранной задаче проверки по требованию можно изменять заданные по умолчанию параметры безопасности, настроив их либо едиными для всей области защиты или проверки, либо различными для разных узлов или элементов в списке файловых ресурсов устройства.

Если один объект входит в несколько записей области защиты и эти записи имеют разные уровни безопасности, то приоритет последнего правила в списке выше. Например, область защиты включает в себя две записи: **Все жесткие диски** (уровень безопасности **Информировать**) и `*\Users\*\Downloads\*` (уровень безопасности **Другой**). Приложение будет проверять память жестких дисков в соответствии с уровнем безопасности Информировать, кроме папки `Downloads`. Папку `Downloads` приложение будет проверять в соответствии с параметрами, заданными вручную, так как эта запись последняя в списке области защиты.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются ко всем вложенным узлам. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

- выбрать один из трех стандартных уровней безопасности (**Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**);
- Вручную изменить параметры безопасности для выбранных узлов или элементов в списке файловых ресурсов защищаемого устройства (уровень безопасности примет значение **Другой**).

Стандартные области проверки

Список файловых ресурсов защищаемого устройства для выбранной задачи проверки по требованию отображается в окне **Область проверки**.

В списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие стандартные области проверки:

- **Все жесткие диски**. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты на жестких дисках защищаемого устройства. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.
- **Все съемные диски**. Kaspersky Industrial CyberSecurity for Nodes проверяет файлы на внешних устройствах, например, на компакт-дисках или съемных дисках. Вы можете включать в область проверки или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Все сетевые диски**. Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, используемая для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются с правами системной учетной записи.

  Подключенные сетевые диски также не отображаются в дереве файловых ресурсов защищаемого устройства. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

- **Память ядра**. Kaspersky Industrial CyberSecurity for Nodes проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.
- **Запущенные процессы и объекты автозапуска**. Kaspersky Industrial CyberSecurity for Nodes проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM.INI, а также программные модули, которые автоматически запускаются при запуске защищаемого устройства.
- **Загрузочные секторы**. Kaspersky Industrial CyberSecurity for Nodes проверяет загрузочные секторы жестких и съемных дисков.

- **Системное резервное хранилище**. Kaspersky Industrial CyberSecurity for Nodes проверяет содержимое папки System Volume Information.

  В Kaspersky Industrial CyberSecurity for Nodes версии 5.0 почта исключена из области проверки приложения. Если вы используете плагин управления более ранней версии, то приложение исключает почту из области проверки, даже если эта область включена в политике.

Стандартные области проверки по умолчанию отображаются в дереве сетевых файловых ресурсов. Они доступны для добавления в список сетевых файловых ресурсов при его формировании в параметрах области проверки.

По умолчанию задачи проверки по требованию выполняются в следующих областях:

- Задача *Проверка при старте операционной системы*:
  - **Память ядра**.
  - **Загрузочные секторы**.
- Задача *Проверка важных областей*:
  - **Все жесткие диски** (исключая папки Windows).
  - **Все съемные диски**.
  - **Память ядра**.
  - **Запущенные процессы и объекты автозапуска**.
- Задача *Проверка по требованию*:
  - **Все жесткие диски** (исключая папки Windows).
  - **Все съемные диски**.
  - **Память ядра**.
  - **Запущенные процессы и объекты автозапуска**.
- Задача *Полная проверка*:
  - **Все жесткие диски** (исключая папки Windows).
  - **Все съемные диски**.
  - **Память ядра**.
  - **Запущенные процессы и объекты автозапуска**.
  - **Системное резервное хранилище**.
  - **Загрузочные секторы**.

Проверка файлов в интернет-хранилище

Об облачных файлах

Kaspersky Industrial CyberSecurity for Nodes может взаимодействовать с облачными файлами Microsoft OneDrive. Программа поддерживает новую функцию "файлы из OneDrive по запросу" (OneDrive Files On-Demand).

Kaspersky Industrial CyberSecurity for Nodes не поддерживает другие интернет-хранилища.

Функция "файлы из OneDrive по запросу" помогает получить доступ к вашим файлам OneDrive без необходимости загружать их и занимать дисковое пространство на вашем устройстве. При необходимости можно загрузить файлы на жесткий диск вашего устройства.

Когда функция "файлы из OneDrive по запросу" включена, рядом с каждым файлом в графе **Статус** в проводнике Windows отображается значок статуса. Файл может иметь один из следующих статусов:

Этот значок показывает, что файл доступен *только через интернет*. Файлы, доступные только через интернет, не хранятся физически на жестком диске. Если ваше устройство не подключено к интернету, не удастся открыть файлы, доступные только через интернет.

Этот значок показывает, что файл *доступен локально*. Он отображается, если вы открыли файл, доступный только через интернет, и он загрузился на ваше устройство. Доступные локально файлы можно открывать в любое время, даже без доступа в интернет. Чтобы освободить пространство, вы можете снова сделать файл доступным только через интернет ( ).

Этот значок показывает, что файл *хранится на жестком диске и всегда доступен*.

Проверка облачных файлов

Kaspersky Industrial CyberSecurity for Nodes может выполнять проверку только облачных файлов, сохраненных локально на защищаемом устройстве. Такие файлы OneDrive имеют статус или . Проверка файлов со статусом не выполняется, поскольку физически они не хранятся на защищаемом устройстве.

Во время проверки Kaspersky Industrial CyberSecurity for Nodes не выполняет автоматическую загрузку файлов со статусом из облачного хранилища, даже если они включены в область проверки.

Обработка облачных файлов выполняется различными задачами Kaspersky Industrial CyberSecurity for Nodes в различных сценариях, в зависимости от типа задачи:

- Постоянная проверка облачных файлов: вы можете добавить папки, содержащие облачные файлы, в область проверки компонента Постоянная защита файлов. Проверка файла выполняется, когда пользователь открывает его. Если пользователь открывает файл со статусом , этот файл загружается и становится доступным локально; его статус меняется на . Поэтому этот файл может быть обработан компонентом Постоянная защита файлов.

- Проверка облачных файлов по требованию: вы можете добавить папки, содержащие облачные файлы, в область проверки задачи проверки по требованию. Задача выполняет проверку файлов со статусами и . Если в области проверки задачи обнаружены файлы со статусом , эти файлы будут пропущены при проверке, а в журнале выполнения задачи будет зарегистрировано информационное событие, показывающее, что проверяемый файл является временной заменой облачного файла и отсутствует на локальном диске.

- Формирование и использование правил контроля запуска программ: можно создавать разрешающие и запрещающие правила для файлов со статусами и с помощью задачи *Формирование правил контроля запуска программ*. Компонент Контроль запуска программ обрабатывает и блокирует облачные файлы в соответствии с принципом запрета по умолчанию и созданными правилами.

  > Компонент Контроль запуска программ блокирует запуск всех облачных файлов, независимо от статуса файла. Файлы со статусом не входят в область формирования правила, поскольку они не хранятся физически на жестком диске. Для таких файлов невозможно создать разрешающих правил, поэтому они подчиняются принципу запрета по умолчанию.

Если в облачном файле OneDrive обнаружена угроза, программа применяет действие, указанное в параметрах задачи, выполняющей проверку. Таким образом, файл может быть удален, вылечен, помещен на карантин или в резервное хранилище.

> При изменении локальные файлы синхронизируются с копиями в облачном хранилище OneDrive в соответствии с принципами, описанными в документации к Microsoft OneDrive.

Стандартные уровни безопасности

> Параметр безопасности **Использовать эвристический анализ** не входит в набор параметров стандартных уровней безопасности. При изменении этого параметра, выбранный вами стандартный уровень безопасности не изменится.

Для выбранного узла в дереве файловых ресурсов узла можно задать один из четырех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый**, **Максимальная защита** или **Информировать**. Каждый из этих уровней имеет свои стандартные параметры безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Industrial CyberSecurity for Nodes на защищаемых устройствах и рабочих станциях, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность устройств. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты устройств в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если в сети организации предъявляются повышенные требования к безопасности устройств.

Информировать

Уровень безопасности **Информировать** рекомендуется, если в сети организации потенциально много зараженных компьютеров и их блокировка может существенно нарушить работу организации.

Стандартные уровни безопасности и соответствующие им значения параметров безопасности

Параметры	Уровень безопасности			
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**	**Информировать**
Типы объектов	Объекты, проверяемые по формату	Все объекты	Все объекты	Все объекты
Проверять только новые и измененные файлы	Включено	Выключено	Выключено	Выключено
Действия над зараженными и другими обнаруженными объектами	Лечить. Удалять, если лечение невозможно	Выполнять рекомендованное специалистами "Лаборатории Касперского" действие	Лечить. Удалять, если лечение невозможно	Информировать
Проверка составных файлов	Проверять все дистрибутивы и файлы офисных форматов	Проверять все архивы, дистрибутивы, файлы офисных форматов	Проверять все архивы, дистрибутивы, файлы офисных форматов	Проверять все архивы, дистрибутивы, файлы офисных форматов
Системно-критические объекты – это файлы, необходимые для работы операционной системы и Kaspersky Industrial CyberSecurity for Nodes. Такие объекты нельзя удалить. Процессы, относящиеся к таким объектам, не могут быть прекращены.				
Применять действие к выбранным типам объектов	По умолчанию проверяются все типы объектов	По умолчанию проверяются все типы объектов	По умолчанию проверяются все типы объектов	По умолчанию проверяются все типы объектов
Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением	Нет	Нет	Нет	Нет
Исключать файлы	Нет	Нет	Нет	Нет
Не проверять объекты по типу	Нет	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	Нет	Нет	Нет
Не проверять составные объекты размером более (МБ)	8 МБ	Нет	Нет	Нет
Использовать технологию iSwift	Да	Да	Да	Да
Использовать технологию iChecker	Да	Да	Да	Да

Проверка съемных дисков

Вы можете настроить проверку съемных дисков, подключенных к защищаемому устройству по USB.

Kaspersky Industrial CyberSecurity for Nodes запускает проверку подключенных съемных дисков при их регистрации в операционной системе в качестве внешних устройств, подключаемых по USB. Приложение не выполняет проверку съемного диска, если его подключение было заблокировано компонентом Контроль устройств.

Kaspersky Industrial CyberSecurity for Nodes не блокирует доступ к съемному диску на время проверки.

Результаты проверки каждого съемного диска доступны в журнале выполнения задачи проверки по требованию, созданной при подключении этого съемного диска.

Вы можете изменять значения параметров компонента Проверка съемных дисков (см. таблицу ниже).

Параметры проверки съемных дисков

Параметр	Значение по умолчанию	Описание
Проверять съемные диски при их подключении по USB	Флажок снят	Вы можете включать или выключать проверку съемных дисков при их подключении к защищаемому устройству.
Проверять съемный диск, если его размер не превышает (МБ)	4096 МБ	Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на проверяемом диске. Kaspersky Industrial CyberSecurity for Nodes не выполняет проверку съемного диска, если объем содержащихся на нем данных превышает указанное значение.
Запускать проверку с уровнем безопасности	Максимальная защита	Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности: • **Максимальная защита**; • **Рекомендуемый**; • **Максимальное быстродействие**; • **Информировать**. Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют стандартным уровням безопасности в задачах проверки по требованию.

Заданные по умолчанию параметры задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать локальные системные и пользовательские задачи проверки по требованию.

Заданные по умолчанию параметры задач проверки по требованию

Параметр	Значение по умолчанию	Описание
Область проверки	Применяется в следующих локальных системных и пользовательских задачах: • **Проверка при старте операционной системы**: защищаемое устройство целиком, за исключением папок общего доступа и объектов автозапуска. • **Проверка важных областей**: защищаемое устройство целиком, за исключением папок общего доступа и некоторых файлов операционной системы. • **Проверка по требованию** (пользовательские задачи): защищаемое устройство целиком. • **Полная проверка**: тщательная проверка защищаемого устройства.	Вы можете изменить область проверки. Область проверки нельзя настроить для локальных системных задач **Проверка съемных дисков** и **Проверка целостности приложения**.
Параметры безопасности	Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**.	Для узлов, выбранных в списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия: • выбрать другой стандартный уровень безопасности; • вручную изменить параметры безопасности.
Использовать эвристический анализ	Применяется с уровнем анализа **Средний** для задач *Проверка важных областей*, *Проверка при старте операционной системы*, *Проверка по требованию* и *Полная проверка*.	Вы можете включать и выключать применение эвристического анализатора и регулировать уровень анализа.
Параметры запуска задачи с определенными правами	Задача запускается с правами системной учетной записи.	Вы можете изменять параметры запуска задач с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задачи *Проверка целостности приложения*.
Выполнять задачу в фоновом режиме	Не применяется.	Вы можете настраивать приоритетность выполнения задач проверки по требованию.
Считать выполнение задачи проверкой важных областей	Применяется для задач *Проверка по требованию*, *Проверка при старте операционной системы*, *Проверка важных областей* и *Полная проверка*.	Вы можете настраивать приоритетность выполнения задач проверки по требованию.
Не запускать несколько задач проверки одновременно	Не применяется.	Вы можете настраивать приоритетность выполнения задач проверки по требованию.
Расписание запуска задачи	Применяется в локальных системных задачах: • *Проверка при старте операционной системы* – **После запуска приложения**; • *Проверка важных областей*, *Проверка целостности приложения* и *Полная проверка* – **Еженедельно**.	Можно настроить параметры для запуска задачи по расписанию.

Управление задачами проверки по требованию

В этом разделе описаны создание и настройка параметров задачи *Проверка по требованию* на защищаемом устройстве.

Создание задачи проверки по требованию

Создание задачи проверки по требованию в Консоли администрирования Kaspersky Security Center

1. Запустите мастер создания задачи.
2. В окне **Выбор типа задачи** выберите **Проверка по требованию** и нажмите на кнопку **Далее**.
3. В окне **Область проверки** сформируйте область проверки.

   По умолчанию область проверки включает критические области защищаемого устройства. Проверяемые области помечены в таблице значком ☑. Области, являющиеся исключениями из проверки, помечены в таблице значком ☐. Вы можете изменять область проверки: включать в нее отдельные стандартные области, диски, папки, сетевые объекты и файлы и устанавливать особые параметры безопасности для каждой из добавленных областей.

   - Чтобы исключить из проверки какую-либо область проверки, выберите соответствующий элемент списка и нажмите **Удалить**.
   - Чтобы включить стандартную область проверки, диск, папку, сетевой объект или файл в область проверки, выполните следующие действия:
     a. Нажмите на кнопку **Добавить**.
     b. В окне **Выбор области проверки** выберите стандартную область из списка и нажмите **ОК**.
   - Чтобы исключить вложенные папки или файлы из области проверки, выполните следующие действия:
     a. Выберите добавленную папку (диск) в окне **Область проверки.**
     b. Нажмите на кнопку **Изменить**.
     c. Снимите флажок **Включить вложенные папки**.
   - Чтобы изменить параметры безопасности области проверки, выполните следующие действия:
     a. Выберите область проверки, параметры которой требуется изменить, и нажмите на кнопку **Настроить**.
     b. В открывшемся окне выберите один из стандартных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную.

     Параметры безопасности настраиваются таким же образом, как и для задачи Постоянная защита файлов.

4. Настройте эвристический анализатор и интеграцию с другими компонентами:
   - Настройте применение эвристического анализатора.

- Установите флажок **Запускать задачу проверки в фоновом режиме**, если вы хотите присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*.

  По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes, имеют приоритет *Средний*.

- Установите флажок **Считать выполнение задачи проверкой важных областей**, если вы хотите использовать создаваемую задачу в качестве задачи *Проверка важных областей*.

- Установите флажок **Не запускать несколько задач проверки одновременно**, чтобы оптимизировать нагрузку на компьютер.

5. В окне **Выбор устройств, которым будет назначена задача** укажите список устройств и нажмите **Далее**.

6. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись и нажмите **Далее**.

7. В окне **Настройка расписания запуска задачи** укажите параметры запуска задачи по расписанию и нажмите **Далее**.

8. Введите название задачи.

   Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

9. Откроется окно **Завершение создания задачи**. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

Будет создана новая задача *Проверка по требованию* для выбранного защищаемого устройства или группы защищаемых устройств.

Создание задачи проверки по требованию в Web Console

1. Запустите мастер создания задачи.

2. В окне **Новая задача** в раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.

3. В раскрывающемся списке **Тип задачи** выберите **Проверка по требованию** и нажмите на кнопку **Далее**.

4. Выберите область действия задачи и нажмите **Далее**.

5. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись и нажмите **Далее**.

6. Введите название задачи.

   Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

7. Откроется окно **Завершение создания задачи**. Нажмите на кнопку **Готово**, чтобы завершить создание задачи.

Будет создана новая задача *Проверка по требованию* для выбранного защищаемого устройства или группы защищаемых устройств.

Создание задачи проверки по требованию в Консоли приложения

Вы можете создавать пользовательские задачи для отдельного защищаемого устройства в узле **Проверка по требованию**.

Чтобы создать и настроить задачу проверки по требованию, выполните следующие действия:

1. В дереве Консоли приложения откройте контекстное меню узла **Проверка по требованию**.
2. Выберите вариант **Создать задачу**.

   Откроется окно **Создать задачу**.
3. Укажите имя задачи и нажмите **OK**.

Будет создана задача *Проверка по требованию* для отдельного защищаемого устройства.

Выполнение задач проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes, имеют приоритет *Средний*.

Вы можете присвоить процессу, в котором будет выполняться задача *Проверка по требованию*, приоритет *Низкий*. Понижение приоритета процесса увеличивает время выполнения задачи, но может положительно повлиять на скорость выполнения процессов других запущенных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме.

Чтобы изменить приоритет задачи *Проверка по требованию*, установите или снимите флажок **Запускать задачу проверки в фоновом режиме** в настройках задачи.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Регистрация выполнения задачи Проверка важных областей

По умолчанию статус защиты устройства отображается в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** и обновляется еженедельно после завершения задачи *Проверка важных областей*.

Время обновления статуса защиты устройства привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**.

Настройка области проверки для задачи проверки по требованию

Если вы изменили область проверки в задачах *Проверка при старте операционной системы* и *Проверка важных областей*, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Industrial CyberSecurity for Nodes, запустив мастер установки приложения.

Настройка области проверки для задачи проверки по требованию в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный компьютер.
2. В рабочей области выберите вкладку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. Перейдите в раздел **Задачи**.
5. Двойным щелчком мыши откройте окно свойств задачи **Проверка по требованию**.
6. Выберите раздел **Область проверки**.
7. Чтобы включить элементы списка в область проверки, установите флажки напротив соответствующих областей проверки.
8. Если вы хотите добавить область проверки, которой нет в списке, то выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне выберите область проверки, отдельный диск, папку или сетевой объект.
   c. Если хотите включать вложенные папки в область проверки, установите флажок **Включить вложенные папки**.
9. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов.
10. Чтобы изменить область проверки, выберите эту область в списке и нажмите на кнопку **Изменить**.
11. Чтобы скрыть добавленную ранее область проверки из списка сетевых файловых ресурсов, выберите область проверки и нажмите на кнопку **Удалить**.

    Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

12. Нажмите на кнопку **ОК**.

Окно параметров области проверки закроется. Настроенные параметры задачи будут сохранены.

Настройка области проверки для задачи проверки по требованию в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить задачу.
3. Выберите раздел **Задачи**.
4. В открывшемся окне двойным щелчком мыши откройте свойства задачи **Проверка по требованию**.
5. Перейдите на закладку **Параметры приложения**.

6. Чтобы добавить элементы списка в область проверки, включите переключатели напротив соответствующих областей проверки.

7. Если вы хотите добавить область проверки, которой нет в списке, то выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне выберите область проверки, отдельный диск, папку или сетевой объект.

   c. Если хотите включать вложенные папки в область проверки, установите флажок **Вложенные папки**.

8. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих элементов списка.

9. Чтобы изменить область проверки, выберите эту область в списке и нажмите на кнопку **Изменить область**.

10. Чтобы скрыть добавленную ранее область проверки из списка сетевых файловых ресурсов, выберите область проверки и нажмите на кнопку **Удалить**.

    Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

11. Нажмите на кнопку **Сохранить**.

Окно параметров области проверки закроется. Настроенные параметры задачи будут сохранены.

Настройка области проверки для задачи проверки по требованию в Консоли приложения

1. В дереве Консоли приложения разверните узел **Проверка по требованию**.

2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.

3. В панели результатов выбранного узла перейдите по ссылке **Настройка области защиты**.

4. Чтобы включить элементы списка в область проверки, в открывшемся окне установите флажки напротив соответствующих областей проверки.

5. Если вы хотите добавить область проверки, которой нет в списке, то выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне выберите область проверки, отдельный диск, папку или сетевой объект.

   c. Если хотите включать вложенные папки в область проверки, установите флажок **Включить вложенные папки**.

6. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих элементов списка.

7. Чтобы изменить область проверки, выберите эту область в списке и нажмите на кнопку **Изменить область**.

8. Чтобы скрыть добавленную ранее область проверки из списка сетевых файловых ресурсов, выберите область проверки и нажмите на кнопку **Удалить**.

   Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

9. Нажмите на кнопку **OK**.

Окно параметров области проверки закроется. Настроенные параметры задачи будут сохранены.

Настройка параметров задачи Проверка по требованию

Настройка параметров задачи Проверка по требованию в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный компьютер.
2. В рабочей области выберите вкладку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. Перейдите в раздел **Задачи**.
5. Двойным щелчком мыши откройте окно свойств задачи **Проверка по требованию**.
6. Выберите раздел **Настройки**.
7. Снимите или установите флажок **Использовать эвристический анализ**.
8. При необходимости измените уровень анализа.
9. Установите флажок **Запускать задачу проверки в фоновом режиме**, если вы хотите присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*.

   По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes, имеют приоритет *Средний*.

10. Установите флажок **Считать выполнение задачи проверкой важных областей**, если вы хотите использовать создаваемую задачу в качестве задачи *Проверка важных областей*.
11. Установите флажок **Не запускать несколько задач проверки одновременно**, чтобы оптимизировать нагрузку на компьютер.
12. Сохраните внесенные изменения.

Настройка параметров задачи Проверка по требованию в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить задачу.

3. Выберите раздел **Задачи**.
4. В открывшемся окне двойным щелчком мыши откройте свойства задачи **Проверка по требованию**.
5. Выберите раздел **Параметры приложения**.
6. Перейдите в раздел **Настройки**.
7. Снимите или установите флажок **Использовать эвристический анализ**.
8. При необходимости в раскрывающемся списке **Уровень эвристического анализа** выберите уровень анализа.
9. Установите флажок **Выполнять только во время простоя компьютера**, если вы хотите присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*.

   По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes, имеют приоритет *Средний*.

10. Установите флажок **Считать выполнение задачи проверкой важных областей**, если вы хотите использовать создаваемую задачу в качестве задачи *Проверка важных областей*.
11. Установите флажок **Не запускать несколько задач проверки одновременно**, чтобы оптимизировать нагрузку на компьютер.
12. Сохраните внесенные изменения.

Настройка параметров задачи Проверка по требованию в Консоли приложения

1. В дереве Консоли приложения разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла нажмите **Свойства**.
4. Перейдите на закладку **Настройки задачи**.
5. Снимите или установите флажок **Использовать эвристический анализ**.
6. При необходимости измените уровень анализа.
7. Установите флажок **Запускать задачу проверки в фоновом режиме**, если вы хотите присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*.

   По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes, имеют приоритет *Средний*.

8. Установите флажок **Считать выполнение задачи проверкой важных областей**, если вы хотите использовать создаваемую задачу в качестве задачи *Проверка важных областей*.

9. Установите флажок **Не запускать несколько задач проверки одновременно**, чтобы оптимизировать нагрузку на компьютер.

10. Сохраните внесенные изменения.

Настройка проверки съемных дисков

Настройка проверки съемных дисков в Консоли администрирования Kaspersky Security Center

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой вы хотите настроить задачу.

3. Выберите вкладку **Политики**.

4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.

   В открывшемся окне свойств политики перейдите в раздел **Дополнительные возможности**.

5. Нажмите на кнопку **Настройка** в подразделе **Проверка съемных дисков**.

   Откроется окно **Проверка съемных дисков**.

6. Выполните следующие действия:

   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes автоматически выполняла проверку съемных дисков при их подключении.

   - Если требуется, установите флажок **Проверять съемный диск, если его размер не превышает (МБ)** и укажите максимальное значение объема данных в поле справа.

   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены.

Настройка проверки съемных дисков в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Дополнительные возможности**.

5. Нажмите на кнопку **Настроить** в блоке **Проверка съемных дисков**.

   Откроется окно **Проверка съемных дисков**.

6. Выполните следующие действия:

   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять съемный диск, если его размер не превышает (МБ)** и укажите максимальное значение объема данных в поле справа.
   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены.

Настройка проверки съемных дисков в Консоли приложения

1. В дереве Консоли приложения откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes** и выберите пункт **Проверка съемных дисков**.

   Откроется окно **Проверка съемных дисков**.

2. Выполните следующие действия:

   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять съемный диск, если его размер не превышает (МБ)** и укажите максимальное значение объема данных в поле справа.
   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.

3. Нажмите на кнопку **OK**.

Выбор стандартных уровней безопасности в задачах проверки по требованию

Для узлов, выбранных в списке файловых ресурсов защищаемого устройства, можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

Выбрать один из стандартных уровней безопасности в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный компьютер.
2. В рабочей области выберите вкладку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.

4. Перейдите в раздел **Задачи**.
5. Двойным щелчком мыши откройте окно свойств задачи **Проверка по требованию**.
6. Выберите раздел **Область проверки**.
7. В списке защищаемых устройств выберите элемент, включенный в область проверки, чтобы задать для него стандартный уровень безопасности.
8. Нажмите на кнопку **Настроить**.
9. В открывшемся окне на вкладке **Уровень безопасности** выберите требуемый уровень безопасности.
10. Нажмите на кнопку **OK**.
11. В окне **Свойства: Проверка по требованию** нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Выбрать один из стандартных уровней безопасности в Консоли приложения

1. В дереве Консоли приложения разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла нажмите **Настройка области защиты**.
4. В списке сетевых файловых ресурсов защищаемого устройства выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
5. Убедитесь, что выбранный узел или элемент включен в область проверки.
6. Нажмите на кнопку **Настроить**.
7. В открывшемся окне выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.
8. Нажмите на кнопку **OK**.

Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого устройства.

Настройка параметров безопасности вручную в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный компьютер.
2. В рабочей области выберите вкладку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. Перейдите в раздел **Задачи**.
5. Двойным щелчком мыши откройте окно свойств задачи **Проверка по требованию**.
6. Выберите раздел **Область проверки**.
7. В списке защищаемых устройств выберите элемент, включенный в область проверки, чтобы настроить параметры безопасности.
8. Нажмите на кнопку **Настроить**.
9. В открывшемся окне на закладке **Уровень безопасности** выберите требуемый уровень безопасности.
10. Выберите ресурс, параметры безопасности которого вы хотите настроить.
11. Нажмите на кнопку **Настроить**.
12. В открывшемся окне выберите требуемый уровень безопасности и нажмите на кнопку **Настройка**.
13. На закладке **Общие** укажите следующие настройки:
    - Объекты, которые требуется включить в область защиты:
      - **Все объекты**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты.
      - **Объекты, проверяемые по формату**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании формата файла. Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
      - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
      - **Объекты, проверяемые по указанному списку расширений**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений задается пользователем вручную.
    - В блоке **Оптимизация** установите или снимите флажок **Защита только новых и измененных файлов**.

- В блоке **Проверка составных файлов** укажите составные объекты, которые вы хотите включить в область проверки:
  - **Проверять архивы**
  - **Проверять дистрибутивы**
  - **Проверять файлы офисных форматов**
  - **Проверять файлы почтовых форматов**

14. На закладке **Действия** укажите следующие настройки:

- Выберите действие над зараженными и другими обнаруживаемыми объектами:
  - **Лечить**
  - **Лечить. Удалять, если не удалось вылечить**
  - **Удалять**
  - **Рекомендуемое**
  - **Информировать**
- Настройте действия над объектами в зависимости от типа обнаруженного объекта:
  a. Снимите или установите флажок **Применять действие к выбранным типам объектов**.
  b. Нажмите на кнопку **Настройка** и выберите типы обнаруживаемых объектов.
- Настройте действия над составными файлами, недоступными для изменения: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением**.

15. На закладке **Оптимизация** укажите следующие настройки:

- В блоке **Исключения**:
  - Снимите или установите флажок **Исключать файлы**.
  - Снимите или установите флажок **Не проверять объекты по типу**.
    Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
- В блоке **Расширенные настройки**:
  - **Останавливать проверку, если она длится более (сек.)**
  - **Не проверять составные объекты размером более (МБ)**
  - **Использовать технологию iSwift**
  - **Использовать технологию iChecker**

16. Сохраните новые параметры безопасности.

Настройка параметров безопасности вручную в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить задачу.
3. Выберите раздел **Задачи**.
4. В открывшемся окне двойным щелчком мыши откройте свойства задачи **Проверка по требованию**.
5. Выберите раздел **Параметры приложения**.
6. Перейдите в раздел **Область проверки**.
7. В списке сетевых файловых ресурсов защищаемого устройства выберите элемент, для которого вы хотите настроить параметры безопасности. Убедитесь, что выбранный элемент включен в область проверки.
8. Нажмите на кнопку **Изменить**.
9. Укажите режим защиты объектов в раскрывающемся списке:
   - **Все объекты**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты.
   - **Объекты, проверяемые по формату**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании формата файла. Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
   - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
   - **Объекты, проверяемые по указанному списку расширений**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений задается пользователем вручную.
10. Установите или снимите флажок **Защита только новых и измененных файлов** и укажите, нужно ли включать в проверку Вложенные папки.
11. Укажите настройки защиты составных объектов:
    - **Проверять архивы**
    - **Проверять дистрибутивы**
    - **Проверять файлы офисных форматов**
    - **Проверять файлы почтовых форматов**

12. Выберите действие над зараженными и другими обнаруживаемыми объектами:

    - **Лечить**
    - **Лечить. Удалять, если не удалось вылечить**
    - **Удалять**
    - **Рекомендуемое**
    - **Информировать**

13. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

    a. Снимите или установите флажок **Применять действие к выбранным типам объектов**.

    b. Нажмите на кнопку **Настройка** и выберите типы обнаруживаемых объектов.

14. Настройте действия над составными файлами, недоступными для изменения: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением**.

15. В блоке **Исключения**:

    - Снимите или установите флажок **Исключать файлы**.
    - Снимите или установите флажок **Не проверять объекты по типу**.

16. В блоке **Добавление ключа**:

    - **Останавливать проверку, если она длится более (сек.)**
    - **Не проверять составные объекты размером более (МБ)**
    - **Использовать технологию iSwift**
    - **Использовать технологию iChecker**

17. Сохраните новые параметры безопасности.

Настройка параметров безопасности вручную в Консоли приложения

1. В дереве Консоли приложения разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла нажмите **Настройка области защиты**.
4. В списке сетевых файловых ресурсов защищаемого устройства выберите элемент, для которого вы хотите настроить параметры безопасности.
5. Убедитесь, что выбранный элемент включен в область проверки.
6. Нажмите на кнопку **Настроить**.

7. В открывшемся окне выберите требуемый уровень безопасности и нажмите на кнопку **Настройка**.

8. На закладке **Общие** укажите следующие настройки:

- Объекты, которые требуется включить в область защиты:
  - **Все объекты**. Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты.
  - **Объекты, проверяемые по формату**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании формата файла. Список форматов составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
  - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
  - **Объекты, проверяемые по указанному списку расширений**. Kaspersky Industrial CyberSecurity for Nodes проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений задается пользователем вручную.
- В блоке **Оптимизация** установите или снимите флажок **Защита только новых и измененных файлов**.
- В блоке **Проверка составных файлов** укажите составные объекты, которые вы хотите включить в область проверки:
  - **Проверять архивы**;
  - **Проверять дистрибутивы**;
  - **Проверять файлы офисных форматов**;
  - **Проверять файлы почтовых форматов**.

9. На закладке **Действия** укажите следующие настройки:

- Выберите действие над зараженными и другими обнаруживаемыми объектами:
  - **Лечить**;
  - **Лечить. Удалять, если не удалось вылечить**;
  - **Удалять**;
  - **Рекомендуемое**;
  - **Информировать**.

- Настройте действия над объектами в зависимости от типа обнаруженного объекта:

  a. Снимите или установите флажок **Применять действие к выбранным типам объектов**.

  b. Нажмите на кнопку **Настройка** и выберите типы обнаруживаемых объектов.

- Настройте действия над составными файлами, недоступными для изменения: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением**.

10. На закладке **Оптимизация** укажите следующие настройки:

    - В блоке **Исключения**:

      - Снимите или установите флажок **Исключать файлы**.

      - Снимите или установите флажок **Не проверять объекты по типу**.

      Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

    - В блоке **Расширенные настройки**:

      - **Останавливать проверку, если она длится более (сек.)**;

      - **Не проверять составные объекты размером более (МБ)**;

      - **Использовать технологию iSwift**;

      - **Использовать технологию iChecker**.

11. Сохраните новые параметры безопасности.

Статистика задач проверки по требованию

Пока выполняется задача *Проверка по требованию*, вы можете просматривать информацию о количестве объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes обработала с момента запуска задачи.

Эта информация будет доступна, даже если вы приостановите задачу. Вы можете просмотреть статистику задачи в журнале выполнения задачи.

Чтобы просмотреть статистику задачи Проверка по требованию, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Проверка по требованию**.

2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

В панели результатов выбранного узла в разделе **Статистика** отобразится статистика выполнения задачи.

В таблице ниже приведена информация об объектах, которые программа Kaspersky Industrial CyberSecurity for Nodes обработала с момента запуска задачи.

Статистика задач проверки по требованию

Поле	Описание
Обнаружено	Количество объектов, которые обнаружило приложение Kaspersky Industrial CyberSecurity for Nodes. Например, если приложение Kaspersky Industrial CyberSecurity for Nodes обнаружило один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу.
Зараженных и других обнаруживаемых объектов	Количество объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes обнаружило и признало зараженными, или количество обнаруженных объектов, которые не были исключены из области проверки и были определены как легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным.
Не вылечено объектов	Количество объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes не вылечило по следующим причинам: • Тип обнаруженного объекта не предполагает лечения. • При лечении возникла ошибка.
Вылечено объектов	Количество объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes вылечило.
Удалено объектов	Количество объектов, которые приложению Kaspersky Industrial CyberSecurity for Nodes удалось удалить.
Не проверено объектов	Количество объектов в области защиты, которые приложению Kaspersky Industrial CyberSecurity for Nodes не удалось проверить, например, если доступ к объекту был заблокирован другой программой.
Архивов	Количество архивов, проверенных приложением Kaspersky Industrial CyberSecurity for Nodes.
Упакованных объектов	Количество упакованных объектов, проверенных приложением Kaspersky Industrial CyberSecurity for Nodes.
Защищенных паролем объектов	Количество объектов (например, архивов), которые приложение Kaspersky Industrial CyberSecurity for Nodes пропустила, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes пропустило, так как их формат искажен.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Не удалено объектов	Количество объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes не смогло удалить, например, если доступ к объекту был заблокирован другой программой.
Не обработанных объектов	Общее количество объектов, которые не обработало приложение Kaspersky Industrial CyberSecurity for Nodes.

Вы также можете посмотреть статистику задачи проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в разделе **Управление** панели результатов.

По завершении выполнения задачи рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Защита промышленной сети

В этом разделе описаны задачи получения данных и проверки целостности проектов программируемых логических контроллеров (далее также "проектов ПЛК").

О проверке целостности проектов ПЛК

Функция предназначена для проверки целостности проектов ПЛК, используемых в промышленной сети.

Проект ПЛК – микропрограмма, написанная для ПЛК. Проект ПЛК хранится в памяти ПЛК и выполняется в рамках технологического процесса, использующего ПЛК.

Для проверки целостности проектов ПЛК требуется сетевой доступ к ПЛК со стороны защищаемого устройства с установленным приложением Kaspersky Industrial CyberSecurity for Nodes.

Перед началом использования функции требуется выполнить следующие подготовительные действия:

1. Получить информацию о проектах ПЛК с помощью локальной задачи Консоли приложения **Получение данных о проектах ПЛК**.

2. В параметрах локальной задачи Консоли приложения **Проверка целостности проектов ПЛК** указать эталонные проекты ПЛК из списка проектов, полученных на предыдущем шаге.

Чтобы посмотреть информацию о проектах ПЛК в задаче Проверка целостности проектов ПЛК,

откройте окно **Взаимодействие с Сервером администрирования** в свойствах политики и настройте передачу данных на Сервер администрирования, установив флажок **Версии проектов ПЛК**.

После запуска локальной задачи *Проверка целостности проектов ПЛК* приложение выводит предупреждения в случае изменения проектов ПЛК в сравнении с эталонными проектами ПЛК.

По умолчанию Проверка целостности проектов ПЛК выключена.

Отчеты

Отчетность входит в число базовых функций Сервера администрирования Kaspersky Security Center. Воспользоваться этой функцией можно только через Консоль администрирования Kaspersky Security Center.

После успешного завершения задачи *Проверка целостности проектов ПЛК* вы можете создать и просмотреть отчет со следующей информацией:

- имя компьютера, на котором завершена задача *Проверка целостности проектов ПЛК*;

- ПЛК, целостность которых контролируется;

- дата последней проверки;
- результаты проверки целостности.

Чтобы создать отчет на Сервере администрирования Kaspersky Security Center,

откройте вкладку **Отчеты** и выберите **Отчет о проверке целостности программируемых логических контроллеров (ПЛК)**.

Подробнее о создании отчетов см. в справке Kaspersky Security Center.

Настройка задачи Проверка целостности проектов ПЛК

В этом разделе приведены инструкции по настройке общих параметров задач по контролю проектов ПЛК.

Настройка получения данных о проектах ПЛК

Перед проверкой целостности проектов ПЛК необходимо получить информацию о проектах ПЛК, которые используются в промышленной сети в настоящее время. Получение информации выполняется с помощью локальной задачи *Получение данных о проектах ПЛК*.

Настройка получения данных о проектах ПЛК в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
2. В рабочей области выберите закладку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. Перейдите в раздел **Задачи**.
5. В открывшемся окне выберите задачу **Получение данных о проектах ПЛК** и нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Получение данных о проектах ПЛК**.
6. Перейдите в раздел **Настройки** и на закладке **Настройки задачи** нажмите на кнопку **Добавить из Реестра ПЛК**.

   Откроется окно **Реестр конфигураций ПЛК 5.0.0**.
7. Нажмите на кнопку **Добавить**.
8. В блоке **Общие настройки** укажите название конфигурации ПЛК и в раскрывающемся списке **Тип ПЛК** выберите тип ПЛК.

   Тип ПЛК представляет собой модель и серию конкретного изготовителя ПЛК.

9. В поле **Описание** введите описание ПЛК.

   Приложение привязывает заданное описание к каждой новой версии проекта ПЛК, полученной в ходе выполнения задачи *Получение данных о проектах ПЛК*.

10. В поле **Ожидать соединения** укажите время ожидания в секундах.

11. В блоке **Настройки соединения**, в зависимости от выбранного типа ПЛК, заполните поля **IP-адрес**, **Порт**, **Стойка, Порт для Telnet, Виртуальный адрес контроллера** и **Слот**.

12. Если необходимо защитить соединения с ПЛК, в зависимости от выбранного типа ПЛК, выберите способ аутентификации:

    - **Пароль**.

      Если флажок установлен, приложение использует указанный пароль при подключении к ПЛК для его опроса.

      Если флажок снят, приложение подключается к ПЛК без использования пароля. По умолчанию флажок снят.

      > Флажок не задает новый пароль для подключения к ПЛК. Установка пароля выполняется на стороне ПЛК.

    - **Использовать аутентификацию на контроллере**.

13. Установите или снимите флажок **Читать блоки данных**.

    Если флажок установлен, приложение учитывает блоки данных при расчете контрольной суммы проекта ПЛК. Рекомендуется установить флажок, если в блоке данных содержатся только статические величины, чтобы повысить уровень безопасности проверки.

    Если флажок снят, приложение не учитывает блоки данных. Рекомендуется не устанавливать флажок, если в блоке данных содержатся динамические величины, чтобы избежать ложных срабатываний задачи *Проверка целостности проектов ПЛК* при сравнении выбранного проекта ПЛК с эталонным.

    По умолчанию флажок снят.

14. Нажмите на кнопку **OK**.

    > Резервные контроллеры не поддерживаются.

    Добавленные конфигурации ПЛК отобразятся на закладке **Настройки задачи**.

15. Чтобы добавить конфигурацию ПЛК, полученную после завершения задачи *Получение данных о проектах ПЛК* на локальном компьютере с Консолью Kaspersky Industrial CyberSecurity for Nodes:

    a. В списке конфигураций ПЛК выберите ту, которую хотите добавить в Реестр ПЛК.

    b. Нажмите на кнопку **Привязать к Реестру ПЛК**.

    > У каждой конфигурации ПЛК из реестра есть уникальный идентификационный номер, указанный в последнем столбце. После добавления конфигурации ПЛК из задачи на локальном компьютере в Реестр ПЛК этой конфигурации присваивается идентификационный номер.

16. Нажмите на кнопку **Удалить**, если вы хотите удалить выбранную конфигурацию ПЛК из списка задачи.

    Конфигурация ПЛК не удаляется из реестра ПЛК, и ее можно добавить снова в любой момент.

17. Сохраните внесенные изменения.

Информация, полученная в результате выполнения задачи *Получение данных о проектах ПЛК*, используется для выбора эталонных проектов ПЛК и настройки задачи *Проверка целостности проектов ПЛК*.

Настройка получения данных о проектах ПЛК в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить задачу *Получение данных о проектах ПЛК*.
3. Выберите закладку **Задачи**.
4. В открывшемся окне двойным щелчком мыши откройте свойства задачи **Получение данных о проектах ПЛК**.
5. Перейдите на вкладку **Параметры приложения** и нажмите на кнопку **Добавить из Реестра ПЛК**.

   Откроется окно **Конфигурация ПЛК**.
6. В разделе **Настройки контроллеров** в раскрывающемся списке **Тип контроллера** выберите тип ПЛК.

   Тип ПЛК представляет собой модель и серию конкретного изготовителя ПЛК.
7. В поле **Описание** введите описание ПЛК.

   Приложение привязывает заданное описание к каждой новой версии проекта ПЛК, полученной в ходе выполнения задачи *Получение данных о проектах ПЛК*.
8. В поле **Ожидание подключения, сек** укажите время ожидания в секундах.
9. В разделе **Настройки подключения**, в зависимости от выбранного типа ПЛК, заполните поля **Адрес контроллера**, **Порт**, **Стойка, Порт для Telnet, Виртуальный адрес контроллера** и **Слот**.
10. Если необходимо защитить соединения с ПЛК, в зависимости от выбранного типа ПЛК, выберите способ аутентификации:

    - **Использовать пароль**.

      Если флажок установлен, приложение использует указанный пароль при подключении к ПЛК для его опроса.

      Если флажок снят, приложение подключается к ПЛК без использования пароля. По умолчанию флажок снят.

      Флажок не задает новый пароль для подключения к ПЛК. Установка пароля выполняется на стороне ПЛК.

    - **Использовать аутентификацию на контроллере**.
11. Установите или снимите флажок **Читать блоки данных**.

Если флажок установлен, приложение учитывает блоки данных при расчете контрольной суммы проекта ПЛК. Рекомендуется установить флажок, если в блоке данных содержатся только статические величины, чтобы повысить уровень безопасности проверки.

Если флажок снят, приложение не учитывает блоки данных. Рекомендуется не устанавливать флажок, если в блоке данных содержатся динамические величины, чтобы избежать ложных срабатываний задачи *Проверка целостности проектов ПЛК* при сравнении выбранного проекта ПЛК с эталонным.

По умолчанию флажок снят.

12. Нажмите на кнопку **ОК**.

    Резервные контроллеры не поддерживаются.

    Добавленные конфигурации ПЛК отобразятся на закладке **Параметры приложения**.

13. Чтобы добавить конфигурацию ПЛК, полученную после завершения задачи *Получение данных о проектах ПЛК* на локальном компьютере с Консолью Kaspersky Industrial CyberSecurity for Nodes:

    a. В списке конфигураций ПЛК выберите ту, которую хотите добавить в Реестр ПЛК.

    b. Нажмите на кнопку **Привязать к Реестру ПЛК**.

    У каждой конфигурации ПЛК из реестра есть уникальный идентификационный номер, указанный в последнем столбце. После добавления конфигурации ПЛК из задачи на локальном компьютере в Реестр ПЛК этой конфигурации присваивается идентификационный номер.

14. Нажмите на кнопку **Удалить**, если вы хотите удалить выбранную конфигурацию ПЛК из списка задачи.

    Конфигурация ПЛК не удаляется из реестра ПЛК, и ее можно добавить снова в любой момент.

15. Сохраните внесенные изменения.

Настройка получения данных о проектах ПЛК в Консоли приложения

1. В дереве Консоли приложения разверните узел **Защита промышленной сети**.
2. Выберите вложенный узел **Получение данных о проектах ПЛК**.
3. Перейдите по ссылке **Свойства** в панели результатов узла **Получение данных о проектах ПЛК**.

   Откроется окно **Свойства: Получение данных о проектах ПЛК**.
4. На закладке **Настройки задачи** нажмите на кнопку **Добавить**.

   Откроется окно **Конфигурация ПЛК**.
5. В блоке **Общие настройки** в раскрывающемся списке **Тип ПЛК** выберите тип ПЛК.

   Тип ПЛК представляет собой модель и серию конкретного изготовителя ПЛК.
6. В поле **Описание** введите описание ПЛК.

   Приложение привязывает заданное описание к каждой новой версии проекта ПЛК, полученной в ходе выполнения задачи *Получение данных о проектах ПЛК*.

7. В поле **Ожидать соединения** укажите время ожидания в секундах.

8. В блоке **Настройки соединения**, в зависимости от выбранного типа ПЛК, заполните поля **IP-адрес**, **Порт**, **Стойка, Порт для Telnet, Виртуальный адрес контроллера** и **Слот**.

9. Если необходимо защитить соединения с ПЛК, в зависимости от выбранного типа ПЛК, выберите способ аутентификации:

   - **Пароль**.

     Если флажок установлен, приложение использует указанный пароль при подключении к ПЛК для его опроса.

     Если флажок снят, приложение подключается к ПЛК без использования пароля. По умолчанию флажок снят.

     > Флажок не задает новый пароль для подключения к ПЛК. Установка пароля выполняется на стороне ПЛК.

   - **Использовать аутентификацию на контроллере**.

10. Установите или снимите флажок **Читать блоки данных**.

    Если флажок установлен, приложение учитывает блоки данных при расчете контрольной суммы проекта ПЛК. Рекомендуется установить флажок, если в блоке данных содержатся только статические величины, чтобы повысить уровень безопасности проверки.

    Если флажок снят, приложение не учитывает блоки данных. Рекомендуется не устанавливать флажок, если в блоке данных содержатся динамические величины, чтобы избежать ложных срабатываний задачи *Проверка целостности проектов ПЛК* при сравнении выбранного проекта ПЛК с эталонным.

    По умолчанию флажок снят.

11. Нажмите на кнопку **ОК**.

    > Резервные контроллеры не поддерживаются.

    Добавленные конфигурации ПЛК отобразятся на закладке **Настройки задачи**.

12. Нажмите на кнопку **Удалить**, если вы хотите удалить выбранную конфигурацию ПЛК из списка задачи.

    > Конфигурация ПЛК не удаляется из реестра ПЛК, и ее можно добавить снова в любой момент.

13. Сохраните внесенные изменения.

Информация, полученная в результате выполнения задачи *Получение данных о проектах ПЛК*, используется для выбора эталонных проектов ПЛК и настройки задачи *Проверка целостности проектов ПЛК*.

Настройка проверки целостности проектов ПЛК

Настройка проверки целостности проектов ПЛК в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
2. В рабочей области выберите закладку **Устройства**.
3. Откройте свойства компьютера двойным щелчком мыши.
4. Перейдите в раздел **Задачи**.
5. В открывшемся окне выберите задачу **Проверка целостности проектов ПЛК** и нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Проверка целостности проектов ПЛК**.
6. Перейдите в раздел **Настройки**.
7. В открывшемся окне нажмите на кнопку **Добавить**, чтобы добавить в список конфигурации, для которых будет выполняться задача *Проверка целостности проектов ПЛК*.

   Откроется окно **Данные для проверки целостности проекта ПЛК**.

   Все данные в этом окне получены в результате выполнения задачи Kaspersky Security Center *Получение данных о проектах ПЛК*.
8. В раскрывающемся списке **Тип контроллера** выберите тип ПЛК, целостность проекта которого вы хотите проверить.
9. Выберите из списка конфигурацию для выбранного типа ПЛК и укажите эталонную версию для проекта ПЛК. По результатам сравнения с параметрами эталонного проекта ПЛК приложение делает вывод о целостности проекта ПЛК
10. В окне **Данные для проверки целостности проекта ПЛК** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения. Данные проекта ПЛК будут добавлены в задачу.
11. Выберите добавленную конфигурацию ПЛК из списка в окне **Свойства: Проверка целостности проектов ПЛК**.

    - На закладке **Конфигурация ПЛК** отображается информация о хеше проекта ПЛК и дате, когда он был получен.
    - На закладке **Эталонная версия проекта ПЛК** содержится подробная информация о конфигурации ПЛК.
12. Сохраните внесенные изменения.

Настройка проверки целостности проектов ПЛК в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить задачу *Проверка целостности проектов ПЛК*.
3. Выберите раздел **Задачи**.

4. В открывшемся окне двойным щелчком мыши откройте свойства задачи **Проверка целостности проектов ПЛК**.

5. Перейдите на закладку **Параметры приложения** и нажмите на кнопку **Добавить**.

   Откроется окно **Данные для проверки целостности проекта ПЛК**.

   Все данные в этом окне получены в результате выполнения задачи Kaspersky Security Center *Получение данных о проектах ПЛК*.

6. Нажмите на кнопку **Выбрать конфигурацию ПЛК**, чтобы выбрать конфигурацию ПЛК.

7. Укажите промежуток времени, через который приложение запрашивает информацию о параметрах проектов ПЛК.

8. Нажмите на кнопку **Выбрать эталонный проект ПЛК** и укажите эталонную версию для проекта ПЛК. По результатам сравнения с параметрами эталонного проекта ПЛК приложение делает вывод о целостности проекта ПЛК

9. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

10. Выберите добавленную конфигурацию ПЛК из списка.

11. Сохраните внесенные изменения.

Настройка проверки целостности проектов ПЛК в Консоли приложения

1. В дереве Консоли приложения разверните узел **Защита промышленной сети**.

2. Выберите вложенный узел **Проверка целостности проектов ПЛК**.

3. Перейдите по ссылке **Свойства** в панели результатов узла **Проверка целостности проектов ПЛК**.

   Откроется окно **Расписание и режим запуска**.

4. В открывшемся окне настройте следующие параметры:

   - Укажите настройки расписания задачи.

   - При необходимости включите функцию **Запускать задачу с правами пользователя** и укажите имя и пароль пользователя, учетную запись которого вы хотите использовать для запуска задачи.

5. В панели результатов узла **Проверка целостности проектов ПЛК** перейдите по ссылке **Настройка области защиты**.

6. В открывшемся окне нажмите на кнопку **Добавить**, чтобы добавить в список конфигурации, для которых будет выполняться задача *Проверка целостности проектов ПЛК*.

   Откроется окно **Данные для проверки целостности проекта ПЛК**. Все данные в этом окне получены в результате выполнения задачи Kaspersky Security Center *Получение данных о проектах ПЛК*.

7. В раскрывающемся списке **Тип контроллера** выберите тип ПЛК, целостность проекта которого вы хотите проверить.

8. Выберите из списка конфигурацию для выбранного типа ПЛК и укажите эталонную версию для проекта ПЛК. По результатам сравнения с параметрами эталонного проекта ПЛК приложение делает вывод о целостности проекта ПЛК

9. В окне **Данные для проверки целостности проекта ПЛК** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения. Данные проекта ПЛК будут добавлены в задачу.

10. Выберите добавленную конфигурацию ПЛК из списка в окне **Свойства: Проверка целостности проектов ПЛК**.

    - На закладке **Конфигурация ПЛК** отображается информация о хеше проекта ПЛК и дате, когда он был получен.

    - На закладке **Эталонная версия проекта ПЛК** содержится подробная информация о конфигурации ПЛК.

11. Сохраните внесенные изменения.

Включение и выключение проверки целостности проектов ПЛК

Задача *Проверка целостности проектов ПЛК* выполняется только после того, как Kaspersky Industrial CyberSecurity for Nodes получит информацию с помощью задачи *Получение данных о проектах ПЛК*.

Включение или выключение проверки целостности проектов ПЛК в Консоли администрирования Kaspersky Security Center

1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.

2. В рабочей области выберите закладку **Устройства**.

3. Откройте свойства компьютера двойным щелчком мыши.

4. Перейдите в раздел **Задачи**.

5. В открывшемся окне выберите задачу **Получение данных о проектах ПЛК** и выполните одно из следующих действий:

    - Чтобы включить проверку целостности проектов ПЛК, в контекстном меню задачи выберите **Запустить**.

      Задача *Проверка целостности проектов ПЛК* будет запущена.

    - Чтобы выключить проверку целостности проектов ПЛК, в контекстном меню задачи выберите **Остановить**.

      Задача *Проверка целостности проектов ПЛК* будет остановлена.

Включение или выключение проверки целостности проектов ПЛК в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

2. Нажмите на имя компьютера, на котором вы хотите настроить задачу *Проверка целостности проектов ПЛК*.

3. Выберите закладку **Задачи**.

4. Установите флажок напротив задачи **Получение данных о проектах ПЛК** и выполните одно из следующих действий:

   - Чтобы включить проверку целостности проектов ПЛК, нажмите на кнопку **Запустить**.

     Задача *Проверка целостности проектов ПЛК* будет запущена.

   - Чтобы выключить проверку целостности проектов ПЛК, нажмите на кнопку **Остановить**.

     Задача *Проверка целостности проектов ПЛК* будет остановлена.

Включение или выключение проверки целостности проектов ПЛК в Консоли приложения

1. В дереве Консоли приложения разверните узел **Защита промышленной сети**.
2. Выберите вложенный узел **Получение данных о проектах ПЛК**.
3. В разделе **Управление** в панели результатов узла **Получение данных о проектах ПЛК** перейдите по ссылке **Запустить**.
4. Выберите вложенный узел **Проверка целостности проектов ПЛК**.
5. В разделе **Управление** в панели результатов узла **Проверка целостности проектов ПЛК** выполните одно из следующих действий:

   - Чтобы включить проверку целостности проектов ПЛК, перейдите по ссылке **Запустить**.

     Задача *Проверка целостности проектов ПЛК* будет запущена.

   - Чтобы выключить проверку целостности проектов ПЛК, перейдите по ссылке **Остановить**.

     Задача *Проверка целостности проектов ПЛК* будет остановлена.

О реестре конфигураций ПЛК

Реестр конфигураций ПЛК (далее также Реестр) это единый список всех конфигураций ПЛК, которые используются приложением Kaspersky Industrial CyberSecurity for Nodes. *Конфигурация ПЛК* – это совокупность частных параметров ПЛК, которые вы можете указать в настройках (IP-адрес, номер слота, модель и т.д.). Вы можете добавлять, изменять и удалять конфигурации ПЛК через реестр.

В Kaspersky Industrial CyberSecurity for Nodes версии 4.5 порядок расчета хеша конфигурации для ПЛК типа Siemens SIMATIC S7-300 / 400 / 400H изменился. Поэтому после обновления версии приложения вам нужно перезапустить задачу *Получение данных о проектах ПЛК*, чтобы создать новые эталонные версии для этих проектов ПЛК.

Реестр конфигураций ПЛК может быть наполнен вручную или с помощью импорта конфигурационного файла, содержащего данные о конфигурациях ПЛК.

Список конфигураций ПЛК в реестре используется для формирования области защиты задачи *Проверка целостности проектов ПЛК*, настраиваемой через Консоль администрирования Kaspersky Security Center. Во время наполнения списка конфигураций задачи *Получение данных о проектах ПЛК* вы можете добавлять и удалять конфигурации ПЛК в реестре. При удалении конфигурации ПЛК из списка задач, эта конфигурация не удаляется из реестра.

Каждая конфигурация ПЛК, добавленная в реестр, имеет уникальный идентификационный номер. При внесении изменений в конфигурацию ПЛК, идентификационный номер изменяется. Конфигурации ПЛК, добавленные через задачу *Получение данных о проектах ПЛК* в локальной Консоли Kaspersky Industrial CyberSecurity for Nodes не имеют идентификационных номеров. Такие конфигурации ПЛК можно добавить в реестр вручную при создании области защиты в задаче *Получение данных о проектах ПЛК* в Kaspersky Security Center.

Список конфигураций ПЛК в задаче *Получение данных о проектах ПЛК* в Kaspersky Security Center формируется из двух источников:

- Конфигурации ПЛК без идентификационных номеров, добавленные в список локальной задачи в Консоли приложения (список синхронизируется автоматически).
- Конфигурации ПЛК с идентификационными номерами, добавленные администратором из реестра конфигураций ПЛК.

Если конфигурация ПЛК, добавленная в список задачи *Получение данных о проектах ПЛК*, удалена из Реестра, Kaspersky Industrial CyberSecurity for Nodes уведомляет вас о том, что результаты проверки целостности будут искажены. Перезапустите задачу *Получение данных о проектах ПЛК*, убедившись, что все конфигурации ПЛК в списке задачи в Kaspersky Security Center существуют в реестре.

Настройка реестра ПЛК

Чтобы настроить реестр ПЛК:

1. Откройте окно **Реестр конфигураций ПЛК** одним из следующих способов:

   - **Из параметров локальной задачи Получение данных о проектах ПЛК**

     1. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
     2. В рабочей области выберите закладку **Устройства**.
     3. Откройте свойства компьютера двойным щелчком мыши.
     4. Перейдите в раздел **Задачи**.
     5. В открывшемся окне выберите задачу **Получение данных о проектах ПЛК** и нажмите на кнопку **Свойства**.

        Откроется окно **Свойства: Получение данных о проектах ПЛК**.

     6. Перейдите в раздел **Настройки** и на вкладке **Настройки задачи** нажмите на кнопку **Добавить из Реестра ПЛК**.

        Откроется окно **Реестр конфигураций ПЛК 5.0.0**.

   - **Из папки Оборудование Консоли администрирования Kaspersky Security Center**

     a. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Сервер администрирования <имя сервера>**.

     b. Разверните узел **Дополнительно**.

c. В папке **Хранилища** выберите вложенную папку **Оборудование**.

> Если папка **Оборудование** не отображается, в параметрах интерфейса Сервера администрирования установите флажок **Отображать Системное администрирование**.

d. В рабочей области папки **Оборудование** в контекстном меню кнопки **Дополнительные действия** выберите **Реестр конфигураций ПЛК 5.0.0**.

Откроется окно **Реестр конфигураций ПЛК 5.0.0**.

2. Добавьте вручную необходимые конфигурации ПЛК.

3. Если необходимо, **импортируйте данные о конфигурациях проектов ПЛК из XML-файла**.

a. Нажмите на кнопку **Импорт**.

Откроется стандартное окно Microsoft Windows **Открыть файл**.

b. Укажите путь к XML-файлу с параметрами ПЛК.

c. Нажмите на кнопку **Открыть**.

Новые записи с данными о конфигурациях ПЛК отобразятся в списке в окне **Реестр конфигураций ПЛК**.

4. Если необходимо, **экспортируйте данные о конфигурациях проектов ПЛК в XML-файл**.

a. Нажмите на кнопку **Экспорт**.

b. В открывшемся окне укажите путь и имя XML-файла, в который вы хотите экспортировать данные о конфигурациях проектов ПЛК.

c. Нажмите на кнопку **Сохранить**.

5. Для изменения параметров конфигурации ПЛК, нажмите на кнопку **Изменить**.

Изменение конфигурации ПЛК в реестре ПЛК влияет на результаты задачи *Проверка целостности проектов ПЛК*. Вам потребуется запустить задачу *Получение данных о проектах ПЛК*, чтобы получить обновленные данные, и затем снова запустить задачу *Проверка целостности проектов ПЛК*, чтобы получить актуальные результаты.

1. Нажмите на кнопку **Удалить**, если конфигурация проектов ПЛК больше не используется.

> После удаления из реестра ПЛК проект ПЛК становится недоступным для получения данных и проверки целостности.

2. Используйте поле **Фильтр**, чтобы найти конфигурации ПЛК с требуемыми значениями.

3. Если необходимо, установите флажок **Показывать только конфигурации ПЛК, доступные для управления с помощью Kaspersky Industrial CyberSecurity for Nodes**.

4. Нажмите на кнопку **Закрыть**.

Реестр ПЛК будет сохранен.

Аудит безопасности

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

Задача аудита безопасности – это групповая и локальная задача поиска уязвимостей на устройствах и оценки соответствия устройств стандартам операционных систем. Для выполнения задачи аудита безопасности Kaspersky Industrial CyberSecurity for Nodes использует поставляемые с продуктом или пользовательские базы правил, помещенные в XML-файлы:

- Для поиска уязвимостей на устройствах программа использует правила, написанные на языке OVAL.
- Для оценки безопасности устройств и соответствия стандартам для операционных систем программа использует конфигурации правил, написанные на языках OVAL и XCCDF.

Правила аудита безопасности разделяются на классы:

- Compliance – проверяют конфигурационные настройки системы на соответствие политике безопасности.
- Inventory – проверяют, присутствует ли в системе указанное в правилах программное или аппаратное обеспечение.
- Miscellaneous – содержат пользовательские проверки.
- Patch – проверяют, установлены ли в системе указанные в правилах патчи.
- Vulnerability – проверяют, присутствуют ли в системе указанные в правилах уязвимости.

Ограничения для параметров задачи аудита безопасности

При создании и настройке задачи аудита безопасности учитывайте следующие ограничения:

- Совокупное ограничение в 2 МБ на совокупный размер файлов, использующихся при выборе источника **Пользовательская база правил из файла**.
- Ограничение на размер отчета о результатах выполнения задачи аудита безопасности – 7,5 МБ.

Поддерживаемые типы OVAL-проверок

Для выполнения задачи аудита безопасности поддерживаются следующие типы OVAL-проверок:

- accesstoken;
- auditeventpolicy;

- auditeventpolicysubcategories;
- cmdlet – доступно для Windows Vista/Server 2008 и выше;
- environmentvariable58;
- environmentvariable;
- family;
- file;
- fileauditedpermissions53;
- filehash58;
- filehash;
- group_sid;
- interface;
- lockoutpolicy;
- passwordpolicy;
- port;
- process58;
- process;
- registry;
- rpmverifyfile;
- service;
- sid;
- textfilecontent54;
- user;
- user_sid;
- variable;
- wmi57;
- wmi;
- xmlfilecontent.

Для неподдерживаемых типов OVAL-проверок в отчете о результатах выполнения задачи аудита безопасности будут отображаться ошибки.

Управление задачами аудита безопасности

Запуск задачи доступен только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионным объектом ICS Audit.

Задачи аудита безопасности – это локальные или групповые задачи, которые создаются и настраиваются через Web Console или через интерфейс командной строки. Эти задачи используются для поиска уязвимостей и оценки соответствия производственных систем стандартам безопасности.

В этом разделе приведены инструкции по управлению задачами аудита безопасности.

Создание и настройка задачи аудита безопасности с параметрами по умолчанию

Чтобы создать и настроить задачу аудита безопасности с параметрами по умолчанию:

1. В главном окне Web Console Kaspersky Security Center перейдите в раздел **Управление активами** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Приложение** выберите Kaspersky Industrial CyberSecurity for Nodes.
4. В раскрывающемся списке **Тип задачи** выберите **Аудит безопасности**.
5. Введите название задачи или оставьте название по умолчанию.
6. Выберите устройства, для которых будет назначена задача.
7. Нажмите на кнопку **Далее**.
8. В окне **Выбор учетной записи для запуска задачи** выполните одно из следующих действий:
   - Выберите учетную запись по умолчанию.
   - Введите имя и пароль пользователя, с правами учетной записи которого вы хотите выполнять задачу.
9. Нажмите на кнопку **Далее**.
10. В окне **Завершение создания задачи** установите флажок **Открыть окно свойств задачи после ее создания**.
11. Нажмите на кнопку **Готово**.

    Откроется окно свойств задачи с параметрами по умолчанию.

12. Откройте вкладку **Параметры приложения**.

    В разделе **Источник правил** по умолчанию выбрано **Пользовательская база правил из файла**.

13. Нажмите на кнопку **Импортировать базу правил из файла**.

14. В открывшемся окне укажите архив с базой правил.

    Вы можете загрузить только один архив, содержащий XML-файлы с OVAL- и XCCDF-правилами.

    > Совокупный размер архива не должен превышать 2 МБ.

15. Нажмите на кнопку **Открыть**.

    В разделе **Источник правил** отобразятся данные по загруженным правилам. По ссылке **Подробнее** в поле **Платформы** вы можете открыть окно со списком операционных систем, которые упомянуты в правилах выбранного источника.

16. Если необходимо, загрузите файл с внешними переменными:

    > Использование внешних переменных недоступно, если выбранный источник правил содержит XCCDF-правила.

    a. Установите флажок **Использовать данные с внешними переменными для пользовательских баз**.

    b. Нажмите на ссылку **Импортировать внешние переменные из файла**.

    c. В открывшемся окне укажите путь к файлу с внешними переменными.

    d. Нажмите на кнопку **Открыть**.

17. В разделе **Область применения**, если необходимо, измените режим проверки на уязвимости:

    > Раздел **Область применения** недоступен, если выбранный источник правил содержит XCCDF-правила.

    a. Выберите один из режимов:

    - **Проверять все уязвимости**.

      Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей.

    - **Проверять все уязвимости, кроме добавленных в список**.

      Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей, кроме добавленных в список ниже.

- **Проверять уязвимости, добавленные в список**.

  Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на уязвимости, добавленные в список ниже.

b. Если вы выбрали режим **Проверять все уязвимости, кроме добавленных в список** или **Проверять уязвимости, добавленные в список**, с помощью кнопок **Добавить** и **Добавить в соответствии с условиями** создайте список уязвимостей.

18. В разделе **Расширенные настройки**, если необходимо, определите статусы проверки по директивам, которые будут включаться в отчет задачи аудита безопасности:

    Применение директив недоступно, если выбранный источник правил содержит XCCDF-правила.

    a. Установите флажок **Применять директивы**.

    b. С помощью переключателей напротив каждой директивы определите статусы проверки по директивам, которые будут отображаться в отчете задачи аудита безопасности.

    Если переключатель напротив статуса директивы включен, результат проверки по правилам директивы с этим статусом будет отображаться в отчете задачи аудита безопасности.

    По умолчанию переключатели включены для статусов **True** и **False** для всех директив.

19. В разделе **Расширенные настройки**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

    a. Установите флажок **Включить запись в журнал**.

    b. Выберите необходимый **Уровень записи в журнал** из списка.

    Журнал доступен в папке по умолчанию C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

    Доступны следующие уровни записи в журнал:

    - **Критический уровень** – только критические события;
    - **Уровень предупреждений** – только критические и предупреждающие события;
    - **Информационный уровень** – все критические, предупреждающие и информационные события;
    - **Отладочный уровень** – все критические, предупреждающие, информационные и отладочные события.

20. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Вы можете запускать созданную задачу вручную или настроить автоматический запуск задачи по расписанию. Подробнее читайте в справке Kaspersky Security Center.

Настройка параметров задачи аудита безопасности с использованием базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП

База данных уязвимостей Kaspersky ICS CERT для АСУ ТП поставляется и обновляется вместе с обновлениями баз и модулей Kaspersky Industrial CyberSecurity for Nodes. Поэтому, прежде чем приступить к настройке параметров задачи аудита безопасности с использованием базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП в качестве источника правил, обновите базы и модули программы.

Чтобы настроить параметры задачи аудита безопасности с использованием базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП в качестве источника правил:

1. В главном окне Web Console перейдите в раздел **Управление активами** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи аудита безопасности.
3. Выберите вкладку **Параметры приложения**.
4. В разделе **Источник правил** выберите **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП**.

   Отобразится информация о базе уязвимостей. По ссылке **Подробнее** в поле **Платформы** вы можете открыть окно со списком операционных систем, которые упомянуты в правилах выбранного источника.
5. В разделе **Область применения**, если необходимо, измените режим проверки на уязвимости:

   a. Выберите один из режимов:

   - **Проверять все уязвимости**.

     Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП.

   - **Проверять все уязвимости, кроме добавленных в список**.

     Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, кроме добавленных в список ниже.

   - **Проверять уязвимости, добавленные в список**.

     Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на уязвимости, добавленные в список ниже.

   b. Если вы выбрали режим **Проверять все уязвимости, кроме добавленных в список** или **Проверять уязвимости, добавленные в список**, с помощью кнопок **Добавить** и **Добавить в соответствии с условиями** создайте список уязвимостей.
6. В разделе **Расширенные настройки**, если необходимо, определите статусы проверки по директивам, которые будут включаться в отчет задачи аудита безопасности:

   a. Установите флажок **Применять директивы**.

b. С помощью переключателей напротив каждой директивы определите статусы проверки по директивам, которые будут отображаться в отчете задачи аудита безопасности.

Если переключатель напротив статуса директивы включен, результат проверки по правилам директивы с этим статусом будет отображаться в отчете задачи аудита безопасности.

По умолчанию переключатели включены для статусов **True** и **False** для всех директив.

7. В разделе **Расширенные настройки**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

a. Установите флажок **Включить запись в журнал**.

b. Выберите необходимый **Уровень записи в журнал** из списка.

Журнал доступен в папке по умолчанию C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

Доступны следующие уровни записи в журнал:

- **Критический уровень** – только критические события;
- **Уровень предупреждений** – только критические и предупреждающие события;
- **Информационный уровень** – все критические, предупреждающие и информационные события;
- **Отладочный уровень** – все критические, предупреждающие, информационные и отладочные события.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры задачи.

Настройка параметров задачи аудита безопасности с использованием конфигурации безопасности и соответствий стандартам

Конфигурации безопасности и соответствий стандартам поставляются и обновляются вместе с обновлениями баз и модулей Kaspersky Industrial CyberSecurity for Nodes. Поэтому, прежде чем приступить к настройке параметров задачи аудита безопасности с использованием конфигурации безопасности и соответствий стандартам, обновите базы и модули программы.

Чтобы настроить параметры задачи аудита безопасности с использованием конфигурации безопасности и соответствий стандартам в качестве источника правил:

1. В главном окне Web Console перейдите в раздел **Управление активами → Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи аудита безопасности.
3. Выберите вкладку **Параметры приложения**.
4. В разделе **Источник правил** выберите **Конфигурации безопасности и соответствий стандартам для операционных систем**.
5. Нажмите на кнопку **Выбрать конфигурацию правил**.

6. В открывшемся окне выберите одну из конфигураций безопасности и соответствий стандартам.
7. Нажмите на кнопку **ОК**.

   В разделе **Источник правил** отобразится информация о выбранной конфигурации безопасности и соответствий стандартам. А в разделе **Правила** отобразится список правил, входящих в выбранную в качестве источника конфигурацию безопасности и соответствий стандартам.
8. В разделе **Расширенные настройки**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

   a. Установите флажок **Включить запись в журнал**.

   b. Выберите необходимый **Уровень записи в журнал** из списка.

      Журнал доступен в папке по умолчанию C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

      Доступны следующие уровни записи в журнал:

      - **Критический уровень** – только критические события;
      - **Уровень предупреждений** – только критические и предупреждающие события;
      - **Информационный уровень** – все критические, предупреждающие и информационные события;
      - **Отладочный уровень** – все критические, предупреждающие, информационные и отладочные события.
9. В разделе **Правила** изучите список правил, входящих в выбранную конфигурацию безопасности и соответствий стандартам:

   - Нажатием на название правила откройте описание правила.
   - Нажатием на кнопку **Фильтр** откройте окно для фильтрации правил.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры задачи.

Настройка параметров задачи аудита безопасности с использованием пользовательской базы правил из хранилища Kaspersky Security Center

Прежде чем приступить к настройке параметров задачи аудита безопасности с использованием пользовательской базы из хранилища Kaspersky Security Center:

1. Создайте отпечаток сертификата подписи пользовательской базы через интерфейс командной строки.

   Вы можете использовать уже существующий отпечаток сертификата подписи пользовательской базы.

2. Создайте инсталляционный пакет Kaspersky Security Center с именем package.zip через интерфейс командной строки.

3. Добавьте архив package.zip с OVAL- и XCCDF-правилами, созданный на предыдущем шаге, в репозиторий Kaspersky Security Center. Для этого создайте и запустите задачу установки инсталляционного пакета со следующими параметрами:

   - Инсталляционный пакет должен быть создан на основе файлов архива package.zip, созданного на предыдущем шаге.
   - В окне выбора устройств, которым будет назначена задача установки инсталляционного пакета, вручную задайте адрес компьютера, на котором установлен Сервер администрирования Kaspersky Security Center.

В Kaspersky Industrial CyberSecurity for Nodes можно только обновить установленный и развернутый пакет с пользовательской базой правил. Удалить пакет правил невозможно.

Чтобы настроить параметры задачи аудита безопасности с использованием пользовательской базы правил из хранилища Kaspersky Security Center:

1. В главном окне Web Console откройте раздел **Управление активами** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи.
3. Выберите вкладку **Параметры приложения**.
4. В разделе **Источник правил** выберите **Пользовательская база правил из хранилища Kaspersky Security Center**.
5. Нажмите на кнопку **Выбрать файл из пользовательской коллекции**.
6. В открывшемся окне выберите архив с базой правил.

   Вы можете загрузить только один архив, содержащий XML-файлы с OVAL- и/или XCCDF-правилами.

   Совокупный размер архива не должен превышать 2 МБ.

7. Нажмите на кнопку **Открыть**.

   В разделе **Источник правил** отобразятся данные о загруженных правилах. По ссылке **Подробнее** в поле **Платформы** вы можете открыть окно со списком операционных систем, которые упомянуты в правилах выбранного источника.

8. Если необходимо, укажите отпечаток сертификата подписи пользовательской базы правил:

   a. Установите флажок **Использовать отпечаток**. Если функция включена, при выполнении задачи Kaspersky Security Center производит проверку отпечатка. Если отпечаток не совпадает с указанным в настройках задачи, выполнение задачи прерывается с ошибкой.

      Если функция выключена, Kaspersky Security Center не проверяет отпечаток.

   b. В поле **Отпечаток** введите отпечаток, полученный через интерфейс командной строки.

9. Если необходимо, загрузите файл с внешними переменными:

Использование внешних переменных недоступно, если выбранный источник правил содержит XCCDF-правила.

a. Установите флажок **Использовать данные с внешними переменными для пользовательских баз**.

b. Нажмите на кнопку **Импортировать внешние переменные из файла**.

c. В открывшемся окне укажите путь к файлу с внешними переменными.

d. Нажмите на кнопку **OK**.

10. В разделе **Область применения**, если необходимо, измените режим проверки на уязвимости:

Раздел **Область применения** недоступен, если выбранный источник правил содержит XCCDF-правила.

a. Выберите один из режимов:

- **Проверять все уязвимости**.

  Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП.

- **Проверять все уязвимости, кроме добавленных в список**.

  Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, кроме добавленных в список ниже.

- **Проверять уязвимости, добавленные в список**.

  Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на уязвимости, добавленные в список ниже.

b. Если вы выбрали режим **Проверять все уязвимости, кроме добавленных в список** или **Проверять уязвимости, добавленные в список**, с помощью кнопок **Добавить** и **Добавить в соответствии с условиями** создайте список уязвимостей.

11. В разделе **Расширенные настройки**, если необходимо, определите статусы проверки по директивам, которые будут включаться в отчет задачи аудита безопасности:

Применение директив недоступно, если выбранный источник правил содержит XCCDF-правила.

a. Установите флажок **Применять директивы**.

b. С помощью переключателей напротив каждой директивы определите статусы проверки по директивам, которые будут отображаться в отчете задачи аудита безопасности.

Если переключатель напротив статуса директивы включен, результат проверки по правилам директивы с этим статусом будет отображаться в отчете задачи аудита безопасности.

По умолчанию переключатели включены для статусов **True** и **False** для всех директив.

12. В разделе **Расширенные настройки**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

    a. Установите флажок **Включить запись в журнал**.

    b. Выберите необходимый **Уровень записи в журнал** из списка.

    Журнал доступен в папке по умолчанию C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

    Доступны следующие уровни записи в журнал:

    - **Критический уровень** – только критические события;
    - **Уровень предупреждений** – только критические и предупреждающие события;
    - **Информационный уровень** – все критические, предупреждающие и информационные события;
    - **Отладочный уровень** – все критические, предупреждающие, информационные и отладочные события.

13. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры задачи.

Настройка параметров задачи аудита безопасности с использованием пользовательской базы из файла

Чтобы настроить параметры задачи аудита безопасности с использованием пользовательской базы из файла:

1. В главном окне Web Console откройте раздел **Управление активами** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи.
3. Откройте вкладку **Параметры приложения**.
4. В разделе **Источник правил** выберите **Пользовательская база правил из файла**.
5. Нажмите на кнопку **Импортировать базу правил из файла**.
6. В открывшемся окне укажите архив с базой правил.

   Вы можете загрузить только один архив, содержащий XML-файлы с OVAL- и XCCDF-правилами.

   > Совокупный размер архива не должен превышать 2 МБ.

7. Нажмите на кнопку **Открыть**.

   В разделе **Источник правил** отобразятся данные по загруженным правилам. По ссылке **Подробнее** в поле **Платформы** вы можете открыть окно со списком операционных систем, которые упомянуты в правилах выбранного источника.

8. Если необходимо, загрузите файл с внешними переменными:

Использование внешних переменных недоступно, если выбранный источник правил содержит XCCDF-правила.

a. Установите флажок **Использовать данные с внешними переменными для пользовательских баз**.

b. Нажмите на ссылку **Импортировать внешние переменные из файла**.

c. В открывшемся окне укажите путь к файлу с внешними переменными.

d. Нажмите на кнопку **Открыть**.

9. В разделе **Область применения**, если необходимо, измените режим проверки на уязвимости:

Раздел **Область применения** недоступен, если выбранный источник правил содержит XCCDF-правила.

a. Выберите один из режимов:

- **Проверять все уязвимости**.

  Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей.

- **Проверять все уязвимости, кроме добавленных в список**.

  Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на все уязвимости, описанные в правилах базы данных уязвимостей, кроме добавленных в список ниже.

- **Проверять уязвимости, добавленные в список**.

  Kaspersky Industrial CyberSecurity for Nodes проверяет устройства, для которых назначена задача, на уязвимости, добавленные в список ниже.

b. Если вы выбрали режим **Проверять все уязвимости, кроме добавленных в список** или **Проверять уязвимости, добавленные в список**, с помощью кнопок **Добавить** и **Добавить в соответствии с условиями** создайте список уязвимостей.

10. В разделе **Расширенные настройки**, если необходимо, определите статусы проверки по директивам, которые будут включаться в отчет задачи аудита безопасности:

Применение директив недоступно, если выбранный источник правил содержит XCCDF-правила.

a. Установите флажок **Применять директивы**.

b. С помощью переключателей напротив каждой директивы определите статусы проверки по директивам, которые будут отображаться в отчете задачи аудита безопасности.

Если переключатель напротив статуса директивы включен, результат проверки по правилам директивы с этим статусом будет отображаться в отчете задачи аудита безопасности.

По умолчанию переключатели включены для статусов **True** и **False** для всех директив.

11. В разделе **Расширенные настройки**, если необходимо, настройте параметры записи в журнал событий о выполнении задачи:

    a. Установите флажок **Включить запись в журнал**.

    b. Выберите необходимый **Уровень записи в журнал** из списка.

    Журнал доступен в папке по умолчанию C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

    Доступны следующие уровни записи в журнал:

    - **Критический уровень** – только критические события;
    - **Уровень предупреждений** – только критические и предупреждающие события;
    - **Информационный уровень** – все критические, предупреждающие и информационные события;
    - **Отладочный уровень** – все критические, предупреждающие, информационные и отладочные события.

12. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры задачи.

Просмотр результатов выполнения задачи аудита безопасности

Чтобы просмотреть результаты выполнения задачи аудита безопасности:

1. В главном окне Web Console откройте раздел **Управление активами** → **Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Отчеты**.

Список отчетов содержит результаты выполнения задачи в отсортированном по дате порядке. Каждая строка списка содержит **статус выполнения задачи** на указанном в параметрах задачи узле, а также дату и время завершения выполнения задачи.

Kaspersky Industrial CyberSecurity for Nodes возвращает статус результата выполнения задачи аудита безопасности:

- *Passed*.

  Задача аудита безопасности получает этот статус, если результат проверки по директиве **Vulnerability** имеет статус *False*, для остальных директив – *True*.

- *Not Passed*.

  Задача аудита безопасности получает этот статус, если результат проверки по директиве **Vulnerability** имеет статус *True*, для остальных директив – *False*.

- *Warning*.

  Задача аудита безопасности получает этот статус, если результаты проверки по всем директивам имеют статус *Error*.

- *Other*.

  Задача аудита безопасности получает этот статус, если результаты проверки по всем директивам имеют статусы *Unknown*, *Not evaluated* или *Not applicable*.

Вы можете фильтровать данные в отчете с помощью фильтра.

Отчет о выполнении задачи аудита безопасности доступен для просмотра в Kaspersky Security Center в течение семи дней с момента выполнения задачи или до момента удаления задачи.

Экспорт результатов выполнения задачи аудита безопасности в отдельный файл

Чтобы экспортировать результаты выполнения задачи аудита безопасности в отдельный файл:

1. В главном окне Web Console откройте раздел **Управление активами → Задачи**.
2. Откройте окно настройки параметров задачи, нажав на имя задачи.
3. Выберите вкладку **Параметры приложения**.
4. В разделе **Отчет** выберите необходимый отчет и нажмите на кнопку **Подробнее**.
5. В открывшемся окне **Результаты выполнения задачи аудита безопасности** выполните одно из следующих действий:

   - Если вы хотите получить архив с отчетом по всем результатам выполнения задачи в формате XML, нажмите на кнопку **Экспорт**.

     В стандартную папку операционной системы для загрузки файлов будет сохранен ZIP-архив с отчетом в формате XML. Если в параметрах задачи была включена запись событий о выполнении аудита безопасности в журнал, то дополнительно добавится ZIP-архив с журналом в TXT- файле.

   - Если вы хотите получить архив с отчетом выполнения задачи в формате HTML:

     a. При необходимости, отфильтруйте данные отчета с помощью кнопки **Фильтр**.

     b. Нажмите на кнопку **Создать отчет**.

     В стандартную папку операционной системы для загрузки файлов будет сохранен ZIP-архив с отчетом в формате HTML. В отчет будут включены только отфильтрованные строки.

   Название архива с отчетом содержит имя узла, для которого выполнялась задача, а также дату и время создания архива отчета.

Создание отпечатка сертификата подписи для файлов с OVAL- или XCCDF-правилами

Чтобы создать отпечаток сертификата подписи файлов с OVAL-или XCCDF-правилами:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt `cmd.exe`) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл ovaldbmgr.exe.

   По умолчанию файл расположен в папке \tools\ovaldbmgr комплекта поставки.
3. В зависимости от размещения сертификата выполните одну из следующих команд:

   - Для создания сертификата с последующим размещением в System Storage Local Machine:

     ```
     ovaldbmgr.exe --signer=make-cert --subject=<certificate name>
     ```

   - Для создания сертификата с последующим размещением в PFX-контейнере:

     ```
     ovaldbmgr.exe --signer=make-cert --subject=<certificate_name> --export --pwd=
     <password_for_accessing_the_PFX_container> --pfx=<full_path_and_file_name_of_the_PFX_container>
     ```

   В случае успешного формирования сертификата в командной строке возвращается отпечаток сертификата.

Создание инсталляционного пакета Kaspersky Security Center с пользовательскими OVAL- или XCCDF-правилами

Чтобы создать инсталляционный пакет Kaspersky Security Center в виде подписанного архива с OVAL- или XCCDF-правилами:

1. На устройстве запустите интерпретатор командной строки (например, Command Prompt `cmd.exe`) с правами учетной записи локального администратора.
2. С помощью команды `cd` перейдите в папку, где находится файл ovaldbmgr.exe.

   По умолчанию файл расположен в папке \tools\ovaldbmgr комплекта поставки.
3. В зависимости от размещения сертификата подписи для файла с OVAL- или XCCDF-правилами выполните одну из следующих команд:

   - Если сертификат подписи расположен в System Storage Local Machine:

     ```
     ovaldbmgr.exe --make-package --command={replace|merge} --subject=<certificate name> --output=<full path> --
     source=<full path> <full path to the file with OVAL or XCCDF rules>
     ```

- Если сертификат подписи расположен в PFX-контейнере:

```
ovaldbmgr.exe --make-package --command={replace|merge} --pfx=<full path to the PFX container> --pwd=
<password to access the PFX container> --output=<full path> --source=<full path> <full path to the file
with OVAL or XCCDF rules>
```

Параметры команды для создания инсталляционного пакета Kaspersky Security Center

Параметры	Описание
`--make-package`	Обязательный параметр. Создает архив с файлами.
`--command={replace|merge}`	Обязательный параметр. Параметр определяет режим развертывания пакета в Kaspersky Security Center. Доступные значения: • `replace` – замена существующего в хранилище Kaspersky Security Center инсталляционного пакета на создаваемый. • `merge` – объединение создаваемого инсталляционного пакета с уже существующим в хранилище Kaspersky Security Center пакетом. Если значение параметра не задано, команда завершается с ошибкой.
`--pfx=<full path to the PFX container>`	Обязательный параметр. Параметр указывает полный путь к PFX-контейнеру, который содержит отпечаток сертификата подписи для файла с OVAL- или XCCDF-правилами.
`--pwd=<password to access the PFX container>`	Обязательный параметр. Параметр передает пароль доступа к PFX-контейнеру.
`--subject=<certificate name>`	Обязательный параметр. Параметр передает имя сертификат подписи. Если указано имя несуществующего сертификата подписи, команда завершается с ошибкой.
`--output=<full path>`	Обязательный параметр. Параметр указывает полный путь к папке, в которой в результате выполнения команды будет создан инсталляционный пакет.
`--source=<full path>`	Параметр указывает полный путь к папке, в которой содержится папка с OVAL- и XCCDF-правилам, которые вы желаете включить в пакет Kaspersky Security Center.
`<full path to the file with OVAL or XCCDF rules>`	Параметр указывает полный путь к файлам с OVAL- или XCCDF-правилами в формате XML, которые вы желаете включить в пакет Kaspersky Security Center. OVAL- и XCCDF-правила должны быть сохранены в кодировке UTF-8 без BOM. Файл с OVAL- или XCCDF-правилами должен быть расположен в папке, которая расположена в еще одной папке. Например: C:\Users\UserName\Desktop\folder\subfolder\OvalRules.xml Вы можете указать несколько значений параметра через пробел. Чтобы указать файлы с OVAL- или XCCDF-правилами, можно выбрать один из следующих вариантов: • Задать только значение параметра `--source=<full path>`. • Указать одно или несколько значений `<full path to OVAL or XCCDF rules>` через пробел. • Одновременно задать значение параметра `--source=<full path>` и указать одно или несколько значений `<full path to the file with OVAL or XCCDF rules>` через пробел. Если не задано ни одного значения `<full path to the file with OVAL or XCCDF rules>` и не задан параметр `--source=<full path>`, задача завершится с ошибкой.

В результате выполнения команды Kaspersky Industrial CyberSecurity for Nodes создает:

- Архив с именем package.zip в папке, указанной в значении параметра `--output=<full path>`. Архив содержит следующие файлы:
  - Один или несколько ZIP-файлов для каждого из пользовательских файлов с OVAL- или XCCDF-правилами. Каждый архив содержит один XML-файл с правилами и файл подписи этого XML-файла.
  - Файл ovaldbmgr.kud для развертывания пакета Kaspersky Security Center.
  - Утилиту развертывания ovaldbmgr.exe.
- Отпечаток сертификата, которым подписан архив package.zip.

  Вы можете указать отпечаток в параметрах задачи аудита безопасности с использованием пользовательской базы правил из хранилища Kaspersky Security Center в качестве источника правил.

Использование Kaspersky Security Gateway

Приложение совместимо с Kaspersky Security Gateway версии 4.0 и выше.

Kaspersky Security Gateway предназначен для передачи в систему SCADA диагностической информации из Kaspersky Security Center, полученной от Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks, или от Kaspersky Industrial CyberSecurity for Networks напрямую. Информация о состоянии защиты промышленной сети и отдельных компьютеров сети отображается на экране системы SCADA, что позволяет оператору системы SCADA своевременно реагировать на проблемы защиты промышленной сети.

Kaspersky Security Gateway использует следующие протоколы связи для взаимодействия с системами SCADA:

- **IEC 60870-5-104**. Единый открытый протокол для систем автоматизации.
- **OPC DA**. Спецификация взаимодействия устройств в промышленных сетях, основанная на технологии Microsoft COM.
- **OPC UA**. Спецификация взаимодействия устройств в промышленных сетях, которая обеспечивает кроссплатформенную совместимость.

Параметры передачи данных можно настроить как с помощью графического интерфейса Kaspersky Security Gateway, так и с помощью стандартных средств Microsoft Windows.

Диагностические данные

Kaspersky Security Gateway передает в систему SCADA следующую информацию:

- **SecurityServerAvailable**. Доступность Сервера администрирования Kaspersky Security Center. Возможные значения:
  - `1`. Kaspersky Security Gateway успешно подключен к Серверу администрирования Kaspersky Security Center.
  - `0`. Kaspersky Security Gateway не может подключиться к Серверу администрирования Kaspersky Security Center.
- **AllSecuredHostAvailable**. Доступность всех защищаемых компьютеров сети. Определяется наличием на всех компьютерах работающих приложений для защиты и Агента администрирования. Возможные значения:
  - `0`. Хотя бы один компьютер, управляемый Сервером администрирования Kaspersky Security Center и выбранный для мониторинга в параметрах Kaspersky Security Gateway, недоступен на момент определения состояния.
  - `1`. Все компьютеры, управляемые Сервером администрирования Kaspersky Security Center и выбранные для мониторинга в параметрах Kaspersky Security Gateway, доступны на момент определения состояния.

Если между хотя бы одним компьютером и Сервером администрирования Kaspersky Security Center нет связи, то передается значение `0` (недоступен).

- **GeneralizedThreatOccured**. Состояние защиты сети. Возможные значения:
  - `0`. Угрозы не обнаружены на всех компьютерах сети.
  - `1`. Хотя бы на одном компьютере сети обнаружена угроза.
  - `2`. Хотя бы на одном компьютере сети есть предупреждение.

  При определении состояния защиты сети Kaspersky Security Gateway использует информацию о состоянии компьютеров, выбранных в параметрах Kaspersky Security Gateway для отображения в системе SCADA.

- **<Имя компьютера>**. Доступность и состояние защиты компьютера. Доступность компьютера определяется наличием на компьютере работающего приложения для защиты и Агента администрирования. Возможные значения:
  - `-1`. Невозможно получить статус компьютера.
  - `0`. Компьютер доступен.
  - `1`. На компьютере обнаружена угроза.
  - `2`. На компьютере есть предупреждение.
  - `3`. Компьютер недоступен.

  Kaspersky Security Gateway отправляет информацию о состоянии компьютеров, выбранных в параметрах Kaspersky Security Gateway для отображения в системе SCADA.

  Если между компьютером или Kaspersky Security Gateway и Сервером администрирования Kaspersky Security Center нет связи, то передается значение `-1` (невозможно получить статус компьютера).

- **<Имя ПЛК>**. Статус ПЛК, подключенного к Kaspersky Security Center:
  - `-1`. Невозможно получить статус.
  - `0`. Нет сообщений об ошибках или ПЛК не проверялся.
  - `1`. Есть критическая ошибка (например, проект ПЛК не совпадает с эталонным проектом ПЛК).
  - `2`. Есть предупреждения.
  - `3`. ПЛК недоступен.

- **<Имя устройства>**. Статус устройства (ПЛК или IED), подключенного к Kaspersky Industrial CyberSecurity for Networks:
  - `-1`. Невозможно получить статус.
  - `0`. Нет сообщений об ошибках или устройство не проверялось.
  - `1`. Есть критическая ошибка (например, проект ПЛК не совпадает с эталонным проектом ПЛК).
  - `2`. Есть предупреждения.
  - `3`. Устройство недоступно.
- **UnauthorizedSystemCommandCount**. Счетчик новых событий для устройства, подключенного к Kaspersky Industrial CyberSecurity for Networks. Возможные значения:
  - `<number>`. Количество новых событий.
  - `-1`. Невозможно получить статус.

Ограничения и известные ошибки для Kaspersky Security Gateway

- Для подключения Kaspersky Security Gateway, установленного на устройстве с операционной системой Windows 7, Windows Server 2008 или Windows Server 2012, к Kaspersky Security Center 14 и более поздних версий требуется, чтобы в операционной системе были включены протоколы TLS 1.1 и TLS 1.2 в качестве безопасных протоколов по умолчанию. Подробнее читайте в документации Microsoft.
- Аварийное завершение работы `gateway_service.exe` может быть вызвано ошибками в сторонней библиотеке grpc. Аварийное завершение службы происходит при подключении к Kaspersky Industrial CyberSecurity for Networks одновременно с выполнением динамического анализа кода с помощью утилиты проверки программ (Application Verifier).
- Kaspersky Security Gateway совместим с Kaspersky Industrial CyberSecurity for Networks версий 4.2 и выше.
- При использовании сервера KSG OPC UA совместно с PcVue 16.2, PcVue 16.2 может аварийно завершить работу при открытии узла SessionsDiagnosticsSummary.
- При использовании протоколов OPC DA и OPC UA значения тегов должны иметь тип int.
- Статус тегов Quality не используется и всегда имеет значение GOOD. При отключении отслеживания тега, он исключается из передаваемых данных. Отправка тега с измененным статусом (BAD или COM_FAILURE) не выполняется.
- После запуска Kaspersky Security Gateway не передает в систему SCADA значения тегов до получения данных от Kaspersky Security Center или Kaspersky Industrial CyberSecurity for Networks.

  При обновлении Kaspersky Security Gateway версии 4.5 и ниже до версии 5.0 запись файлов трассировки отключается. При необходимости настройте запись файлов трассировки заново.

- Если отслеживаемое устройство было удалено из Kaspersky Industrial CyberSecurity for Networks, данное устройство перестает отображаться в блоке **Отслеживаемые данные** консоли Kaspersky Security Gateway, однако для данного устройства будут продолжать передаваться теги **<Имя устройства>** со значением `-1` и **UnauthorizedSystemCommandCount** значением `0`. Для того, чтобы остановить отправку данных об удаленном устройстве, выполните следующие действия:

  1. Откройте Консоль Kaspersky Security Gateway.
  2. В узле **Kaspersky Security Gateway** выберите используемый протокол.
  3. В панели результатов в блоке **Отслеживаемые данные** нажмите на ссылку **Изменить**.

     Откроется окно **Выбор отслеживаемых данных**.
  4. Вносить изменения не требуется, закройте окно с помощью кнопки **OK**.

Интерфейс Консоли Kaspersky Security Gateway

Консоль Kaspersky Security Gateway отображается в дереве Microsoft Management Console в виде узла с именем **Kaspersky Security Gateway**.

В дереве Консоли отображается узел **Kaspersky Security Gateway** и дочерние узлы для настройки использования протоколов передачи данных в SCADA-систему:

- **IEC 60870-5-104**;
- **OPC DA**;
- **OPC UA**.

В области результатов узла **Kaspersky Security Gateway** отображаются следующие данные:

- Общая информация о Kaspersky Security Gateway.
- Подробная информация о параметрах подключения к Kaspersky Security Center и Kaspersky Industrial CyberSecurity for Networks и ссылка на окно настройки.
- Подробная информация о текущих дополнительных параметрах Kaspersky Security Gateway и ссылка на окно настройки.

Настройка соединения с Kaspersky Security Center

Чтобы настроить соединение с Kaspersky Security Center:

1. Откройте Консоль Kaspersky Security Gateway.
2. Выберите узел **Kaspersky Security Gateway**.
3. В панели результатов в разделе **Параметры соединения** нажмите на ссылку **Настройка соединения**.

   Откроется окно **Параметры соединения**.

4. В блоке **Kaspersky Security Center** укажите параметры подключения к Серверу администрирования Kaspersky Security Center:

   - **Сервер**. IP-адрес или доменное имя Сервера администрирования Kaspersky Security Center и номер порта для подключения к нему. Подробная информация о настройке подключения к Серверу администрирования приведена в справке Kaspersky Security Center. Диапазон возможных значений номера порта: 1–65535.

   - **Имя пользователя**. Имя учетной записи администратора Сервера администрирования Kaspersky Security Center.

   - **Пароль**. Пароль учетной записи администратора Сервера администрирования Kaspersky Security Center.

5. Выберите тип подключения:

   - **Отключено**. Подключение к Серверу администрирования Kaspersky Security Center не выполняется.

   - **Open API**. Если в качестве поставщика данных выбран интерфейс Open API, необходимо **экспортировать корневой сертификат Kaspersky Security Center** и установить его в Хранилище сертификатов доверенных корневых центров сертификации (CA). Для поставщика данных Open API по умолчанию используется номер порта 13299.

     1. В браузере введите `https://<Web Console address>:13299`.

     2. С помощью штатных средств браузера откройте данные сертификата для установленного соединения с Web Console.

     3. В окне **Сертификаты** выберите вкладку **Путь к сертификату**.

     4. Выберите корневой сертификат.

     5. Перейдите на вкладку **Детали**.

     6. Экспортируйте выбранный сертификат с помощью кнопки **Копировать в файл**.

   - **klakaut**. *klakaut* – это утилита автоматизации Kaspersky Security Center, позволяющая управлять Сервером администрирования Kaspersky Security Center через внешний API с помощью объектов COM (Component Object Model). Если в качестве поставщика данных выбрана утилита klakaut, необходимо, чтобы до установки Kaspersky Security Gateway на том же компьютере была установлена Консоль администрирования Kaspersky Security Center. Для поставщика данных klakaut по умолчанию используется номер порта 13291. По умолчанию выбран этот вариант.

     Если Консоль администрирования Kaspersky Security Center установлена после Kaspersky Security Gateway, соединение между Kaspersky Security Gateway и Сервером администрирования Kaspersky Security Center не будет установлено.

- **Автоматически**. Приложение последовательно пытается выполнить подключение к Серверу администрирования Kaspersky Security Center с использованием klakaut и Open API. Данный вариант выбран по умолчанию после обновления Kaspersky Security Gateway версии 4.5 и ниже до версии 5.0.

  Тип подключения **Автоматически** доступен только после установки новой версии Kaspersky Security Gateway поверх предыдущей. После изменения типа подключения данный вариант перестает отображаться в раскрывающемся списке.

6. Нажмите на кнопку **Проверка соединения**.

   Статус *Подключено* показывает, что соединение установлено.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **OK**, чтобы закрыть окно **Kaspersky Security Gateway**.

Параметры подключения можно также настроить с помощью конфигурационного файла `ConnectionSettings.xml`, расположенного в папке `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings`. Обратите внимание, что в файле конфигурации нельзя задать пароль. Для задания пароля используйте Консоль Kaspersky Security Gateway.

Настройка соединения с Kaspersky Industrial CyberSecurity for Networks

Чтобы настроить соединение с Kaspersky Industrial CyberSecurity for Networks:

1. Откройте Консоль Kaspersky Security Gateway.

2. Выберите узел **Kaspersky Security Gateway**.

3. В разделе **Параметры соединения** в панели результатов нажмите на ссылку **Настройка соединения**.

   Откроется окно **Параметры соединения**.

4. В блоке **Kaspersky Industrial CyberSecurity for Networks** добавьте параметры подключения к одному или нескольким серверам Kaspersky Industrial CyberSecurity for Networks:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Параметры соединения с Kaspersky Industrial CyberSecurity for Networks**.

   b. Введите IP-адрес коннектора типа Generic, предварительно добавленного в Kaspersky Industrial CyberSecurity for Networks, и номер порта для подключения к нему. Диапазон возможных значений номера порта: 1–65535.

      Параметры подключения к коннектору отличаются от параметров подключения к серверу интеграции Kaspersky Industrial CyberSecurity for Networks. Подробная информация о коннекторах приведена в справке Kaspersky Industrial CyberSecurity for Networks.

c. Если вы хотите настроить доверенное соединение с Kaspersky Industrial CyberSecurity for Networks:

1. Установите флажок **Использовать закрепленный сертификат для защиты соединения**.
2. Нажмите на кнопку **Загрузить**.
3. В открывшемся окне выберите файл с TLS-сертификатом.
4. Нажмите на кнопку **Открыть**.

Данные о добавленном TLS-сертификате отобразятся в блоке параметров **Данные TLS-сертификата**.

> Если вы указали закрепленный сертификат для защиты соединения, необходимо также указать сертификат клиента. В противном случае соединение с сервером Kaspersky Industrial CyberSecurity for Networks не будет установлено.

d. Если вы хотите настроить дополнительную защиту подключения с использованием сертификата клиента:

1. Установите флажок **Защитить подключение с помощью сертификата клиента**.
2. Нажмите на кнопку **Загрузить**.
3. В открывшемся окне выберите файл формата PFX с сертификатом клиента.
4. Нажмите на кнопку **Открыть**.
5. В одноименном поле введите пароль для сертификата клиента, если он был задан.

e. Нажмите на кнопку **Проверить**.

Статус *Подключено* показывает, что соединение установлено.

f. Нажмите на кнопку **OK**.

g. Если необходимо, повторите пункты a-f для добавления параметров подключения с другими серверами Kaspersky Industrial CyberSecurity for Networks.

Данные для соединения с Kaspersky Industrial CyberSecurity for Networks отобразятся в списке в окне **Параметры соединения**.

5. Нажмите на кнопку **OK**.

> Параметры подключения можно также настроить с помощью конфигурационного файла `ConnectionSettings.xml`, расположенного в папке `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings`. Обратите внимание, что в файле конфигурации нельзя задать пароль. Для задания пароля используйте Консоль Kaspersky Security Gateway.

Настройка протокола DCOM

Если компьютеры, участвующие в передаче и получении данных по протоколу OPC DA, не присоединены к домену Active Directory, для каждого из этих компьютеров создайте учетные записи пользователей с одинаковыми именем и паролем.

Чтобы установить соединение по протоколу OPC DA, необходимо настроить права доступа для протокола распределенной объектной модели компонентов (DCOM).

Как настроить протокол DCOM для взаимодействия Kaspersky Security Gateway и SCADA-системы, установленных на одном компьютере

1. На компьютере с установленными Kaspersky Security Gateway и SCADA-системой, между которыми настраивается взаимодействие, нажмите комбинацию клавиш **Win+R**.

   Откроется стандартное окно Microsoft Windows **Выполнить**.

2. В поле **Открыть** введите *dcomcnfg* и нажмите на кнопку **OK**.

   Откроется окно **Службы компонентов**.

3. В левой части окна в дереве папок выберите **Службы компонентов** → **Компьютеры** → **Мой компьютер**.

4. Откройте контекстное меню папки **Мой компьютер** и выберите **Свойства**.

5. В окне **Свойства: Мой компьютер** выберите вкладку **Безопасность COM**.

6. В блоке **Права доступа** нажмите на кнопку **Изменить значения по умолчанию**.

   Откроется окно **Разрешение на доступ**.

7. В блоке **Группы или пользователи** выберите группу **NETWORK SERVICE**.

8. В таблице разрешений для группы **NETWORK SERVICE**, в столбце **Разрешить** установите флажки **Локальный доступ** и **Удаленный доступ**.

9. Выберите вкладку **Свойства по умолчанию** и убедитесь, что установлены следующие значения настроек: **Уровень проверки подлинности по умолчанию –** *Подключиться*, **Уровень олицетворения по умолчанию –** *Определить*.

10. Нажмите на кнопку **OK**.

11. В окне **Свойства: Мой компьютер** нажмите на кнопку **OK**.

12. Перезагрузите компьютер.

Как настроить протокол DCOM для взаимодействия Kaspersky Security Gateway и SCADA-системы, установленных на разных компьютерах

На обоих компьютерах выполните следующие действия:

1. Нажмите комбинацию клавиш **Win+R**.

   Откроется стандартное окно Microsoft Windows **Выполнить**.

2. В поле **Открыть** введите *dcomcnfg* и нажмите на кнопку **OK**.

   Откроется окно **Службы компонентов**.

3. В левой части окна в дереве папок выберите **Службы компонентов → Компьютеры → Мой компьютер**.

4. Откройте контекстное меню папки **Мой компьютер** и выберите **Свойства**.

5. В окне **Свойства: Мой компьютер** выберите вкладку **Безопасность COM**.

6. В блоке **Права доступа** нажмите на кнопку **Изменить ограничения**.

   Откроется окно **Разрешение на доступ**.

7. В блоке **Группы или пользователи** выберите группу **ANONYMOUS LOGON**.

8. В таблице разрешений для группы **ANONYMOUS LOGON**, в столбце **Разрешить** установите флажки **Локальный доступ** и **Удаленный доступ**.

   > Разрешение удаленного доступа для группы ANONYMOUS LOGON влияет на уровень безопасности системы. Рекомендуем проверить работу по протоколу OPC DA без использования этого разрешения и предоставлять разрешение только в том случае, если работа без него невозможна.

9. В блоке **Права доступа** нажмите на кнопку **Изменить значения по умолчанию** и повторите пункты 7-8 инструкции.

10. В блоке **Разрешения на запуск и активацию** нажмите на кнопку **Изменить ограничения** и повторите пункты 7-8 инструкции.

11. В блоке **Разрешения на запуск и активацию** нажмите на кнопку **Изменить значения по умолчанию** и повторите пункты 7-8 инструкции.

12. На вкладке **Свойства по умолчанию** убедитесь, что установлены следующие значения настроек: **Уровень проверки подлинности по умолчанию –** *Подключиться*, **Уровень олицетворения по умолчанию** – *Определить*.

13. Нажмите на кнопку **OK**.

14. В окне **Свойства: Мой компьютер** нажмите на кнопку **OK**.

15. Настройте приложение OPCEnum.

    a. В левой части окна в дереве папок выберите **Службы компонентов → Компьютеры → Мой компьютер → Настройка DCOM → OPCEnum**.

    b. По правой клавише мыши откройте контекстное меню **OPCEnum** и выберите **Свойства**.

       Откроется окно **Свойства: OPCEnum**.

    c. На вкладке **Общие** убедитесь, что для настройки **Уровень проверки подлинности по умолчанию** установлено значение *Подключиться*.

    d. На вкладке **Безопасность** в блоке **Разрешения на запуск и активацию** нажмите на кнопку **Изменить**.

    e. В блоке **Группы или пользователи** выберите группу **Все**.

f. В таблице разрешений для группы **Все** в столбце **Разрешить** установите флажки **Локальный доступ**, **Удаленный доступ**, **Локальная активация**, **Удаленная активация**.

g. В блоке **Права доступа** нажмите на кнопку **Изменить**.

h. В блоке **Группы или пользователи** выберите группу **Все**.

i. В таблице разрешений для группы **Все** в столбце **Разрешить** установите флажки **Локальный доступ** и **Удаленный доступ**.

j. На вкладке **Удостоверение** выберите **Системная учетная запись**.

k. Нажмите на кнопку **OK**.

16. Перезагрузите компьютер.

На компьютере с установленной утилитой Kaspersky Security Gateway выполните следующие действия:

1. Нажмите комбинацию клавиш **Win+R**.

   Откроется стандартное окно Microsoft Windows **Выполнить**.

2. В поле **Открыть** введите *dcomcnfg* и нажмите на кнопку **OK**.

   Откроется окно **Службы компонентов**.

3. В левой части окна в дереве папок выберите **Службы компонентов** → **Компьютеры** → **Мой компьютер** → **Настройка DCOM** → **Kaspersky Gateway OPC Service**.

4. Откройте контекстное меню **Kaspersky Gateway OPC Service** и выберите **Свойства**.

   Откроется окно **Свойства: Kaspersky Gateway OPC Service**.

5. На вкладке **Общие** убедитесь, что для настройки **Уровень проверки подлинности по умолчанию** установлено значение *Подключиться*.

6. Нажмите на кнопку **OK**.

7. Если Kaspersky Security Gateway и SCADA-система установлены на компьютерах, относящихся к разным доменам:

   a. В операционной системе откройте **Панель управления** – **Администрирование** – **Локальная политика безопасности**.

   b. В дереве консоли локальной политики безопасности выберите раздел **Локальные политики** – **Параметры безопасности**.

   c. В рабочей области раздела **Параметры безопасности** в контекстном меню локальной политики **Сетевой доступ: разрешить применение разрешений для всех к анонимным пользователям** выберите пункт **Включить**.

8. Перезагрузите компьютер.

Настройка параметров передачи данных с использованием протоколов связи

В этом разделе приведены инструкции по настройке передачи данных с использованием доступных протоколов связи.

Настройка передачи данных по протоколу IEC 60870-5-104

Чтобы настроить передачу данных по протоколу IEC 60870-5-104 через Консоль Kaspersky Security Gateway:

1. Откройте Консоль Kaspersky Security Gateway.
2. В узле **Kaspersky Security Gateway** выберите **IEC 60870-5-104**.
3. В панели результатов в разделе **Настройка передачи данных** нажмите на ссылку **Изменить**.

   Откроется окно **Параметры**.
4. В блоке **Параметры передачи** выключите или включите функцию **Разрешить передачу данных**.

   Если функция включена, Kaspersky Security Gateway передает состояние защиты узлов промышленной сети в систему SCADA. По умолчанию функция выключена.
5. В блоке **Параметры соединения со SCADA-системой** настройте следующие параметры:

   - **Адрес устройства**. Дополнительный адрес, присвоенный компьютеру в системе SCADA. Диапазон возможных значений: 1–65535.
   - **Порт устройства**. Номер порта для подключения к системе SCADA. Диапазон возможных значений: 1–65535.
   - **Период ожидания TCP-соединения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания отправки сообщения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания подтверждения сообщения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Период ожидания тестового соединения**. Значение указывается в секундах. Диапазон возможных значений: 1–255.
   - **Максимально количество получаемых неподтвержденных сообщений**. Диапазон возможных значений: 1–32767.
   - **Максимально количество отправляемых неподтвержденных сообщений**. Диапазон возможных значений: 1–32767.
6. Нажмите на кнопку **OK**.

7. В разделе **Отслеживаемые данные** в панели результатов нажмите на ссылку **Изменить**.

   Откроется окно **Выбор отслеживаемых данных**. В списке отображаются отслеживаемые данные, добавленные автоматически после соединения с источником данных, – Kaspersky Security Center и/или Kaspersky Industrial CyberSecurity for Networks.

8. С помощью флажков рядом с именами компьютеров включите или выключите отслеживание данных об их доступности и состоянии защиты. Доступность компьютера определяется наличием на компьютере работающего приложения для защиты и Агента администрирования.

   Если отслеживание включено, данные будут передаваться в SCADA-систему.

   Если отслеживание выключено, данные не будут передаваться в SCADA-систему.

   > Если между компьютером или Kaspersky Security Gateway и Сервером администрирования Kaspersky Security Center нет связи, то передается значение `-1` (невозможно получить статус компьютера).

9. Если необходимо, измените или добавьте служебный тег в столбце **Служебный тег**. С помощью служебного тега вы можете фильтровать данные, поступившие в SCADA-систему. Тег может состоять только из цифр.

10. Нажмите на кнопку **OK**.

Параметры передачи данных по протоколу IEC 60870-5-104 можно настроить с помощью конфигурационного файла `ProtocolEICSettings.xml`, расположенного в папке `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings`.

Настройка передачи данных по протоколу OPC DA

Для успешной передачи данных по протоколу OPC DA должны быть выполнены следующие условия:

- Программе OPCEnum предоставлены необходимые права DCOM в системе SCADA и в Kaspersky Security Gateway.
- Для компьютера с установленным Kaspersky Security Gateway и системой SCADA применяется единая аутентификация: либо используется доменная аутентификация, либо для всех компьютеров рабочей группы используется одно и то же имя пользователя и пароль.

Чтобы настроить передачу данных по протоколу OPC DA через Консоль Kaspersky Security Gateway:

1. Откройте Консоль Kaspersky Security Gateway.
2. В узле **Kaspersky Security Gateway** выберите **OPC DA**.
3. В панели результатов в разделе **Параметры передачи данных** нажмите на ссылку **Изменить**.

   Откроется окно **Параметры**.

4. Выключите или включите функцию **Включить передачу данных**.

   Если функция включена, Kaspersky Security Gateway передает состояние защиты узлов промышленной сети в систему SCADA. По умолчанию функция выключена.

5. Нажмите на кнопку **OK**.

6. В разделе **Отслеживаемые данные** в панели результатов нажмите на ссылку **Изменить**.

   Откроется окно **Выбор отслеживаемых данных**. В списке отображаются отслеживаемые данные, добавленные автоматически после соединения с источником данных, – Kaspersky Security Center и/или Kaspersky Industrial CyberSecurity for Networks.

7. С помощью флажков рядом с именами компьютеров включите или выключите отслеживание данных об их доступности и состоянии защиты. Доступность компьютера определяется наличием на компьютере работающего приложения для защиты и Агента администрирования.

   Если отслеживание включено, данные будут передаваться в SCADA-систему.

   Если отслеживание выключено, данные не будут передаваться в SCADA-систему.

   > Если между компьютером или Kaspersky Security Gateway и Сервером администрирования Kaspersky Security Center нет связи, то передается значение `-1` (невозможно получить статус компьютера).

8. Если необходимо, измените или добавьте служебный тег в столбце **Служебный тег**. С помощью служебного тега вы можете фильтровать данные, поступившие в SCADA-систему. Тег может состоять из цифр и букв.

9. Нажмите на кнопку **OK**.

Параметры передачи данных по протоколу OPC DA можно настроить с помощью конфигурационного файла `ProtocolOPCSettings.xml`, расположенного в папке `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings`.

Настройка передачи данных по протоколу OPC UA

Чтобы настроить передачу данных по протоколу OPC UA через Консоль Kaspersky Security Gateway:

1. Откройте Консоль Kaspersky Security Gateway.

2. В узле **Kaspersky Security Gateway** выберите **OPC UA**.

3. В панели результатов в разделе **Параметры передачи данных** нажмите на ссылку **Изменить**.

   Откроется окно **Параметры**.

4. Выключите или включите функцию **Включить передачу данных**.

   Если функция включена, Kaspersky Security Gateway передает состояние защиты узлов промышленной сети в систему SCADA. По умолчанию функция выключена.

5. В блоке **Параметры соединения со SCADA-системой** введите номер порта для подключения к системе SCADA. Диапазон возможных значений номера порта: 1–65535.

6. Нажмите на кнопку **OK**.

7. В разделе **Отслеживаемые данные** в панели результатов нажмите на ссылку **Изменить**.

   Откроется окно **Выбор отслеживаемых данных**. В списке отображаются отслеживаемые данные, добавленные автоматически после соединения с источником данных, – Kaspersky Security Center и/или Kaspersky Industrial CyberSecurity for Networks.

8. С помощью флажков рядом с именами компьютеров включите или выключите отслеживание данных об их доступности и состоянии защиты. Доступность компьютера определяется наличием на компьютере работающего приложения для защиты и Агента администрирования.

   Если отслеживание включено, данные будут передаваться в SCADA-систему.

   Если отслеживание выключено, данные не будут передаваться в SCADA-систему.

   > Если между компьютером или Kaspersky Security Gateway и Сервером администрирования Kaspersky Security Center нет связи, то передается значение `-1` (невозможно получить статус компьютера).

9. Если необходимо, измените или добавьте служебный тег в столбце **Служебный тег**. С помощью служебного тега вы можете фильтровать данные, поступившие в SCADA-систему. Тег может состоять из цифр и букв.

10. Нажмите на кнопку **OK**.

Параметры передачи данных по протоколу OPC UA можно настроить с помощью конфигурационного файла `ProtocolOPCUASettings.xml`, расположенного в папке `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings`.

Настройка передачи данных с помощью конфигурационного файла

Для настройки конфигурационных файлов необходимы специальные знания. Некорректные изменения конфигурационных файлов могут привести к ошибкам в работе Kaspersky Security Gateway.

Чтобы настроить параметры передачи данных с помощью конфигурационного файла:

1. В любом доступном текстовом редакторе откройте конфигурационный файл со служебными параметрами Kaspersky Security Gateway, который находится в папке `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings`:

   - `ProtocolIECSettings.xml` – конфигурационный файл для протокола IEC 60870-5-104;
   - `ProtocolOPCSettings.xml` – конфигурационный файл для протокола OPC DA;
   - `ProtocolOPCUASettings.xml` – конфигурационный файл для протокола OPC UA.

2. Настройте параметры для передачи данных.

3. Сохраните конфигурационный файл.

4. Перезапустите службу Kaspersky Security Gateway, чтобы новые параметры вступили в силу.

Настройка дополнительных параметров Kaspersky Security Gateway

Чтобы настроить дополнительные параметры Kaspersky Security Gateway:

1. Откройте Консоль Kaspersky Security Gateway.
2. Выберите узел **Kaspersky Security Gateway**.
3. В панели результатов в разделе **Параметры программы** нажмите на ссылку **Настройка программы**.
   Откроется окно **Параметры программы**.
4. В разделе **Опрос** задайте **Период опроса (сек)**.
5. В разделе **Трассировка**:
   - Снимите или установите флажок **Записывать файл трассировки**.
   - В раскрывающемся списке выберите **Уровень** детализации регистрируемой информации.
6. В окне **Параметры программы** нажмите на кнопку **OK**.

Дополнительные параметры Kaspersky Security Gateway можно настроить с помощью конфигурационного файла `AppSettings.xml`, расположенного в папке `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings`.

Просмотр событий Kaspersky Security Gateway

Во время работы Kaspersky Security Gateway могут происходить следующие события:

- Включение и выключение экземпляров службы Kaspersky Security Gateway.
- Проблемы взаимодействия Kaspersky Security Gateway с системой SCADA.
- Проблемы подключения к Серверу администрирования Kaspersky Security Center и получения данных от Сервера администрирования.
- Проблемы с доступом к конфигурационному файлу Kaspersky Security Gateway.

Информация о данных событиях записывается в файлы трассировки, которые хранятся в папке `%ProgramData%\Kaspersky Lab\Security Gateway\Traces`.

Управление полнодисковым шифрованием BitLocker

BitLocker – встроенная в операционную систему Windows технология шифрования. Kaspersky Industrial CyberSecurity for Nodes позволяет контролировать и управлять Bitlocker с помощью Kaspersky Security Center. BitLocker шифрует логический том. Подробнее о BitLocker см. в документации Microsoft.

Kaspersky Industrial CyberSecurity for Nodes не поддерживает управление BitLocker на компьютерах под управлением операционных систем Windows Vista и Windows Server 2008.

При шифровании диска BitLocker помещает загрузчик и другие служебные файлы в системный раздел (англ. system partition). Этот раздел не зашифрован. Операционная система создает системный раздел автоматически при установке Windows. Если перед установкой Windows диск полностью размечен, операционная система не сможет создать системный раздел. В этом случае при запуске шифрования диска BitLocker операционная система предложит пользователю разметить диск снова и создать системный раздел. После создания системного раздела операционная система запустит шифрование диска BitLocker.

Kaspersky Industrial CyberSecurity for Nodes не поддерживает шифрование съемных дисков с помощью BitLocker.

BitLocker обеспечивает безопасность хранения ключей доступа с помощью доверенного платформенного модуля. *Доверенный платформенный модуль* (англ. Trusted Platform Module, TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Использование TPM является самым безопасным способом хранения ключей доступа BitLocker, так как TPM позволяет проверять целостность операционной системы. На компьютерах без TPM вы также можете зашифровать диски. При этом ключ доступа будет зашифрован паролем. Таким образом, BitLocker использует следующие способы аутентификации:

- TPM.
- TPM и PIN-код.
- Пароль.

Перед шифрованием диска BitLocker создает ключ восстановления. Kaspersky Industrial CyberSecurity for Nodes считывает и отправляет ключ восстановления в Kaspersky Security Center, чтобы вы имели возможность восстановить доступ к диску, если пользователь, например, забыл пароль.

После шифрования системного жесткого диска для загрузки операционной системы пользователю нужно пройти процедуру аутентификации BitLocker. После прохождения процедуры аутентификации BitLocker будет доступен вход в систему. BitLocker не поддерживает технологию единого входа (SSO).

Если пользователь самостоятельно зашифровал диск с помощью BitLocker, Kaspersky Industrial CyberSecurity for Nodes отправит информацию о шифровании диска и ключ восстановления в Kaspersky Security Center.

Если вы используете групповые политики для Windows, выключите управление BitLocker в параметрах политики. Параметры политики для Windows могут противоречить параметрам политики Kaspersky Industrial CyberSecurity for Nodes. При шифровании диска могут возникнуть ошибки.

Запуск шифрования диска BitLocker

Перед запуском полнодискового шифрования рекомендуется убедиться в том, что компьютер не заражен. Для этого запустите полную проверку или проверку важных областей компьютера. Выполнение полнодискового шифрования на компьютере, зараженном руткитом, может привести к неработоспособности компьютера.

Для работы BitLocker на компьютерах под управлением операционной системы Windows для серверов может потребоваться установить компонент шифрования диска BitLocker. Установите компонент средствами операционной системы (мастер добавления ролей и компонентов). Подробнее об установке компонента шифрования диска BitLocker см. в документации Microsoft.

Как запустить шифрование диска BitLocker в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. Выберите раздел **Шифрование данных**.
4. В раскрывающемся списке **Режим шифрования** выберите элемент **Шифровать все жесткие диски**.

   Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой выполнялось шифрование.

5. Настройте дополнительные параметры шифрования диска BitLocker (см. таблицу ниже).
6. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как запустить шифрование диска BitLocker в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных**.

5. В подразделе **Полнодисковое шифрование** нажмите на кнопку **Настроить**.

6. В раскрывающемся списке **Режим шифрования** выберите элемент **Шифровать все жесткие диски**.

Если на компьютере установлено несколько операционных систем, то после шифрования вы сможете выполнить загрузку только той операционной системы, в которой выполнялось шифрование.

7. Настройте дополнительные параметры шифрования диска BitLocker (см. таблицу ниже).

8. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Вы можете контролировать процесс шифрования или расшифровки диска на компьютере пользователя с помощью Консоли приложения.

После применения политики в зависимости от настроек аутентификации приложение отобразит в Диагностическом окне или Консоли приложения следующие запросы:

- Только TPM. Участие пользователя не требуется. Диск будет зашифрован после перезагрузки компьютера.
- TPM + PIN / Пароль. При наличии модуля TPM, появится окно запроса PIN-кода. При отсутствии модуля TPM, появится окно запроса пароля для предзагрузочной аутентификации.
- Только пароль. Появится окно запроса пароля для предзагрузочной аутентификации.

Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), то в операционных системах Windows 8, а также в более ранних версиях появится окно запроса на подключение запоминающего устройства для сохранения файла ключа восстановления. Вы можете сохранять несколько файлов ключей восстановления на одном запоминающем устройстве.

После установки пароля или PIN-кода BitLocker запросит перезагрузку компьютера для проверки совместимости компьютера пользователя с BitLocker. Kaspersky Industrial CyberSecurity for Nodes отобразит в Диагностическом окне или Консоли приложения соответствующее уведомление. Далее пользователю нужно пройти процедуру аутентификации BitLocker. После прохождения процедуры аутентификации BitLocker нужно выполнить вход в систему. После загрузки операционной системы BitLocker запустит шифрование диска.

При отсутствии доступа к ключам шифрования пользователь может запросить у администратора локальной сети организации ключ восстановления (если ключ восстановления не был сохранен ранее на запоминающем устройстве или был утерян).

Параметры компонента Шифрование диска BitLocker

Параметр	Описание
Включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах	Использование аутентификации, требующей ввода данных в предзагрузочной среде, даже если у платформы отсутствует возможность предзагрузочного ввода (например, у сенсорных клавиатур на планшетах). Сенсорная клавиатура планшетов недоступна в предзагрузочной среде. Для прохождения аутентификации BitLocker на планшетах пользователю необходимо подключить, например, USB-клавиатуру. Если флажок установлен, то использование аутентификации, требующей предзагрузочного ввода, разрешено. Рекомендуется использовать этот параметр только для устройств, у которых во время предварительной загрузки, помимо сенсорных клавиатур, имеются альтернативные средства ввода данных, например, USB-клавиатура. Если флажок снят, шифрование диска BitLocker на планшетах невозможно.

Параметр	Описание
Использовать аппаратное шифрование (ОС Windows 8 и выше)	Если флажок установлен, то приложение применяет аппаратное шифрование. Это позволяет увеличить скорость шифрования и сократить использование ресурсов компьютера.
Шифровать только занятое пространство (ОС Windows 8 и выше)	Флажок включает/выключает функцию, ограничивающую область шифрования только занятыми секторами жесткого диска. Это ограничение позволяет сократить время шифрования. Включение/выключение функции **Шифровать только занятое пространство (ОС Windows 8 и выше)** после запуска шифрования не изменяет этого параметра до тех пор, пока жесткие диски не будут расшифрованы. Требуется установить или снять флажок до начала шифрования. Если флажок установлен, то шифруется только та часть жесткого диска, которая занята файлами. Kaspersky Industrial CyberSecurity for Nodes зашифровывает новые данные автоматически по мере их добавления. Если флажок снят, то шифруется весь жесткий диск, в том числе остатки удаленных и отредактированных ранее файлов. Данную функцию рекомендуется применять для новых жестких дисков, данные которых не редактировались и не удалялись. Если вы применяете шифрование на уже используемом жестком диске, рекомендуется зашифровать весь жесткий диск. Это гарантирует защиту всех данных – даже удаленных, но потенциально восстанавливаемых. По умолчанию флажок снят.
Способ аутентификации	**Доверенный платформенный модуль (TPM)** Если выбран этот вариант, BitLocker использует доверенный платформенный модуль (TPM). Доверенный платформенный модуль (англ. Trusted Platform Module, TPM) – микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины. Для компьютеров под управлением операционных систем Windows 7 и Windows Server 2008 R2 доступно только шифрование с использованием модуля TPM. Если модуль TPM не установлен, шифрование BitLocker невозможно. Использование пароля на этих компьютерах не поддерживается. Устройство, оснащенное доверенным платформенным модулем, может создавать ключи шифрования, которые могут быть расшифрованы только с его помощью. Доверенный платформенный модуль шифрует ключи шифрования собственным корневым ключом хранилища. Корневой ключ хранилища хранится внутри доверенного платформенного модуля. Это обеспечивает дополнительную степень защиты ключей шифрования от попыток взлома. Этот вариант действия выбран по умолчанию. Вы можете установить дополнительную защиту для доступа к ключу шифрования и зашифровать ключ паролем или PIN: **Использовать PIN для TPM**. Если флажок установлен, пользователь может использовать PIN-код для получения доступа к ключу шифрования, который хранится в доверенном платформенном модуле (TPM). Если флажок снят, пользователю запрещено использовать PIN-код. Для получения доступа к ключу шифрования пользователь использует пароль. **Доверенный платформенный модуль (TPM), если он недоступен, то пароль** Если выбран этот вариант, то при отсутствии доверенного платформенного модуля (TPM) пользователь может получить доступ к ключам шифрования с помощью пароля. Если флажок снят и модуль TPM недоступен, то полнодисковое шифрование не запускается. **Только пароль (ОС Windows 8 и выше)** Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes запрашивает у пользователя пароль при обращении к зашифрованному диску. Этот вариант действия может быть выбран, если не используется доверенный платформенный модуль (TPM). Для выбранного способа аутентификации необходимо настроить требования к паролю или PIN-коду: • **Минимальная длина PIN-а (символов).** • **Использовать расширенный PIN (с буквами и цифрами)**. Расширенный PIN-код кроме цифр позволяет использовать другие символы: заглавные и строчные латинские буквы, специальные символы и пробел. • **Минимальная длина пароля (символов).** • **Ограничить срок действия пароля / PIN-а для TPM (дни).**
Автоматически пересоздавать ключ восстановления (дни)	Автоматическое обновление пароля для восстановления доступа к диску, защищенному BitLocker. Если флажок установлен, задайте срок действия пароля ключа восстановления.

Расшифровка жесткого диска, защищенного BitLocker

Пользователь может самостоятельно расшифровать диск средствами операционной системы (функция *Выключение BitLocker*). После этого Kaspersky Industrial CyberSecurity for Nodes предложит зашифровать диск повторно. Kaspersky Industrial CyberSecurity for Nodes будет предлагать зашифровать диск пока вы не включите расшифровку дисков в политике.

Как расшифровать жесткий диск, защищенный BitLocker, через Консоль администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. Выберите раздел **Шифрование данных**.
4. В раскрывающемся списке **Режим шифрования** выберите элемент **Расшифровывать все жесткие диски**.
5. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как расшифровать жесткий диск, защищенный BitLocker, через Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Шифрование данных**.
5. В подразделе **Полнодисковое шифрование** нажмите на кнопку **Настроить**.
6. В раскрывающемся списке **Режим шифрования** выберите элемент **Расшифровывать все жесткие диски**.
7. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Вы можете контролировать процесс шифрования или расшифровки диска с помощью Консоли приложения.

Восстановление доступа к диску, защищенному BitLocker

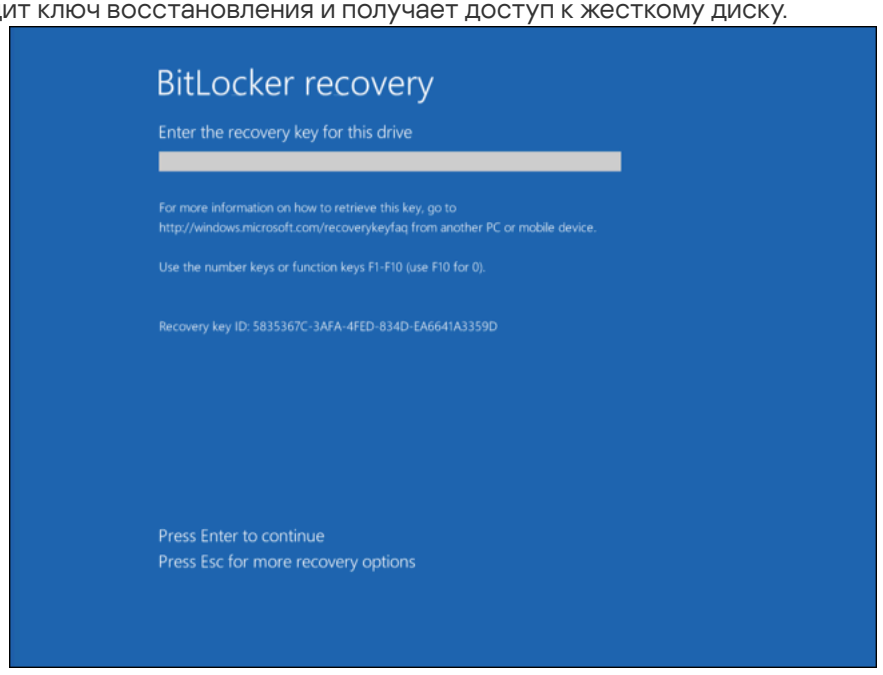
Если пользователь забыл пароль доступа к жесткому диску, зашифрованному BitLocker, нужно запустить процедуру восстановления ("Запрос – Ответ").

Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), то для операционных систем Windows 8, а также более ранних версий, файл ключа восстановления был сохранен на съемный диск перед шифрованием. Для восстановления доступа к диску вставьте съемный диск и следуйте инструкциям на экране.

Восстановление доступа к жесткому диску, зашифрованному BitLocker, состоит из следующих этапов:

1. Пользователь сообщает администратору идентификатор ключа восстановления (см. рис. ниже).
2. Администратор проверяет идентификатор ключа восстановления в свойствах компьютера в Kaspersky Security Center. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в свойствах компьютера.

   Если идентификаторы ключа восстановления совпадают, администратор сообщает пользователю ключ восстановления.
3. Пользователь вводит ключ восстановления и получает доступ к жесткому диску.



Восстановление доступа к жесткому диску, зашифрованному BitLocker

Восстановление доступа к системному диску

Для запуска процедуры восстановления пользователю нужно на этапе предзагрузочной аутентификации нажать клавишу **Esc**.

Как просмотреть ключ восстановления для системного диска, зашифрованного BitLocker, в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Управляемые устройства**.
2. Перейдите на вкладку **Устройства**.
3. Откройте контекстное меню компьютера пользователя, запросившего восстановление доступа к зашифрованным данным.
4. В контекстном меню выберите пункт **Предоставление доступа в офлайн-режиме**.
5. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле **Идентификатор ключа восстановления** на вкладке **Доступ к системному диску с защитой BitLocker**.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

6. Передайте пользователю ключ, указанный в поле **Ключ восстановления**.

Как просмотреть ключ восстановления для системного диска, зашифрованного BitLocker, в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Установите флажок рядом с именем компьютера, доступ к диску которого вы хотите восстановить.
3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
4. Проверьте идентификатор ключа восстановления. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в параметрах компьютера.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

5. Нажмите на кнопку **Получить ключ**.
6. Передайте пользователю ключ, указанный в поле **Ключ восстановления**.

После загрузки операционной системы Kaspersky Industrial CyberSecurity for Nodes предложит пользователю сменить пароль или PIN-код. После установки нового пароля или PIN-кода BitLocker создаст новый пароль восстановления, который будет отправлен приложением в Kaspersky Security Center.

Восстановление доступа к несистемному диску

Для запуска процедуры восстановления пользователю нужно в окне предоставления доступа к диску перейти по ссылке **Забыли пароль**. После получения доступа к зашифрованному диску пользователь может включить автоматическую разблокировку диска при аутентификации Windows в параметрах BitLocker.

Как просмотреть ключ восстановления для несистемного диска, зашифрованного BitLocker, в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Дополнительно → Шифрование и защита данных → Зашифрованные жесткие диски**.

2. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа, и в контекстном меню устройства выберите пункт **Получить доступ к устройству в Kaspersky Industrial CyberSecurity for Nodes**.

3. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле **Идентификатор ключа восстановления**.

   Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

4. Передайте пользователю ключ, указанный в поле **Ключ восстановления**.

Как просмотреть ключ восстановления для несистемного диска, зашифрованного BitLocker, в Web Console

1. В главном окне Web Console выберите **Операции → Шифрование и защита данных → Зашифрованные жесткие диски**.

2. Установите флажок рядом с именем компьютера, доступ к диску которого вы хотите восстановить.

3. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.

   Запустится мастер предоставления доступа к устройству.

4. Следуйте указаниям мастера предоставления доступа к устройству:

   a. Выберите плагин Kaspersky Industrial CyberSecurity for Nodes.

   b. Проверьте идентификатор ключа восстановления. Идентификатор, который предоставил пользователь, должен соответствовать идентификатору, который отображается в параметрах компьютера.

      Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

   c. Нажмите на кнопку **Получить ключ**.

5. Передайте пользователю ключ, указанный в поле **Ключ восстановления**.

Приостановка защиты BitLocker для обновления программного обеспечения

Обновление операционной системы, установка пакетов обновлений операционной системы или обновление другого программного обеспечения с включенной защитой BitLocker имеет ряд особенностей. При установке обновлений может потребоваться перезагрузить компьютер несколько раз. После каждой перезагрузки пользователю необходимо проходить аутентификацию BitLocker. Для корректной установки обновлений вы можете временно выключить аутентификацию BitLocker. При этом диск остается зашифрованным и пользователь имеет доступ к данным после входа в систему. Для управления аутентификацией BitLocker предназначена задача *Управление защитой BitLocker*. С помощью задачи вы можете установить количество перезагрузок компьютера, для которых не требуется аутентификация BitLocker. Таким образом, после установки обновлений и завершении работы задачи *Управление защитой BitLocker* аутентификация BitLocker будет автоматически включена. Вы можете включить аутентификацию BitLocker в любой момент.

Как приостановить защиту BitLocker в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Industrial CyberSecurity for Nodes (5.0)** → **Управление защитой BitLocker**.

Шаг 2. Управление защитой BitLocker

Настройте параметры аутентификации BitLocker. Для приостановки защиты BitLocker выберите **Временно разрешить пропуск аутентификации BitLocker** и установите количество перезагрузок без аутентификации BitLocker (1–15 раз). Если требуется, установите дату и время срока действия задачи. В указанный срок задача автоматически будет выключена и при перезагрузке компьютера пользователю нужно будет проходить аутентификацию BitLocker.

Шаг 3. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 4. Определение названия задачи

Введите название задачи, например, *Обновление до Windows 10*.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи.

Как приостановить защиту BitLocker в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Настройка основных параметров задачи

Настройте основные параметры задачи:

1. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.
2. В раскрывающемся списке **Тип задачи** выберите **Управление защитой BitLocker**.
3. В поле **Название задачи** введите короткое описание, например, *Обновление до Windows 10*.
4. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

Шаг 2. Управление защитой BitLocker

Настройте параметры аутентификации BitLocker. Для приостановки защиты BitLocker выберите **Временно разрешить пропуск аутентификации BitLocker** и установите количество перезагрузок без аутентификации BitLocker (1–15 раз). Если требуется, установите дату и время срока действия задачи. В указанный срок задача автоматически будет выключена и при перезагрузке компьютера пользователю нужно будет проходить аутентификацию BitLocker.

Шаг 3. Завершение создание задачи

Завершите работу мастера. В списке задач отобразится новая задача.

Для выполнения задачи установите флажок напротив задачи и нажмите на кнопку **Запустить**.

В результате после выполнения задачи при следующей перезагрузке компьютера BitLocker не будет запрашивать аутентификацию пользователя. После каждой перезагрузки компьютера Kaspersky Industrial CyberSecurity for Nodes формирует событие о перезагрузке компьютера без аутентификации BitLocker и указывает количество оставшихся перезагрузок.

По истечении заданного количества перезагрузок компьютера или срока действия задачи аутентификация BitLocker будет автоматически включена. Для доступа к данным пользователю нужно пройти процедуру аутентификации BitLocker.

На компьютерах под управлением Windows 7 в BitLocker отсутствует возможность подсчета количества перезагрузок компьютера. Подсчет перезагрузок на компьютерах под управлением Windows 7 выполняет Kaspersky Industrial CyberSecurity for Nodes. Таким образом, для автоматического включения аутентификации BitLocker после каждой перезагрузки должен быть выполнен запуск Kaspersky Industrial CyberSecurity for Nodes.

Для досрочного включения аутентификации BitLocker откройте свойства задачи *Управление защитой BitLocker* и установите значение **Запрашивать пароль каждый раз**.

Интеграция со сторонними системами

Этот раздел содержит описание интеграции Kaspersky Industrial CyberSecurity for Nodes с функциями и технологиями сторонних производителей.

Счетчики производительности для программы Системный монитор

Счетчики производительности – компонент Kaspersky Industrial CyberSecurity for Nodes, с помощью которого вы можете контролировать производительность приложения во время работы компонентов защиты. Kaspersky Industrial CyberSecurity for Nodes регистрирует счетчики производительности при установке.

Вы можете просматривать счетчики производительности приложения с помощью приложения "Системный монитор", доступного в Панели управления Windows. Подробнее об использовании счетчиков производительности см. на сайте Службы технической поддержки Microsoft.

С помощью счетчиков производительности вы можете, например, обнаружить недостаточность ресурсов при совместной работе Kaspersky Industrial CyberSecurity for Nodes с другими приложениями, а также диагностировать сбои в работе и неоптимальную настройку Kaspersky Industrial CyberSecurity for Nodes.

Количество запросов, не обработанных из-за нехватки ресурсов

Количество запросов, не обработанных из-за нехватки ресурсов

Описание	Общее количество запросов драйвера файловых перехватов, не обработанных из-за нехватки системных ресурсов (например, оперативной памяти); рассчитывается с момента последнего запуска Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Industrial CyberSecurity for Nodes пропускает запросы на обработку объектов, которые не обрабатываются драйвером файловых перехватов.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты компьютера, возникающее из-за недостаточности системных ресурсов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нуля, рабочему процессу Kaspersky Industrial CyberSecurity for Nodes требуется больший объем оперативной памяти для обработки запросов. Возможно, активные процессы других программ используют всю доступную оперативную память.

Количество запросов, отданных на обработку

Количество запросов, отданных на обработку

Описание	Количество объектов, ожидающих обработки рабочими процессами.
Назначение	Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Industrial CyberSecurity for Nodes и общий уровень файловой активности на защищаемом устройстве.
Нормальное / пороговое значение	Значение счетчика может изменяться в зависимости от уровня файловой активности на защищаемом устройстве.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Недоступно

Количество объектов, обрабатываемых за секунду

Количество объектов, обрабатываемых за секунду

Описание	Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки времени.
Назначение	Счетчик отражает скорость обработки объектов; позволяет обнаружить и устранить снижение производительности защищаемого устройства, возникшее из-за недостаточности процессорного времени, выделяемого рабочему процессу Kaspersky Industrial CyberSecurity for Nodes, или из-за сбоев в работе Kaspersky Industrial CyberSecurity for Nodes.
Нормальное / пороговое значение	Варьируется / Нет.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Значения счетчика зависят от установленных значений параметров Kaspersky Industrial CyberSecurity for Nodes и от загрузки защищаемого устройства процессами других приложений. Отслеживайте среднее значение показаний счетчика в течение продолжительного времени. Если среднее значение показаний счетчика снизилось, то могла возникнуть одна из следующих ситуаций: • Рабочему процессу Kaspersky Industrial CyberSecurity for Nodes не хватает процессорного времени для обработки объектов. Обеспечьте выделение Kaspersky Industrial CyberSecurity for Nodes дополнительного процессорного времени, например, снизив нагрузку на защищаемое устройство со стороны других программ. • Возник сбой в работе Kaspersky Industrial CyberSecurity for Nodes (простаивает несколько потоков). Перезапустите Kaspersky Industrial CyberSecurity for Nodes.

Количество элементов в очереди зараженных объектов

Количество элементов в очереди зараженных объектов

Описание	Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: • прерывание постоянной защиты компьютера из-за возможного отказа диспетчера файловых перехватов; • перегруженность процессов из-за неравномерного распределения процессорного времени между рабочими процессами и Kaspersky Industrial CyberSecurity for Nodes; • вирусную эпидемию.
Нормальное / пороговое значение	Значение счетчика может быть отличным от нуля, пока Kaspersky Industrial CyberSecurity for Nodes обрабатывает обнаруженные зараженные или возможно зараженные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время.

Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика остается ненулевым длительное время: • Kaspersky Industrial CyberSecurity for Nodes не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов). Перезапустите Kaspersky Industrial CyberSecurity for Nodes. • Не хватает процессорного времени для обработки объектов. Обеспечьте выделение Kaspersky Industrial CyberSecurity for Nodes дополнительного процессорного времени, например, снизив нагрузку на защищаемое устройство со стороны других программ. • Возникла вирусная эпидемия. О возникновении вирусной эпидемии свидетельствует большое количество обнаруженных зараженных или возможно зараженных объектов в компоненте Постоянная защита файлов. Вы можете просмотреть информацию о количестве обнаруженных объектов в статистике компонента или журнале работы компонента.

Общее количество отвергнутых запросов

Общее количество отвергнутых запросов

Описание	**Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были приняты процессами приложения; рассчитывается с момента последнего запуска Kaspersky Industrial CyberSecurity for Nodes.** **Приложение пропускает объекты, запросы на обработку которых отвергаются процессами Kaspersky Industrial CyberSecurity for Nodes.**
Назначение	Счетчик позволяет обнаруживать следующие ситуации: • снижение эффективности постоянной защиты компьютера из-за повышенной нагрузки на процессы Kaspersky Industrial CyberSecurity for Nodes; • прерывание постоянной защиты компьютера из-за отказа диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов. Возможны следующие ситуации в зависимости от поведения счетчика: • Счетчик показывает несколько запросов, отвергнутых в течение длительного времени: процесс Kaspersky Industrial CyberSecurity for Nodes был полностью загружен. Приложение не смогло проверить объекты. Чтобы исключить пропуск объектов, увеличьте выделяемые для приложения системные ресурсы. • Количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Industrial CyberSecurity for Nodes не проверяет объекты при обращении к ним. Перезапустите Kaspersky Industrial CyberSecurity for Nodes.

Общее количество пропущенных запросов

Общее количество пропущенных запросов

Описание	Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Industrial CyberSecurity for Nodes, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска приложения. Если запрос на обработку объекта, принятый одним из рабочих процессов, не отправил события о завершении обработки, драйвер передает этот запрос другому процессу и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1. Если драйвер перебрал все рабочие процессы и ни один из них не принял запрос на обработку (был занят) или не отправил события о завершении обработки, Kaspersky Industrial CyberSecurity for Nodes пропускает такой объект и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1.
Назначение	Счетчик позволяет обнаруживать снижение производительности из-за сбоев диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1

Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нуля, это означает, что зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент. Если скорость проверки не удовлетворительна, перезапустите Kaspersky Industrial CyberSecurity for Nodes, чтобы восстановить простаивающие потоки.

Максимальное количество потоков диспетчера файловых перехватов

Начиная с Kaspersky Industrial CyberSecurity for Nodes версии 5.0 счетчик Максимальное количество потоков диспетчера файловых перехватов не поддерживается.

Среднее количество потоков диспетчера файловых перехватов

Начиная с Kaspersky Industrial CyberSecurity for Nodes версии 5.0 счетчик Среднее количество потоков диспетчера файловых перехватов не поддерживается.

SNMP-счетчики и ловушки в Kaspersky Industrial CyberSecurity for Nodes

Если вы включили компонент Поддержка SNMP-протокола в состав устанавливаемых антивирусных компонентов, вы можете просматривать счетчики и ловушки Kaspersky Industrial CyberSecurity for Nodes по протоколу Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Industrial CyberSecurity for Nodes на компьютере-рабочем месте администратора, запустите на защищаемом устройстве Службу SNMP (SNMP Service), а на рабочем месте администратора – Службу SNMP (SNMP Service) и Службу ловушек SNMP (SNMP Trap Service).

SNMP-счетчики Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит таблицы с описанием параметров SNMP-счетчиков Kaspersky Industrial CyberSecurity for Nodes.

Счетчики производительности

Счетчики производительности

Счетчик	Определение
currentRequestsAmount	Количество запросов, отданных на обработку
currentInfectedQueueLength	Количество элементов в очереди зараженных объектов
currentObjectProcessingRate	Количество объектов, обрабатываемых за секунду
currentWorkProcessesNumber	Количество рабочих процессов Kaspersky Industrial CyberSecurity for Nodes в текущий момент

Счетчик резервного хранилища

Счетчик резервного хранилища

Счетчик	Определение
currentBackupStorageSize	Общий объем данных в папке резервного хранилища (МБ)

Общие счетчики

Общие счетчики

Счетчик	Определение
lastCriticalAreasScanAge	Промежуток времени в секундах с момента завершения задачи *Проверка важных областей*.
licenseExpirationDate	Дата окончания срока действия лицензии. Если добавлен активный и дополнительный ключ, отображается дата окончания срока действия лицензии, связанной с дополнительным ключом.
currentApplicationUptime	Время работы Kaspersky Industrial CyberSecurity for Nodes с момента его последнего запуска, в сотых долях секунды.

Счетчик обновлений

Счетчик обновлений

Счетчик	Определение
avBasesAge	Промежуток времени в сотых долях секунды с момента создания последних установленных обновлений баз.

Счетчики постоянной защиты файлов

Счетчики постоянной защиты файлов

Счетчик	Определение
totalObjectsProcessed	Общее количество проверенных объектов с момента последнего запуска компонента Постоянная защита файлов
totalInfectedObjectsFound	Общее количество обнаруженных зараженных и других объектов с момента последнего запуска компонента Постоянная защита файлов
totalSuspiciousObjectsFound	Общее количество обнаруженных возможно зараженных объектов с момента последнего запуска компонента Постоянная защита файлов

Счетчик	Определение
totalVirusesFound	Общее количество обнаруженных объектов с момента последнего запуска компонента Постоянная защита файлов
totalObjectsQuarantined	Общее количество зараженных, возможно зараженных и прочих объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes поместила на карантин; рассчитывается с момента последнего запуска компонента Постоянная защита файлов
totalObjectsNotQuarantined	Общее количество зараженных или возможно зараженных объектов, которые приложению Kaspersky Industrial CyberSecurity for Nodes не удалось поместить на карантин; рассчитывается с момента последнего запуска компонента Постоянная защита файлов
totalObjectsDisinfected	Общее количество зараженных объектов, которые вылечило приложение Kaspersky Industrial CyberSecurity for Nodes; рассчитывается с момента последнего запуска компонента Постоянная защита файлов
totalObjectsNotDisinfected	Общее количество зараженных и прочих объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes не удалось вылечить; рассчитывается с момента последнего запуска компонента Постоянная защита файлов
totalObjectsDeleted	Общее количество зараженных, возможно зараженных и прочих объектов, которые удалило приложение Kaspersky Industrial CyberSecurity for Nodes; рассчитывается с момента последнего запуска компонента Постоянная защита файлов
totalObjectsNotDeleted	Общее количество зараженных, возможно зараженных и прочих объектов, которые приложению Kaspersky Industrial CyberSecurity for Nodes не удалось удалить; рассчитывается с момента последнего запуска компонента Постоянная защита файлов
totalObjectsBackedUp	Общее количество зараженных и прочих объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes поместила в резервное хранилище; рассчитывается с момента последнего запуска компонента Постоянная защита файлов
totalObjectsNotBackedUp	Общее количество зараженных и прочих объектов, которые приложение Kaspersky Industrial CyberSecurity for Nodes не удалось поместить в резервное хранилище; рассчитывается с момента последнего запуска компонента Постоянная защита файлов
currentFileMonitorTaskStatus	Статус компонента Постоянная защита файлов: • `1` – компонент включен и выполняет функции защиты. • `0` – компонент не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.

Счетчики AMSI-защиты

Счетчики AMSI-защиты

Счетчик	Определение
currentScriptCheckerTaskStatus	Статус компонента AMSI-защита: • `1` – компонент включен и выполняет функции защиты. • `0` – компонент не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.
totalScriptsProcessed	Количество скриптов, обработанных с момента последнего запуска компонента AMSI-защита.
totalInfectedlDangerousScriptsFound	Количество опасных скриптов, обнаруженных с момента последнего запуска компонента AMSI-защита.
totalSuspiciousScriptsFound	Количество подозрительных скриптов, обнаруженных с момента последнего запуска компонента AMSI-защита.
totalScriptsBlocked	Общее количество скриптов, заблокированных с момента последнего запуска компонента AMSI-защита. Значение счетчика изменяется, если компонент включен в режиме **Блокировать**, и равно значению счетчика totalInfectedlDangerousScriptsFound.

SNMP-ловушки Kaspersky Industrial CyberSecurity for Nodes и их параметры

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены следующие параметры SNMP-ловушек:

- eventThreatDetected: Объект обнаружен.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds: Превышен максимальный размер резервного хранилища. Общий объем данных в резервном хранилище превысил значение, заданное параметром **Ограничить размер хранилища до**. Kaspersky Industrial CyberSecurity for Nodes продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds: Превышен порог доступного пространства в резервном хранилище. Объем свободного места в резервном хранилище меньше или равен значению, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Industrial CyberSecurity for Nodes продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotBackuped: Объект не помещен в резервное хранилище.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- objectName
- userName
- computerName
- storageObjectNotAddedEventReason

- eventBackupInternalError: Ошибка резервного хранилища.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated: Базы устарели. Количество дней с момента последнего выполнения задачи *Обновление* (локальной, групповой или задачи для наборов защищаемых устройств).

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated: Базы сильно устарели. Количество дней с момента последнего выполнения задачи *Обновление* (локальной, групповой или задачи для наборов защищаемых устройств).

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted: Приложение запущено.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource

- eventApplicationShutdown: Приложение остановлено.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime: Проверка важных областей защищаемого устройства давно не выполнялась. Количество дней с момента последнего завершения задачи *Проверка важных областей*.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired: Срок действия лицензии истек.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon: Срок действия лицензии скоро истекает. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError: Ошибка выполнения задачи.

В ловушке используются следующие параметры:

- eventSeverity
- eventDateAndTime
- eventSource
- errorCode
- knowledgeBaseId
- taskName

- eventUpdateError: Ошибка при выполнении задачи *Обновление*.
  В ловушке используются следующие параметры:
  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason
  - eventSource

Описания и возможные значения параметров SNMP-ловушек Kaspersky Industrial CyberSecurity for Nodes

Ниже приведено описание и допустимые значения параметров ловушек:

- eventDateAndTime: дата и время события.
- eventSeverity: уровень важности.
  Параметр может принимать следующие значения:
  - critical (1) – критический;
  - warning (2) – предупреждение;
  - info (3) – информационный.
- userName: имя пользователя (например, имя пользователя, который пытался получить доступ к зараженному файлу).
- computerName: имя защищаемого устройства (например, имя защищаемого устройства, с которого пользователь пытался получить доступ к зараженному файлу).
- eventSource: функциональный компонент, в работе которого возникло событие.

Параметр может принимать следующие значения:

- unknown (0) – функциональный компонент не определен;
- quarantine (1) – Карантин;
- backup (2) – Резервное хранилище;
- reporting (3) – Журналы выполнения задач;
- updates (4)– Обновление;
- realTimeProtection (5) – Постоянная защита файлов;
- onDemandScanning (6) – Проверка по требованию;
- product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Industrial CyberSecurity for Nodes в целом;
- systemAudit (8) – Журнал системного аудита.

- eventReason: причина возникновения события.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена.
  - reasonInvalidSettings (1) – только для событий резервного хранилища и карантина. Отображается, если недоступна папка карантина или папка резервного хранилища (недостаточно прав доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Kaspersky Industrial CyberSecurity for Nodes будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.

- objectName: имя объекта (например, имя файла, в котором обнаружен вирус).

- threatName: имя объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название объекта, которое Kaspersky Industrial CyberSecurity for Nodes возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.

- detectType: тип обнаруженного объекта.

  Параметр может принимать следующие значения:

  - undefined (0) – не определен;
  - virware – классические вирусы и сетевые черви;
  - trojware – троянские программы;
  - malware – прочие вредоносные программы;
  - adware – рекламные программы;

- pornware – порнографические программы;
- riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда устройству или личным данным.

- detectCertainty: степень уверенности обнаружения угрозы.

  Параметр может принимать следующие значения:

  - Suspicion (возможно зараженный) – Kaspersky Industrial CyberSecurity for Nodes обнаружило частичное совпадение участка кода объекта с известным участком вредоносного кода.
  - Sure (зараженный) – Kaspersky Industrial CyberSecurity for Nodes обнаружило полное совпадение участка кода объекта с известным участком вредоносного кода.

- days: количество дней (например, количество дней до окончания срока действия лицензии).
- errorCode: код ошибки.
- taskName: название задачи.
- updaterErrorEventReason: причина ошибки обновления.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена;
  - reasonAccessDenied – доступ запрещен;
  - reasonUrlsExhausted – список источников обновлений исчерпан;
  - reasonInvalidConfig – неправильный файл конфигурации;
  - reasonInvalidSignature – неверная подпись;
  - reasonCantCreateFolder – невозможно создать папку;
  - reasonFileOperError – файловая ошибка;
  - reasonDataCorrupted – объект поврежден;
  - reasonConnectionReset – сброс соединения;
  - reasonTimeOut – истекло время ожидания при соединении;
  - reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере;
  - reasonServerAuthError – ошибка проверки подлинности на сервере;
  - reasonHostNotFound – устройство не найдено;
  - reasonServerBusy – сервер недоступен;
  - reasonConnectionError – ошибка соединения;

- reasonModuleNotFound – объект не найден;
- reasonBlstCheckFailed (16) – ошибка проверки списка запрещенных ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.

- storageObjectNotAthreatddedEventReason: причина, по которой объект не был помещен в резервное хранилище или на карантин.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена.
  - reasonStorageInternalError – ошибка базы данных; необходимо восстановление Kaspersky Industrial CyberSecurity for Nodes.
  - reasonStorageReadOnly – база данных доступна только для чтения; необходимо восстановление Kaspersky Industrial CyberSecurity for Nodes.
  - reasonStorageIOError – ошибка ввода-вывода: а) приложение Kaspersky Industrial CyberSecurity for Nodes повреждено и нуждается в восстановлении; б) диск, на котором хранятся файлы Kaspersky Industrial CyberSecurity for Nodes, поврежден.
  - reasonStorageCorrupted – хранилище повреждено; необходимо восстановление Kaspersky Industrial CyberSecurity for Nodes.
  - reasonStorageFull – база данных заполнена; требуется свободное место на диске.
  - reasonStorageOpenError – не удается открыть файл базы данных; необходимо восстановление Kaspersky Industrial CyberSecurity for Nodes.
  - reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Industrial CyberSecurity for Nodes.
  - reasonObjectNotFound – помещаемый на карантин объект отсутствует на диске.
  - reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator.
  - reasonDiskOutOfSpace – недостаточно места на диске.

Интеграция с WMI

Kaspersky Industrial CyberSecurity for Nodes поддерживает интеграцию с инструментарием управления Windows (Windows Management Instrumentation, WMI): вы можете использовать клиентские системы, которые получают с помощью WMI данные по стандарту Web-Based Enterprise Management (WBEM), для получения данных о статусе приложения Kaspersky Industrial CyberSecurity for Nodes и его компонентов.

В момент установки Kaspersky Industrial CyberSecurity for Nodes регистрирует в системе собственный модуль для создания пространства имен Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве. Пространство имен Kaspersky Industrial CyberSecurity for Nodes позволяет работать с классами, экземплярами классов и их свойствами в Kaspersky Industrial CyberSecurity for Nodes.

Значения некоторых свойств экземпляра класса зависят от типа задачи.

Непериодические задачи – это задачи приложения, которые не имеют ограниченного срока действия и либо постоянно выполняются, либо остановлены. Для таких задач невозможно указать прогресс выполнения. Результаты выполнения таких задач фиксируются непрерывно в ходе выполнения и представляют собой отдельные события (например, обнаружение зараженного объекта одной из задач постоянной защиты компьютера). Задачами такого типа можно управлять с помощью политик Kaspersky Security Center.

Периодические задачи – это задачи приложения, срок выполнения которых ограничен, а прогресс выполнения может быть отображен в виде количества процентов. Результаты выполнения таких задач фиксируются по завершении задачи и представляют собой отдельный элемент или факт изменения состояния приложения (например, завершение обновления баз приложения, сформированные конфигурационные файлы для задач автоматического формирования правил). На одном защищаемом устройстве одновременно может быть запущено несколько периодических задач одного типа (например, три задачи проверки по требованию с разными областями проверки). Вы можете управлять периодическими задачами с помощью групповых задач Kaspersky Security Center.

Если в вашей корпоративной сети используются инструменты, которые могут формировать запросы к пространству имен WMI и получать из него динамические данные, вы сможете получить следующие данные о текущем состоянии приложения.

Данные о состоянии приложения

Свойство экземпляра класса	Описание	Значения
`ProductName`	Название установленного приложения.	Полное название приложения без номера версии.
`ProductVersion`	Полный номер версии установленного приложения.	Полный номер версии приложения, включая номер сборки.
`InstalledPatches`	Набор отображаемых имен установленных патчей.	Перечень критических исправлений, установленных для приложения.
`IsLicenseInstalled`	Статус активации приложения.	Статус ключа, с помощью которого активировано приложение. Возможные значения: • `False`. Лицензионный ключ не добавлен. • `True`. Лицензионный ключ добавлен.
`LicenseDaysLeft`	Количество дней до истечения срока действия текущей лицензии.	Количество дней, оставшихся до истечения срока действия текущей лицензии. Возможные неположительные значения: • `0`. Срок действия лицензии истек. • `-1`. Не удалось получить данные о текущем ключе или указанный ключ не может быть использован для активации приложения (например, заблокирован по причине нахождения в списке запрещенных ключей).
`AVBasesDatetime`	Временная отметка для текущей версии антивирусных баз.	Дата и время формирования антивирусных баз, используемых в текущий момент. Если установленное приложение не использует антивирусные базы, поле содержит значение `{Not installed}`.
`IsExploitPreventionEnabled`	Статус компонента Защита от эксплойтов.	Статус компонента Защита от эксплойтов. Возможные значения: • `True`. Компонент Защита от эксплойтов включен и выполняет функции защиты. • `False`. Компонент Защита от эксплойтов не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.
`ProtectionTasksRunning`	Набор запущенных задач защиты.	Перечень задач защиты, контроля и мониторинга, запущенных в текущий момент. В данном поле должны учитываться все запущенные непериодические задачи. Если не запущена ни одна из непериодических задач, поле содержит значение `{No}`.

Свойство экземпляра класса	Описание	Значения
`IsAppControlRunning`	Статус компонента Контроль запуска программ.	Возможные значения • `True`. Компонент Контроль запуска программ включен и выполняет функции защиты. • `False`. Компонент Контроль запуска программ не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.
`AppControlMode`	Режим работы компонента Контроль запуска программ.	Возможные значения: • `Active`. В параметрах компонента указан режим **Блокировать**. • `Statistics Only`. В параметрах компонента указан режим **Информировать**. • `Not installed`. Компонент Контроль запуска программ не установлен. • `Unknown`. Компонент выключен.
`AppControlRulesNumber`	Общее количество правил контроля запуска программ.	Количество правил, заданных в параметрах компонента Контроль запуска программ в текущий момент.
`AppControlLastBlocking`	Временная отметка последней блокировки запуска программы, выполненной компонентом Контроль запуска программ в любом режиме.	Дата и время последней блокировки запуска программы, выполненной компонентом Контроль запуска программ. При заполнении поля учитываются все блокировки программ, независимо от режима работы компонента. Если на момент выполнения запроса WMI не зарегистрировано ни одного случая блокировки запуска программы, в поле отображается значение `{No}`.
`PeriodicTasksRunning`	Набор запущенных периодических задач.	Перечень задач проверки по требованию, обновления и инвентаризации, запущенных в текущий момент. В данном поле должны отображаться все запущенные периодические задачи. Если не запущена ни одна из периодических задач, поле содержит значение `{No}`.
`ConnectionState`	Состояние соединения между компонентом Поставщик WMI и службой Kaspersky Industrial CyberSecurity for Nodes Service.	Информация о статусе соединения между компонентом Поставщик WMI и службой Kaspersky Industrial CyberSecurity for Nodes Service. Возможные значения: • `Success`. Соединение успешно установлено: клиент WMI может принимать данные о статусе приложения. • `Failed. Error Code: <code>`. Соединение не удалось установить из-за ошибки с указанным кодом.
`IsDumpingEnabled`	Статус записи дампов памяти.	Возможные значения • `True`. Запись дампов включена. • `False`. Запись дампов выключена.
`DumpsFolder`	Папка для хранения файлов дампов.	Полный путь к папке. Если запись дампов выключена, поле будет пустым.
`IsTracingEnabled`	Статус трассировки работы приложения.	Возможные значения • `True`. Трассировка работы приложения включена. • `False`. Трассировка работы приложения выключена.
`TraceFolder`	Папка для хранения файлов трассировки.	Полный путь к папке. Если трассировка работы приложения выключена, поле будет пустым.

Свойство экземпляра класса	Описание	Значения
`AllTasksState`	Статус всех задач.	Информация о статусе задач в формате `{<profile-name_1>, <profile-type_1>, <profile-state_1>,...<profile-name_N>, <profile-type_N>, <profile-state_N>}`, где `profile-name` – название задачи, `profile-type` – тип задачи, `profile-state` – текущий статус задачи. Возможные значения статусов: • `not started`. Задача еще не запускалась. • `running`. Задача выполняется. • `running ma`. Задача выполняется, в процессе выполнения задачи произошел сбой. • `paused`. Задача приостановлена. • `stopped`. Задача остановлена. • `completed`. Задача завершилась успешно. • `failed`. Задача завершилась с ошибкой. • `disabled`. Задача отключена и не может быть запущена. • `starting`. Задача в процессе запуска. • `pausing`. Задача в процессе приостановки. • `stopping`. Задача в процессе остановки. • `<unknown>`. Не удалось определить статус.
`IsDevControlRunning`	Статус компонента Контроль устройств.	Возможные значения: • `True`. Компонент Контроль устройств включен и выполняет функции защиты. • `False`. Компонент Контроль устройств не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.
`IsKSNRunning`	Статус компонента Kaspersky Security Network.	Возможные значения: • `True`. Компонент Kaspersky Security Network включен и выполняет функции защиты. • `False`. Компонент Kaspersky Security Network не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.
`IsOASRunning`	Статус компонента Постоянная защита файлов.	Возможные значения: • `True`. Компонент Постоянная защита файлов включен и выполняет функции защиты. • `False`. Компонент Постоянная защита файлов не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.

Указанные данные являются свойствами экземпляра класса `KasperskySecurity_ProductInfo.ProductName=Kaspersky Industrial CyberSecurity for Nodes`, где:

- `KasperskySecurity_ProductInfo` – имя класса Kaspersky Industrial CyberSecurity for Nodes;
- `.ProductName=Kaspersky Industrial CyberSecurity for Nodes` – ключевые свойства Kaspersky Industrial CyberSecurity for Nodes.

Экземпляр класса создается в пространстве имен `ROOT\Kaspersky\Security`.

Обновление баз и модулей Kaspersky Industrial CyberSecurity for Nodes

Этот раздел содержит информацию о задачах обновления и отката обновлений Kaspersky Industrial CyberSecurity for Nodes, а также инструкции по настройке задач.

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

Об обновлении баз и модулей приложения

Обновление баз и модулей приложения Kaspersky Industrial CyberSecurity for Nodes обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие приложения, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Industrial CyberSecurity for Nodes. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули приложения.

Для регулярного обновления требуется действующая лицензия на использование приложения. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Kaspersky Industrial CyberSecurity for Nodes загружает обновления баз и модулей приложения с HTTP- или FTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или из других источников обновлений.

Вы можете загружать обновления на каждое защищаемое устройство или использовать одно защищаемое устройство в качестве посредника. На него будут копироваться обновления, а затем распространяться на защищаемые устройства. Если вы используете программу Kaspersky Security Center для централизованного управления защитой устройств в организации, вы можете использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Если загрузка обновлений прервется или завершится с ошибкой, Kaspersky Industrial CyberSecurity for Nodes автоматически вернется к использованию баз с последними установленными обновлениями. В случае повреждения баз Kaspersky Industrial CyberSecurity for Nodes можно вручную откатить базы до ранее установленных обновлений.

В процессе обновления на ваш компьютер загружаются и устанавливаются следующие объекты:

- Базы Kaspersky Industrial CyberSecurity for Nodes. Защита компьютера обеспечивается на основании баз данных, содержащих сигнатуры вирусов и других приложений, представляющих угрозу, и информацию о способах борьбы с ними. Компоненты защиты используют эту информацию при поиске и обезвреживании зараженных файлов на компьютере. Базы регулярно пополняются записями о появляющихся угрозах и способах борьбы с ними. Поэтому рекомендуем регулярно обновлять базы.

  Наряду с базами Kaspersky Industrial CyberSecurity for Nodes обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

- Модули приложения. Обновления модулей приложения устраняют уязвимости Kaspersky Industrial CyberSecurity for Nodes, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули приложения на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули приложения отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Информация о текущем состоянии баз Kaspersky Industrial CyberSecurity for Nodes отображается в главном окне приложения или в подсказке при наведении курсора на значок приложения в области уведомлений.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в журнал выполнения задачи обновления.

О задачах обновления

В Kaspersky Industrial CyberSecurity for Nodes предусмотрены две задачи обновления: *Обновление* и *Откат обновления*.

Обновление

По умолчанию Kaspersky Industrial CyberSecurity for Nodes копирует базы и, если имеются, модули приложения из источника обновлений на устройство и сразу переходит к их использованию в компонентах защиты. Задачи проверки по требованию переходят к использованию обновленных баз приложения при последующем их запуске.

Вы можете настраивать параметры задачи *Обновление*. После того как вы измените параметры задачи, Kaspersky Industrial CyberSecurity for Nodes применит их новые значения при следующем запуске задачи.

По умолчанию для задачи *Обновление* установлен режим запуска **Вручную**. Вы не можете приостанавливать и возобновлять задачи обновления.

Откат обновления

В ходе выполнения задачи Kaspersky Industrial CyberSecurity for Nodes возвращается к использованию предыдущих баз и модулей приложения.

По умолчанию задача *Откат обновления* не выполняется.

Схемы обновления баз и модулей Kaspersky Industrial CyberSecurity for Nodes

Выбор источника обновлений в задаче *Обновление* зависит от используемой в организации схемы обновления баз и модулей приложения.

Вы можете обновлять базы и модули Kaspersky Industrial CyberSecurity for Nodes на защищаемых устройствах по следующим схемам:

- Загружать обновления напрямую из интернета на каждое защищаемое устройство (схема 1).
- Загружать обновления из интернета на устройство-посредник и распределять обновления на защищаемые устройства с этого устройства.

  Посредником может служить любое устройство, на котором установлены следующие приложения:

  - Kaspersky Industrial CyberSecurity for Nodes (схема 2).
  - Сервер администрирования Kaspersky Security Center (схема 3).

  > Обновление через устройство-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность защищаемых устройств в сети.

- Загружать обновления баз приложения на каждое защищаемое устройство с помощью безопасного съемного диска (схема 4).

Перечисленные схемы обновлений описаны ниже.

Схема 1. Обновление баз и модулей приложения напрямую из интернета

Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes напрямую из интернета,

на каждом защищаемом устройстве в параметрах задачи *Обновление* укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений.

Вы можете указать в качестве источников обновлений другие HTTPS- или HTTP-серверы, на которых имеется папка обновлений.

Схема 1: Обновление баз и модулей приложения напрямую из интернета

Схема 2. Обновление баз и модулей приложения через одно из защищаемых устройств

Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes через одно из защищаемых устройств, выполните следующие действия:

1. Скопируйте обновления на выбранное защищаемое устройство:

   - На выбранном защищаемом устройстве настройте параметры задачи *Обновление*:

     a. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".

     b. Укажите папку общего доступа в качестве папки, в которой будут сохранены обновления.

2. Распределите обновления на остальные защищаемые устройства:

   - На каждом из защищаемых устройств настройте параметры задачи *Обновление*:

     a. В качестве источника обновлений укажите папку на диске устройства-посредника, в которую будут загружаться обновления.

Kaspersky Industrial CyberSecurity for Nodes будет получать обновления через одно из защищаемых устройств.

Схема 2: Обновление баз и модулей приложения через одно из защищаемых устройств

Схема 3. Обновление баз и модулей приложения через Сервер администрирования Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств, можно загружать обновления с помощью Сервера администрирования Kaspersky Security Center, установленного в локальной сети.

Схема 3: Обновление баз и модулей приложения через Сервер администрирования Kaspersky Security Center

Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes через Сервер администрирования Kaspersky Security Center, выполните следующие действия:

1. На каждом из защищаемых устройств установите Агент администрирования – программный компонент, входящий в комплект поставки Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве. Подробная информация об Агенте администрирования и его настройке с помощью Kaspersky Security Center приведена в справке Kaspersky Security Center.

2. Загрузите обновления с серверов обновлений "Лаборатории Касперского" на Сервер администрирования Kaspersky Security Center:

   - Настройте задачу *Загрузка обновлений в хранилище Сервера администрирования* для указанного набора защищаемых устройств:

     a. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".

3. Распределите обновления на защищаемые устройства. Для этого выполните одно из следующих действий:

   - Настройте на Сервере администрирования Kaspersky Security Center групповую задачу *Обновление* для распределения обновлений на защищаемые устройства:
   - Настройте на каждом из защищаемых устройств задачу *Обновление*:

     a. В качестве источника обновлений укажите Сервер администрирования Kaspersky Security Center.

     b. Если требуется, настройте расписание задачи.

Kaspersky Industrial CyberSecurity for Nodes будет получать обновления через Сервер администрирования Kaspersky Security Center.

Схема 4. Обновление баз приложения с помощью защищенного съемного диска

Чтобы обновить базы Kaspersky Industrial CyberSecurity for Nodes с помощью защищенного съемного диска, выполните следующие действия:

1. Подключите защищенный съемный диск к устройству, на котором установлено приложение Kaspersky Industrial CyberSecurity for Nodes и имеется доступ к обновлениям баз приложения.
2. Добавьте разрешающее правило компонента Контроль устройств для подключенного съемного диска.
3. В Консоли приложения настройте и выполните задачу *Безопасное копирование баз приложения*.
4. Подключите защищенный съемный диск с обновлениями баз к устройству, на котором требуется обновить базы приложения.
5. В Консоли приложения настройте и выполните задачу *Безопасное обновление баз приложения*.

Kaspersky Industrial CyberSecurity for Nodes получит обновленные базы приложения с защищенного съемного диска.

Настройка задачи обновления

Как настроить задачу Обновление в Консоли администрирования Kaspersky Security Center

1. В Консоли администрирования Kaspersky Security Center перейдите к параметрам локальной или групповой задачи обновления, которую вы хотите настроить.
2. Откройте раздел **Настройки**.
3. В блоке **Настройки обновления в локальном режиме** для Kaspersky Industrial CyberSecurity for Nodes, подключенного к Серверу администрирования Kaspersky Security Center, настройте использование источников обновлений:

   a. Нажмите на кнопку **Настройка**.

   Откроется окно **Обновление баз и модулей приложения**.

b. Установите флажок напротив источников обновлений, которые вы хотите использовать:

- Сервер администрирования Kaspersky Security Center
- Серверы обновлений "Лаборатории Касперского"

Если необходимо, с помощью кнопки **Добавить** добавьте пользовательский источник обновления.

c. Если вы выбираете несколько источников обновлений, с помощью кнопок **Вверх** и **Вниз** расположите источники обновлений в порядке приоритета. Kaspersky Industrial CyberSecurity for Nodes обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes использует Kaspersky Security Center в качестве первого источника обновлений. Это позволяет сократить расход трафика при обновлении. Если к компьютеру не применена политика, в параметрах локальной задачи *Обновление* выбраны серверы "Лаборатории Касперского" в качестве первого источника обновления, так как у приложения может отсутствовать доступ к Kaspersky Security Center.

d. Если в качестве источника обновлений выбран **Серверы обновлений "Лаборатории Касперского"**, выберите принцип, по которому Kaspersky Industrial CyberSecurity for Nodes будет выбирать сервер обновлений "Лаборатории Касперского":

- **Определять автоматически**. Приложение использует ближайший доступный сервер обновлений "Лаборатории Касперского".
- **Выбрать из списка**. Приложение использует сервер обновлений "Лаборатории Касперского" из выбранной в списке страны.

e. В окне **Обновление баз и модулей приложения** нажмите на кнопку **ОК**.

4. Настройте параметры обновления баз приложения:

a. Установите или снимите флажок **Загружать обновления баз приложения**.

b. Установите или снимите флажок **Снизить нагрузку на дисковую подсистему**. Флажок включает или выключает процесс оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти. По умолчанию флажок снят.

c. Если вы установили флажок **Снизить нагрузку на дисковую подсистему**, в поле **Объем оперативной памяти, используемой для оптимизации (МБ)** укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 640 МБ. Минимально допустимый объем оперативной памяти 400 МБ.

При запуске задачи *Обновление* с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций:

- Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления (например, при первом обновлении), что приведет к завершению задачи с ошибкой.

  В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

- Если указано слишком большое значение, при запуске задачи обновления может не получиться создать виртуальный диск требуемого размера в оперативной памяти. В результате функция оптимизации дисковой подсистемы автоматически отключится и задача обновления будет выполняться без оптимизации.

  В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

5. Настройте параметры обновления модулей приложения:

   a. Установите или снимите флажок **Загружать обновления модулей приложения**.

   Если флажок установлен, то Kaspersky Industrial CyberSecurity for Nodes уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи *Обновление* включает обновления модулей приложения в пакет обновлений. Тип обновлений модулей приложения, который будет применен, определяется отдельно. По умолчанию флажок установлен.

   b. Выберите тип обновлений модулей приложения, который вы хотите применять:

   - **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Industrial CyberSecurity for Nodes устанавливает критические обновления автоматически, а остальные обновления модулей приложения – после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center.

   - **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Industrial CyberSecurity for Nodes устанавливает их после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию.

   Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения, то приложение устанавливает обновление после согласия с положениями Лицензионного соглашения.

6. Настройте параметры копирования обновлений в папку для локального хранения:

   a. Установите или снимите флажок **Копировать обновления в папку для локального хранения**.

   b. Выберите содержимое обновлений, которое приложение будет копировать в папку для локального хранения:

   - **Копировать обновления баз приложения**. Приложение загружает только обновления баз.

   - **Копировать критические обновления модулей приложения**. Приложение загружает только срочные обновления модулей приложения.

   - **Копировать обновления баз и критические обновления модулей приложения**. Приложение загружает обновления баз и срочные обновления модулей приложения.

   c. Укажите локальную или сетевую папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет копировать полученные обновления.

7. Сохраните внесенные изменения.

Как настроить задачу Обновление в Консоли приложения

1. В дереве Консоли приложения откройте узел **Обновление** → **Обновление баз и модулей приложения**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Свойства: Обновление баз и модулей приложения**.

3. В блоке **Настройки обновления в локальном режиме** для Kaspersky Industrial CyberSecurity for Nodes, подключенного к Серверу администрирования Kaspersky Security Center, настройте использование источников обновлений:

   a. Нажмите на кнопку **Настройка**.

      Откроется окно **Обновление баз и модулей приложения**.

   b. Установите флажок напротив источников обновлений, которые вы хотите использовать:

      - Сервер администрирования Kaspersky Security Center
      - Серверы обновлений "Лаборатории Касперского"

      Если необходимо, с помощью кнопки **Добавить** добавьте пользовательский источник обновления.

   c. Если вы выбираете несколько источников обновлений, с помощью кнопок **Вверх** и **Вниз** расположите источники обновлений в порядке приоритета. Kaspersky Industrial CyberSecurity for Nodes обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений.

      По умолчанию Kaspersky Industrial CyberSecurity for Nodes использует Kaspersky Security Center в качестве первого источника обновлений. Это позволяет сократить расход трафика при обновлении. Если к компьютеру не применена политика, в параметрах локальной задачи *Обновление* выбраны серверы "Лаборатории Касперского" в качестве первого источника обновления, так как у приложения может отсутствовать доступ к Kaspersky Security Center.

   d. Если в качестве источника обновлений выбран **Серверы обновлений "Лаборатории Касперского"**, выберите принцип, по которому Kaspersky Industrial CyberSecurity for Nodes будет выбирать сервер обновлений "Лаборатории Касперского":

      - **Определять автоматически**. Приложение использует ближайший доступный сервер обновлений "Лаборатории Касперского".
      - **Выбрать из списка**. Приложение использует сервер обновлений "Лаборатории Касперского" из выбранной в списке страны.

   e. В окне **Обновление баз и модулей приложения** нажмите на кнопку **OK**.

4. Настройте параметры обновления баз приложения:

   a. Установите или снимите флажок **Загружать обновления баз приложения**.

   b. Установите или снимите флажок **Снизить нагрузку на дисковую подсистему**. Флажок включает или выключает процесс оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти. По умолчанию флажок снят.

c. Если вы установили флажок **Снизить нагрузку на дисковую подсистему**, в поле **Объем оперативной памяти, используемой для оптимизации (МБ)** укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 640 МБ. Минимально допустимый объем оперативной памяти 400 МБ.

При запуске задачи *Обновление* с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций:

- Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления (например, при первом обновлении), что приведет к завершению задачи с ошибкой.

  В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

- Если указано слишком большое значение, при запуске задачи обновления может не получиться создать виртуальный диск требуемого размера в оперативной памяти. В результате функция оптимизации дисковой подсистемы автоматически отключится и задача обновления будет выполняться без оптимизации.

  В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

5. Настройте параметры обновления модулей приложения:

a. Установите или снимите флажок **Загружать обновления модулей приложения**.

Если флажок установлен, то Kaspersky Industrial CyberSecurity for Nodes уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи *Обновление* включает обновления модулей приложения в пакет обновлений. Тип обновлений модулей приложения, который будет применен, определяется отдельно. По умолчанию флажок установлен.

b. Выберите тип обновлений модулей приложения, который вы хотите применять:

- **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Industrial CyberSecurity for Nodes устанавливает критические обновления автоматически, а остальные обновления модулей приложения – после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center.

- **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Industrial CyberSecurity for Nodes устанавливает их после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию.

Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения, то приложение устанавливает обновление после согласия с положениями Лицензионного соглашения.

6. Настройте параметры копирования обновлений в папку для локального хранения:

   a. Установите или снимите флажок **Копировать обновления в папку для локального хранения**.

   b. Выберите содержимое обновлений, которое приложение будет копировать в папку для локального хранения:

      - **Копировать обновления баз приложения**. Приложение загружает только обновления баз.
      - **Копировать критические обновления модулей приложения**. Приложение загружает только срочные обновления модулей приложения.
      - **Копировать обновления баз и критические обновления модулей приложения**. Приложение загружает обновления баз и срочные обновления модулей приложения.

   c. Укажите локальную или сетевую папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет копировать полученные обновления.

7. Сохраните внесенные изменения.

Как настроить задачу Обновление в Web Console

1. В Web Console перейдите к параметрам локальной или групповой задачи *Обновление*, которую вы хотите настроить.

2. Откройте раздел **Настройки**.

3. Выберите вкладку **Локальный режим** для настройки параметров задачи *Обновление* для Kaspersky Industrial CyberSecurity for Nodes, подключенного к Серверу администрирования Kaspersky Security Center.

4. Настройте использование источников обновлений:

   a. В блоке **Источники обновлений** установите флажок напротив источников обновлений, которые вы хотите использовать:

      - **Сервер администрирования Kaspersky Security Center**
      - **Серверы обновлений "Лаборатории Касперского"**

      Если необходимо, с помощью кнопки **Добавить** добавьте пользовательский источник обновления.

   b. Если вы выбираете несколько источников обновлений, с помощью кнопок **Вверх** и **Вниз** расположите источники обновлений в порядке приоритета. Kaspersky Industrial CyberSecurity for Nodes обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений.

      По умолчанию Kaspersky Industrial CyberSecurity for Nodes использует Kaspersky Security Center в качестве первого источника обновлений. Это позволяет сократить расход трафика при обновлении. Если к компьютеру не применена политика, в параметрах локальной задачи *Обновление* выбраны серверы "Лаборатории Касперского" в качестве первого источника обновления, так как у приложения может отсутствовать доступ к Kaspersky Security Center.

5. Настройте параметры обновления баз приложения:

   a. Установите или снимите флажок **Загружать обновления баз приложения**.

   b. Установите или снимите флажок **Снизить нагрузку на дисковую подсистему**. Флажок включает или выключает процесс оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти. По умолчанию флажок снят.

   c. Если вы установили флажок **Снизить нагрузку на дисковую подсистему**, в поле **Объем оперативной памяти, используемой для оптимизации (МБ)** укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 640 МБ. Минимально допустимый объем оперативной памяти 400 МБ.

      При запуске задачи *Обновление* с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций:

      - Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи (например, при первом обновлении), что приведет к завершению задачи с ошибкой.

        В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

      - Если указано слишком большое значение, при запуске задачи может не получиться создать виртуальный диск требуемого размера в оперативной памяти. В результате функция оптимизации дисковой подсистемы автоматически отключится и задача обновления будет выполняться без оптимизации.

        В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

6. Настройте параметры обновления модулей приложения:

   a. Установите или снимите флажок **Загружать обновления модулей приложения**.

      Если флажок установлен, то Kaspersky Industrial CyberSecurity for Nodes уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи *Обновление* включает обновления модулей приложения в пакет обновлений. Тип обновлений модулей приложения, который будет применен, определяется отдельно. По умолчанию флажок установлен.

   b. Выберите тип обновлений модулей приложения, который вы хотите применять:

      - **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Industrial CyberSecurity for Nodes устанавливает критические обновления автоматически, а остальные обновления модулей приложения – после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center.

      - **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей приложения Kaspersky Industrial CyberSecurity for Nodes устанавливает их после одобрения их установки, локально через интерфейс приложения или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию.

      Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения, то приложение устанавливает обновление после согласия с положениями Лицензионного соглашения.

7. Настройте параметры копирования обновлений в папку для локального хранения:

   a. Установите или снимите флажок **Копировать обновления в папку**.

   b. Выберите содержимое обновлений, которое приложение будет копировать в папку для локального хранения:

      - **Копировать обновления баз приложения**. Приложение загружает только обновления баз.
      - **Копировать критические обновления модулей приложения**. Приложение загружает только срочные обновления модулей приложения.
      - **Копировать обновления баз и критические обновления модулей приложения**. Приложение загружает обновления баз и срочные обновления модулей приложения.

   c. Укажите локальную или сетевую папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет копировать полученные обновления.

8. Сохраните внесенные изменения.

SMU-обновление приложения

Для обновления приложения через службу обновлений "Лаборатории Касперского" (Seamless Update – SMU) не нужно запускать инсталлятор в отличии от других способов обновления. Kaspersky Industrial CyberSecurity for Nodes получает новую версию приложения вместе с антивирусными базами из того же источника.

SMU-обновление позволяет обновить версию приложения на всех компьютерах организации до последней версии. Перед SMU-обновлением рекомендуется проверить новую версию приложения на нескольких компьютерах. Для этого вам нужно обновить версию приложения на компьютерах вручную (например, локально с помощью с помощью мастера установки приложения). Выбрать отдельные компьютеры для SMU-обновления приложения невозможно.

Расписание обновления приложения устанавливают специалисты "Лаборатории Касперского". Для проверки работы новой версии приложения специалисты "Лаборатории Касперского" распространяют обновления поэтапно. В результате вы можете получить SMU-обновление с задержкой до двух месяцев после выпуска новой версии.

Управление SMU-обновлением приложения осуществляется с помощью задачи *Обновление*. Для включения новой версии приложения в один пакет с антивирусными базами вам нужно включить обновление *модулей приложения* в параметрах задачи *Обновление*.

Этапы SMU-обновления приложения

1. **После выпуска новой версии или обновления модулей приложения "Лаборатория Касперского" распространяет обновление.**

2. **Пользователь одобряет обновление приложения.**

   Если компьютер подключен к Kaspersky Security Center, обновление будет доступно в консоли Kaspersky Security Center в разделе **Обновления баз и модулей приложений "Лаборатории Касперского"**. Подробнее об одобрении обновлений см. в справке Kaspersky Security Center.

   Если компьютер не подключен к Kaspersky Security Center, обновление будет доступно в Консоли приложения. Для одобрения обновления откройте раздел **Обновление** → **Обновление приложения**, выберите версию приложения и, при необходимости, примите условия соглашений.

3. **Kaspersky Industrial CyberSecurity for Nodes запускает задачу Обновление по заданному расписанию.**

В результате Kaspersky Industrial CyberSecurity for Nodes выполняет обновление версии приложения в тихом режиме.

Безопасное копирование баз приложения

Задача может быть настроена только с помощью Консоли приложения. Настройка задачи с помощью Консоли управления Kaspersky Security Center и Web Console невозможна.

Чтобы настроить параметры и запустить задачу Безопасное копирование баз приложения:

1. В дереве Консоли приложения в контекстном меню узла **Обновление** выберите **Начать безопасное копирование баз**.

   Откроется окно приветствия мастера настройки безопасного копирования баз приложения.

2. Нажмите на кнопку **Далее >**.

3. В блоке **Источник обновлений** выберите источник обновления баз приложения:

   - **Сервер администрирования Kaspersky Security Center**.

     Вы можете выбрать этот вариант, если в вашей сети управление приложениями "Лаборатории Касперского" осуществляется с помощью системы удаленного доступа Kaspersky Security Center и на защищаемом устройстве установлен Агент администрирования – компонент Kaspersky Security Center, обеспечивающий связь защищаемых устройств с Сервером администрирования.

     Этот вариант выбран по умолчанию.

   - **Серверы обновлений "Лаборатории Касперского"**.

     HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложений.

   - **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

4. Если на предыдущем шаге вы выбрали **Сервер администрирования Kaspersky Security Center,** настройте функцию **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes будет использовать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений, если Сервер администрирования Kaspersky Security Center недоступен.

5. В блоке **Настройки соединения с источниками обновлений** настройте использование прокси-сервера для соединения с источниками обновлений.

6. Нажмите на кнопку **Далее >**.

7. В раскрывающемся списке выберите подключенный безопасный съемный диск Рутокен, на который будут скопированы антивирусные базы приложения.

   Вы не можете использовать один и тот же съемный диск Рутокен одновременно для создания Portable Auditor и для безопасного копирования баз приложения.

   В качестве безопасного съемного диска может быть использован только съемный диск Рутокен, для которого добавлено разрешающее правило компонента Контроль устройств.

8. В блоке **Настройки безопасности** в поле **Введите текущий PIN-код администратора** введите PIN-код администратора, который был установлен на съемном диске Рутокен для защиты его содержимого от чтения, копирования и записи потенциальными злоумышленниками.

9. Если вы хотите изменить текущий PIN-код администратора:

   a. Установите флажок **Изменить текущий PIN-код администратора (допускаются только цифры и латинские символы)**.

   b. Введите новый PIN-код.

   c. Повторите новый PIN-код.

10. Задайте PIN-код пользователя. Этот PIN-код потребуется сотруднику, который будет обновлять базы приложения с помощью задачи *Безопасное обновление баз приложения* и выбранного съемного диска Рутокен:

    a. Введите PIN-код пользователя.

    b. Повторите PIN-код пользователя.

11. Нажмите на кнопку **Далее >**.

Безопасное копирование баз приложения на съемный диск Рутокен будет запущено. Настройки будут сохранены и применены во время выполнения задачи.

Не рекомендуется подключать к одному устройству два съемных дисках Рутокен и одновременно запускать безопасное копирование баз приложения и создание Portable Auditor. В таком случае выполнение этих задач может завершаться с ошибкой.

Безопасное обновление баз приложения

Задача *Безопасное обновление баз приложения* необходима для обновления баз приложения в закрытом контуре организации на устройствах, не имеющих доступа к базам приложения, с помощью безопасного съемного диска, защищенного от чтения, копирования и записи потенциальными злоумышленниками.

Задача может быть запущена только с помощью Консоли приложения, установленной на том же устройстве, что и Kaspersky Industrial CyberSecurity for Nodes. Настройка задачи в Консоли администрирования и Web Console невозможна.

Чтобы запустить задачу Безопасное обновление баз приложения:

1. В дереве Консоли приложения в контекстном меню узла **Обновление** выберите **Начать безопасное обновление баз**.

   Откроется окно приветствия мастера настройки безопасного обновления баз приложения.Нажмите на кнопку **Далее >**.

2. В раскрывающемся списке выберите подключенный безопасный съемный диск, на который записаны антивирусные базы приложения.

   В качестве безопасного съемного диска может быть использован только съемный диск Рутокен, для которого добавлено разрешающее правило компонента Контроль устройств.

3. Введите PIN-код съемного диска Рутокен, заданный на этапе копирования баз приложения.

4. Нажмите на кнопку **Завершить**.

Безопасное обновление баз приложения будет запущено. Базы приложения будут скопированы со съемного диска Рутокен.

Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes

Перед обновлением баз Kaspersky Industrial CyberSecurity for Nodes создает резервные копии баз, которые использовались ранее. Если обновление было прервано или завершилось с ошибкой, Kaspersky Industrial CyberSecurity for Nodes автоматически возвращается к использованию ранее установленных баз.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу *Откат последнего обновления*.

Чтобы запустить задачу Откат последнего обновления:

1. В дереве Консоли приложения откройте раздел **Обновление** → **Откат последнего обновления**.

2. В панели результатов нажмите на ссылку **Запустить**.

Статистика задачи Обновление

Во время выполнения задачи Обновление отображается актуальная информация об объеме данных, загруженных с момента запуска задачи, а также прочая информация о выполнении задачи.

После завершения или остановки задачи эта информация доступна в журнале выполнения задачи.

Чтобы просмотреть статистику задачи Обновление:

1. В дереве Консоли приложения откройте раздел **Обновление** → **Обновление баз и модулей приложения**.

2. В панели результатов в блоке **Статистика** отобразится информация об общем объеме полученных данных.

Решения Detection and Response

Решения Detection and Response от "Лаборатории Касперского" представляют собой системы безопасности, предназначенные для обнаружения сложных угроз и признаков атак на разных уровнях инфраструктуры организации. Решения Detection and Response предоставляют вам информацию об обнаруженной угрозе и позволяют управлять действиями по реагированию на обнаружения.

Таким образом, решения Detection and Response выполняют следующие действия:

- Получение данных о работе компьютера, сервера или других устройств (телеметрия).
- Автоматический анализ данных для выявления угроз.
- Формирование деталей алерта в виде граф цепочки развития угрозы для анализа и выбора действий по реагированию на обнаружение.
- Выполнение действий по реагированию на обнаружение (например, сетевая изоляция компьютера).

Kaspersky Industrial CyberSecurity for Nodes обеспечивает работу решений Detection and Response с помощью встроенного в приложение агента *Endpoint Agent* (далее также *встроенный агент*). Встроенный агент отправляет телеметрию на серверы решений и выполняет действия по реагированию на обнаружение. Встроенный агент обеспечивает работу следующих решений:

- Kaspersky Managed Detection and Response (MDR);
- Kaspersky Industrial CyberSecurity Endpoint Detection and Response;
- Kaspersky Endpoint Detection and Response Expert (on-premise);
- Kaspersky Anti Targeted Attack Platform (только отправка телеметрии).

Kaspersky Industrial CyberSecurity Endpoint Detection and Response

Kaspersky Industrial CyberSecurity Endpoint Detection and Response – это решение, предназначенное для защиты IT-инфраструктуры организации от сложных киберугроз. Функционал решения сочетает автоматическое обнаружение угроз с возможностью реагировать на эти угрозы для противостояния сложным атакам, в том числе новым эксплойтам (англ. exploits), программам-вымогателям (англ. ransomware), бесфайловым атакам (англ. fileless attacks), а также методам, использующим законные системные инструменты.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response выполняет обзор и анализ развития угрозы и предоставляет сотруднику службы безопасности или администратору информацию о потенциальной атаке, необходимую для принятия своевременных действий по реагированию, или автоматически применяет заданные вами действия по реагированию.

Пользователям с лицензией Kaspersky Security для бизнеса Профессиональный доступна дополнительная функциональность Kaspersky Industrial CyberSecurity Endpoint Detection and Response, расширяющая возможности анализа и реагирования:

- Отправка файла из карантина в Kaspersky TIP.
- Действия по реагированию для пользователей Active Directory из деталей алерта.
- Назначение учебных курсов Kaspersky ASAP пользователям из деталей алерта.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в решении на территории США.

Архитектура решения

В состав решения Kaspersky Industrial CyberSecurity Endpoint Detection and Response входят следующие компоненты:

- EPP-приложение "Лаборатории Касперского" (Kaspersky Industrial CyberSecurity for Nodes или Kaspersky Industrial CyberSecurity for Linux Nodes) с поддержкой функциональности Kaspersky Industrial CyberSecurity Endpoint Detection and Response, которое устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации. Это приложение осуществляет постоянное наблюдение за процессами, запущенными на защищаемых устройствах, открытыми сетевыми соединениями и изменяемыми файлами.
- Kaspersky Endpoint Agent – приложение, осуществляющее постоянный контроль и передачу информации о процессах, открытых сетевых соединениях и изменяемых файлах на устройстве в Kaspersky Industrial CyberSecurity for Nodes версии с 3.1 до 4.0 включительно. Kaspersky Endpoint Agent не требуется устанавливать, если вы используете Kaspersky Industrial CyberSecurity for Linux Nodes или Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и выше.
- Решение для централизованного управления сетевой безопасностью (Kaspersky Security Center).
- Средства анализа угроз (англ. Threat Intelligence):
  - Инфраструктура облачных служб Kaspersky Security Network (далее также KSN), предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.
  - Интеграция с решением Kaspersky Private Security Network (далее также KPSN), предоставляющим возможность получать доступ к репутационным базам KSN, а также другим статистическим данным, не отправляя в KSN данные со своих устройств.

- Интеграция с веб-порталом Kaspersky Threat Intelligence Portal, которая содержит и отображает информацию о репутации файлов и веб-адресов. Интеграция с Kaspersky Threat Intelligence Portal позволяет:
  - Искать дополнительную информацию об объектах в деталях алерта.
  - Отправлять файл из карантина на анализ угроз (при использовании расширенных возможностей Kaspersky Industrial CyberSecurity Endpoint Detection and Response).
- База угроз Kaspersky Threats.

Мультитенантность

Режим мультитенантности – это режим работы, при котором решение используется для защиты инфраструктуры нескольких организаций одновременно.

Вы можете использовать Kaspersky Industrial CyberSecurity Endpoint Detection and Response для защиты инфраструктуры нескольких организаций одновременно с помощью Kaspersky Security Center. Для этого вам требуется в рамках физического Сервера администрирования организации-провайдера создать виртуальные Серверы администрирования организаций, для защиты которых вы хотите использовать Kaspersky Industrial CyberSecurity Endpoint Detection and Response. Подробнее о создании виртуальных Серверов администрирования см. в справке Kaspersky Security Center.

Для каждой организации-тенанта требуется создать отдельный виртуальный Сервер администрирования. Администратор физического Сервера администрирования может управлять решением на всех устройствах, которые управляются этим Сервером. Администратор виртуального Сервера администрирования может управлять решением только на устройствах, подключенных к Серверу, который он администрирует.

Совместимость с приложениями "Лаборатории Касперского"

Kaspersky Industrial CyberSecurity Endpoint Detection and Response работает со следующими версиями приложений "Лаборатории Касперского":

- Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5 и выше.

  С Kaspersky Industrial CyberSecurity for Linux® Nodes необходимо использовать следующие версии Kaspersky Security Center:
  - Kaspersky Security Center Windows версии 14.2 и выше.
  - Kaspersky Security Center Linux 15.1 и выше.
- Kaspersky Industrial CyberSecurity for Nodes версии 3.1 и выше.

  При работе с Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0 включительно для работы решения Kaspersky Industrial CyberSecurity for Nodes дополнительно требуется установка Kaspersky Endpoint Agent. Kaspersky Endpoint Agent устанавливается на отдельные устройства, входящие в IT-инфраструктуру организации и работающие под управлением операционной системы Microsoft® Windows®. Приложение обеспечивает поддержку Kaspersky Industrial CyberSecurity Endpoint Detection and Response для Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Industrial CyberSecurity Endpoint Detection and Response поддерживает работу с Kaspersky Endpoint Agent версии 3.13 и выше.

  В Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и выше добавлен встроенный агент для работы в составе решения Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

С указанными версиями Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Endpoint Agent необходимо использовать следующие версии Kaspersky Security Center:

- Kaspersky Security Center версии с 10.5 до 12.1 – ограниченная поддержка функциональности Kaspersky Industrial CyberSecurity Endpoint Detection and Response (вы можете уточнить информацию о работе Kaspersky Industrial CyberSecurity Endpoint Detection and Response с разными версиями Kaspersky Security Center у партнера "Лаборатории Касперского", у которого вы приобрели лицензию).
- Kaspersky Security Center Windows версии 12.1 и выше – полная поддержка функциональности Kaspersky Industrial CyberSecurity Endpoint Detection and Response.
- Kaspersky Security Center Linux версии 15.1 и выше.

Расширенная функциональность Kaspersky Industrial CyberSecurity Endpoint Detection and Response для пользователей с лицензией Kaspersky Security для бизнеса Профессиональный совместима со следующими версиями приложений "Лаборатории Касперского":

- Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и выше.
- Kaspersky Security Center Linux версии 15.4 и выше, с установленным плагином Endpoint Detection and Response версии 15.4 и выше.

Развертывание и первоначальная настройка решения

Для работы Kaspersky Industrial CyberSecurity Endpoint Detection and Response должны быть выполнены следующие условия:

- Установлена поддерживаемая версия Kaspersky Security Center с Web Console.

  Подробную информацию об установке Kaspersky Security Center см. в справках Kaspersky Security Center и Kaspersky Security Center Linux.

- На защищаемых устройствах установлено приложение Kaspersky Industrial CyberSecurity for Nodes или Kaspersky Industrial CyberSecurity for Linux Nodes (информацию об установке Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Industrial CyberSecurity for Linux Nodes).

- Установлен веб-плагин управления Kaspersky Industrial CyberSecurity for Nodes или Kaspersky Industrial CyberSecurity for Linux Nodes.

  Подробную информацию об установке веб-плагинов управления см. в справке Kaspersky Security Center.

- Установлен веб-плагин Endpoint Detection and Response.

Развертывание и первоначальная настройка решения при использовании Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и выше

Сценарий развертывания и первоначальной настройки состоит из следующих этапов:

1. **Установка компонента Endpoint Detection and Response (Industrial CyberSecurity)**

   В параметрах инсталляционного пакета или мастере установки приложения, а также с помощью изменения состава компонентов приложения через Панель управления Windows на этапе выбора компонентов приложения для установки выберите **Полная функциональность** → **Endpoint Agent** → **Endpoint Detection and Response (Industrial CyberSecurity)**.

   > Для завершения изменения состава компонентов приложения необходимо перезагрузить компьютер.

2. **Активация Kaspersky Industrial CyberSecurity Endpoint Detection and Response**

3. **Включение необходимых компонентов Kaspersky Industrial CyberSecurity for Nodes**

   Убедитесь, что следующие компоненты Kaspersky Industrial CyberSecurity for Nodes включены и работают:

   - Постоянная защита файлов.
   - Защита от эксплойтов.
   - Защита от шифрования.
   - Откат вредоносных действий.

4. **Включение и настройка компонента Endpoint Detection and Response (Industrial CyberSecurity)**

   Как включить и настроить компонент Endpoint Detection and Response (Industrial CyberSecurity) в Web Console

   1. В главном окне Web Console выберите **Управление активами** → **Политики**.
   2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

      Откроется окно свойств политики.
   3. Выберите вкладку **Параметры приложения**.
   4. Выберите раздел **Серверы сбора телеметрии**.
   5. В блоке **Endpoint Detection and Response (Industrial CyberSecurity)** нажмите на кнопку **Настройка**.

      Откроется окно **Endpoint Detection and Response (Industrial CyberSecurity)**.
   6. Установите флажок **Включить Endpoint Detection and Response (Industrial CyberSecurity)**.
   7. Настройте параметры Сетевой изоляции.
   8. Настройте параметры Запрета запуска объектов.
   9. Если необходимо включите счетчик угроз, обнаруженных с помощью Cloud Sandbox, с помощью одноименного переключателя.
   10. Сохраните внесенные изменения.

Информацию о включении и настройке компонента интеграции с Kaspersky Industrial CyberSecurity Endpoint Detection and Response в Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Industrial CyberSecurity for Linux Nodes.

5. **Включение передачи данных на Сервер администрирования Kaspersky Security Center**

   Для работы всех функций Kaspersky Industrial CyberSecurity Endpoint Detection and Response должна быть включена передача следующих данных:

   - Данные о файлах карантина.

     В Web Console вы можете загрузить для анализа файлы из карантина на компьютер.

   - Данные о цепочке развития угрозы.

     В Web Console вы можете просматривать детали алерта и выполнять действия по реагированию.

   Как включить передачу данных на Сервер администрирования в Web Console

   1. В главном окне Web Console выберите **Управление активами** → **Политики**.
   2. Выберите политику, которую вы хотите настроить.
   3. В открывшемся окне **<Имя политики>** выберите вкладку **Параметры приложения**.
   4. Перейдите в раздел **Журналы и уведомления**.
   5. В блоке **Взаимодействие с Сервером администрирования** нажмите на кнопку **Настройка**.
   6. В открывшемся окне установите следующие флажки:
      - **Файлы карантина**.
      - **Цепочка развития угрозы**.
   7. Сохраните внесенные изменения.

   Для взаимодействия решения Kaspersky Industrial CyberSecurity Endpoint Detection and Response с Сервером администрирования через Kaspersky Security Center Web Console вам нужно установить новое безопасное соединение – *фоновое соединение*.

   Как установить фоновое соединение в Web Console

   1. В главном окне Web Console выберите **Параметры** → **Интеграция**.
   2. Перейдите в раздел **Интеграция**.
   3. Включите переключатель **Фоновое соединение для интеграции Включено**.
   4. Сохраните внесенные изменения.

6. **Настройка отчета об угрозах**

   Настройте отчет об угрозах для просмотра карточек инцидентов.

7. **Добавление виджета**

   Добавьте виджет EDR-алертов на информационную панель для мониторинга алертов.

8 **Отображение списка алертов**

Включите отображение раздела **Алерты** в Kaspersky Security Center Web Console.

Решение Kaspersky Industrial CyberSecurity Endpoint Detection and Response готово к использованию.

Развертывание и первоначальная настройка решения при использовании Kaspersky Industrial CyberSecurity for Nodes версии 3.1–4.0

При использовании Kaspersky Industrial CyberSecurity for Nodes версии 3.1–4.0 вам необходимо дополнительно установить и активировать Kaspersky Endpoint Agent на защищаемом устройстве, а также установить веб-плагин управления Kaspersky Endpoint Agent и создать соответствующую политику. Подробнее см. в справке Kaspersky Endpoint Agent.

Развертывание и первоначальная настройка решения при использовании Kaspersky Industrial CyberSecurity for Linux Nodes

Информацию о включении и настройке компонента интеграции с Kaspersky Industrial CyberSecurity Endpoint Detection and Response в Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Активация решения

Активация решения Kaspersky Industrial CyberSecurity Endpoint Detection and Response заключается в активации следующих приложений:

- Kaspersky Industrial CyberSecurity for Nodes.

  При использовании Kaspersky Industrial CyberSecurity for Nodes версий от 3.1 до 4.0 включительно требуется также активация приложения Kaspersky Endpoint Agent.

- Kaspersky Industrial CyberSecurity for Linux Nodes.

Эти приложения должны быть установлены на защищаемых устройствах и активированы с использованием лицензии, которая включает функциональность Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

Вы можете приобрести лицензию на использование функциональности Kaspersky Industrial CyberSecurity Endpoint Detection and Response следующими способами:

- В составе лицензии на использование Kaspersky Industrial CyberSecurity for Nodes.

  В этом случае использование Kaspersky Industrial CyberSecurity Endpoint Detection and Response станет доступно после того, как вы выполните первоначальную настройку решения.

- Отдельно, в дополнение к ранее приобретенной лицензии на использование Kaspersky Industrial CyberSecurity for Nodes.

  Если вы приобрели лицензию на использование Kaspersky Industrial CyberSecurity Endpoint Detection and Response отдельно, уже после установки и активации приложения Kaspersky Industrial CyberSecurity for Nodes на устройства, то вам нужно активировать Kaspersky Industrial CyberSecurity for Nodes (при использовании приложения версии от 3.1 до 4.0 включительно – также приложение Kaspersky Endpoint Agent) с помощью нового кода активации или файла ключа.

После активации приложений требуется выполнить первоначальную настройку решения.

Активация расширенной функциональности Kaspersky Industrial CyberSecurity Endpoint Detection and Response заключается в активации Kaspersky Security Center Linux лицензией Kaspersky Security для бизнеса Профессиональный.

Вы можете приобрести лицензию Kaspersky Security для бизнеса Профессиональный для использования расширенной функциональности Kaspersky Industrial CyberSecurity Endpoint Detection and Response следующими способами:

- В составе лицензии на использование EPP-приложений и Kaspersky Security Center.

  В этом случае использование решения станет доступно после того, как вы выполните первоначальную настройку решения.

- Отдельно, в дополнение к ранее приобретенной лицензии на использование Kaspersky Security Center.

  Если вы приобрели лицензию Kaspersky Security для бизнеса Профессиональный отдельно, уже после установки и активации приложений "Лаборатории Касперского" на устройствах, вам необходимо активировать Kaspersky Security Center Linux повторно с помощью нового кода активации или файла ключа. После этого необходимо выполнить первоначальную настройку решения.

Подробнее об активации решения см. в справке приложений "Лаборатории Касперского":

- Kaspersky Security Center.
- Kaspersky Industrial CyberSecurity for Linux Nodes.
- Kaspersky Endpoint Agent.

Настройка отчета об угрозах для отображения деталей алертов

Чтобы настроить возможность перейти в окно деталей алерта из отчета об угрозах:

1. В главном окне Web Console перейдите в раздел **Мониторинг** → **Отчеты**.
2. В списке отчетов установите флажок напротив отчета шаблона **Отчет об угрозах** и нажмите на кнопку **Открыть свойства шаблона отчета**.
3. В открывшемся окне изменения отчета перейдите на вкладку **Поля**.
4. Убедитесь, что в блоке параметров **Детальные данные** в списке полей отчета присутствует поле с именем **Открыть алерт**.
5. Если поле **Открыть алерт** отсутствует в списке, выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.
   b. В правой части окна в раскрывающемся списке выберите поле с именем **Открыть алерт**.
   c. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**.

Добавление виджета EDR-алертов

В виджете EDR-алертов отображается информация о количестве алертов на устройствах за последний месяц. Виджет доступен для отображения на вкладке **Панель мониторинга** в Kaspersky Security Center Web Console. Из виджета вы можете перейти в раздел **Алерты** со списком алертов на устройствах.

Чтобы добавить виджет EDR-алертов на информационную панель:

1. Перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
3. В списке доступных виджетов выберите виджет **Алерты** в категории **Статистика угроз**.
4. Нажмите на кнопку **Добавить**.

   Веб-виджет будет добавлен в конец информационной панели.

Подробнее о работе с виджетами см. в справке Kaspersky Security Center.

Проверка работоспособности решения на устройствах

Функциональность Kaspersky Security Center позволяет получить информацию о текущем статусе защиты на устройствах и о том, на каких устройства в вашей инфраструктуре не установлено EPP-приложение с поддержкой Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

Вы можете получить эту информацию, построив выборку устройств по статусу компонента Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

Чтобы построить выборку устройств, выполните следующие действия:

1. В Kaspersky Security Center Web Console перейдите в раздел **Управление активами** → **Выборки устройств**.
2. Создайте новую выборку устройств со следующим условием:

   a. Выберите раздел **Информация о приложениях "Лаборатории Касперского"**.

   b. В списке **Компоненты приложения** выберите один из следующих вариантов:

   - Компонент **Endpoint Detection and Response (Industrial CyberSecurity)** для Kaspersky Industrial CyberSecurity for Nodes версии 4.5 или выше.
   - Компонент **Endpoint Detection and Response Optimum** для Kaspersky Endpoint Agent (если на устройстве установлено приложение Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0).
   - Компонент **Интеграция с Kaspersky Industrial CyberSecurity Endpoint Detection and Response** для Kaspersky Industrial CyberSecurity for Linux Nodes.

c. В раскрывающемся списке **Статус** выберите необходимое значение критерия выборки, чтобы отобразить устройства с этим статусом работы.

d. Нажмите на кнопку **Сохранить**.

Новая выборка отобразит список устройств с выбранным статусом работы решения Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

Переход на Kaspersky Industrial CyberSecurity Endpoint Detection and Response с расширенной функциональностью

Если вы приобрели лицензию Kaspersky Security для бизнеса Профессиональный, вы можете использовать Kaspersky Industrial CyberSecurity Endpoint Detection and Response с расширенной функциональностью.

Переход на Kaspersky Industrial CyberSecurity Endpoint Detection and Response с расширенной функциональностью включает в себя следующие этапы:

1. **Обновление Kaspersky Security Center Linux до версии 15.4 или выше, включая компоненты приложения Агент администрирования на компьютерах пользователей и Kaspersky Security Center Web Console для Linux**

   Подробнее см. в справке Kaspersky Security Center.

2. **Обновление EPP-приложений на защищаемых устройствах до версии, поддерживающей работу с Kaspersky Industrial CyberSecurity Endpoint Detection and Response с расширенной функциональностью**

3. **Установка веб-плагина Endpoint Detection and Response версии 15.4 и выше в Kaspersky Security Center**

   Подробную информацию об установке веб-плагинов см. в справке Kaspersky Security Center.

4. **Активация лицензии Kaspersky Security для бизнеса Профессиональный**

5. **Настройка интеграции с Active Directory для реагирования на угрозы**

   Подробную информацию о настройке интеграции см. в справке Kaspersky Security Center.

6. **Настройка интеграции с Kaspersky Automated Security Awareness Platform для реагирования на угрозы**

   Подробную информацию о настройке интеграции см. в справке Kaspersky Security Center.

7. **Настройка интеграции с Kaspersky Threat Intelligence Portal для реагирования на угрозы**

   Подробную информацию о настройке интеграции см. в справке Kaspersky Security Center.

Действия по реагированию

Этот раздел содержит информацию о действиях по реагированию на обнаруженные угрозы, доступных в рамках Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

Сетевая изоляция устройства

Kaspersky Industrial CyberSecurity Endpoint Detection and Response предоставляет возможность изолировать устройства от сети по требованию (вручную) или в качестве автоматического действия по реагированию на обнаруженные угрозы.

При автоматическом реагировании на устройствах будут выполнены соответствующие команды без подтверждения оператором. Несмотря на использование стандартных механизмов ОС, возможно возникновение непредвиденных проблем, вызванных неправильной или узкоспециализированной настройкой устройств, проблем совместимости или ошибок в программном обеспечении устройств и автоматизированных систем управления технологическим процессом (далее "АСУ ТП"), которые не проявляются при обычном использовании. Например, возможно появление следующих проблем: выключение устройства; потеря связи с устройством; потеря работоспособности устройства; другие сбои в работе решения и оборудования. Также возможно непреднамеренное влияние на работу АСУ ТП.

Администратор Kaspersky Industrial CyberSecurity Endpoint Detection and Response несет полную ответственность за влияние автоматических действий решения в отношении обнаруженных угроз на стабильность работы АСУ ТП и технологического процесса.

После включения сетевой изоляции приложение разрывает все активные соединения TCP/IP и блокирует все новые сетевые соединения TCP/IP на устройствах, кроме следующих соединений:

- соединения, указанные в исключениях из сетевой изоляции;
- соединения, инициированные службами Kaspersky Industrial CyberSecurity for Nodes или Kaspersky Industrial CyberSecurity for Linux Nodes;
- соединения, инициированные Агентом администрирования Kaspersky Security Center.

Управление сетевой изоляцией доступно из Web Console.

Способы работы с сетевой изоляцией

Доступны следующие способы работы с сетевой изоляцией:

- Автоматическое включение сетевой изоляции при обнаружении IOC.
- Включение сетевой изоляции для устройства вручную.
- Включение сетевой изоляции из карточки деталей алерта.
- Отключение сетевой изоляции для устройства вручную.
- Настройка интервала сетевой изоляции с помощью политики Kaspersky Industrial CyberSecurity.
- Настройка интервала сетевой изоляции для устройства.

Автоматический режим Сетевой изоляции

Вы можете настроить автоматическое включение Сетевой изоляции, в результате реагирования на обнаружение IOC. Для настройки автоматического режима Сетевой изоляции предназначена групповая политика.

Как настроить автоматическое включение Сетевой изоляции компьютера при обнаружении IOC

1. В главном окне Web Console выберите **Управление активами → Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Industrial CyberSecurity for Nodes **Поиск IOC**.

   Откроется окно свойств задачи.

   Если требуется, создайте задачу *Поиск IOC*.

3. Выберите закладку **Параметры приложения**.

4. В блоке **Действия при обнаружении IOC** установите флажки **Применять действия по реагированию при обнаружении IOC** и **Изолировать компьютер от сети**.

5. Сохраните внесенные изменения.

   В результате при обнаружении IOC приложение изолирует компьютер от сети для предотвращения распространения угрозы.

Вы можете настроить автоматическое выключение Сетевой изоляции по истечении заданного периода времени. По умолчанию приложение выключает Сетевую изоляцию через 8 часов с момента включения. Также вы можете выключить Сетевую изоляцию вручную (см. инструкцию ниже). После выключения Сетевой изоляции компьютер может работать в сети без ограничений.

Как задать период выключения Сетевой изоляции компьютера в автоматическом режиме

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Серверы сбора телеметрии → Endpoint Detection and Response (Industrial CyberSecurity)** и нажмите **Настроить**.

5. В блоке **Сетевая изоляция** нажмите **Настроить разблокировку компьютера**.

6. В открывшемся окне установите флажок **Разблокировать автоматически изолированный компьютер через** и задайте период времени, по истечении которого Сетевая изоляция должна быть выключена.

7. Сохраните внесенные изменения.

Ручной режим Сетевой изоляции

Вы можете включать или выключать Сетевую изоляцию вручную. Для настройки ручного режима Сетевой изоляции предназначены свойства компьютера в Консоли администрирования Kaspersky Security Center.

Вы можете включить Сетевую изоляцию следующими способами:

- В деталях алерта.
- С помощью локальных параметров приложения.

Как вручную включить Сетевую изоляцию компьютера

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите закладку **Приложение**.
4. Нажмите на **Kaspersky Industrial CyberSecurity for Nodes**.

   Откроются локальные параметры приложения.
5. Выберите закладку **Параметры приложения**.
6. Перейдите в раздел **Серверы сбора телеметрии → Endpoint Detection and Response (Industrial CyberSecurity)** и нажмите **Настроить**.
7. В блоке параметров **Сетевая изоляция** нажмите на кнопку **Изолировать компьютер от сети**.
8. Нажмите **OK**.

Вы можете настроить автоматическое выключение Сетевой изоляции по истечении заданного периода времени. По умолчанию приложение выключает Сетевую изоляцию через 8 часов с момента включения. После выключения Сетевой изоляции компьютер может работать в сети без ограничений.

Как задать период выключения Сетевой изоляции компьютера в ручном режиме

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите закладку **Задачи**.

   Откроется список задач, доступных на компьютере.
4. Выберите задачу **Сетевая изоляция**.
5. Выберите закладку **Параметры приложения**.
6. В открывшемся окне задайте период времени, по истечении которого Сетевая изоляция должна быть выключена.
7. Сохраните внесенные изменения.

Как вручную выключить Сетевую изоляцию компьютера

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.
3. Выберите закладку **Приложение**.
4. Нажмите на **Kaspersky Industrial CyberSecurity for Nodes**.

   Откроются локальные параметры приложения.
5. Выберите закладку **Параметры приложения**.
6. Перейдите в раздел **Серверы сбора телеметрии** → **Endpoint Detection and Response (Industrial CyberSecurity)** и нажмите **Настроить**.
7. В блоке параметров **Сетевая изоляция** нажмите на кнопку **Разблокировать изолированный от сети компьютер**.
8. Сохраните внесенные изменения.

Вы также можете выключить Сетевую изоляцию локально из командной строки.

Исключения из Сетевой изоляции

Вы можете задать исключения из Сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на компьютере после включения Сетевой изоляции.

Для настройки исключений из Сетевой изоляции в приложении доступен список стандартных сетевых профилей. По умолчанию в исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент. Также вы можете изменить параметры стандартных сетевых профилей или задать исключения вручную (см. инструкцию ниже).

Исключения, заданные в свойствах политики, применяются, только если Сетевая изоляция включена приложением автоматически, в результате реагирования на обнаружение угрозы. Исключения, заданные в свойствах компьютера, применяются, только если Сетевая изоляция включена вручную в свойствах компьютера в консоли Kaspersky Security Center или в деталях алерта.

Активная политика не блокирует применение исключений из Сетевой изоляции, заданных в свойствах компьютера, так как сценарии применения этих параметров разные.

Как добавить исключение из Сетевой изоляции в автоматическом режиме

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Серверы сбора телеметрии** → **Endpoint Detection and Response (Industrial CyberSecurity)** и нажмите **Настроить**.

5. В блоке **Исключения из сетевой изоляции** нажмите **Исключения**.

6. В открывшемся окне нажмите на кнопку **Добавить из профиля** и выберите стандартные сетевые профили для настройки исключений.

   Сетевые соединения из профиля будут добавлены в список исключений из Сетевой изоляции. Вы можете просмотреть свойства сетевых соединений. При необходимости, вы можете изменить параметры сетевого соединения.

7. Если требуется, добавьте исключение из Сетевой изоляции вручную. Для этого в окне со списком исключений нажмите на кнопку **Добавить** и задайте параметры сетевого соединения вручную.

8. Сохраните внесенные изменения.

Как добавить исключение из Сетевой изоляции в ручном режиме

1. В главном окне Web Console выберите **Управление активами** → **Активы (Устройства)**.

2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.

   Откроются свойства компьютера.

3. Выберите закладку **Задачи**.

   Откроется список задач, доступных на компьютере.

4. Выберите задачу **Сетевая изоляция**.

5. Выберите закладку **Параметры приложения**.

6. В открывшемся окне нажмите **Исключения**.

7. В открывшемся окне нажмите на кнопку **Добавить из профиля** и выберите стандартные сетевые профили для настройки исключений.

   Сетевые соединения из профиля будут добавлены в список исключений из Сетевой изоляции. Вы можете просмотреть свойства сетевых соединений. При необходимости, вы можете изменить параметры сетевого соединения.

8. Если требуется, добавьте исключение из Сетевой изоляции вручную. Для этого в окне со списком исключений нажмите на кнопку **Добавить** и задайте параметры сетевого соединения вручную.

9. Сохраните внесенные изменения.

Вы также можете просмотреть список исключений из Сетевой изоляции локально из командной строки. При этом компьютер должен быть изолирован.

Тег для изолированных устройств

Для всех изолированных устройств добавляется тег ISOLATED FROM NETWORK. Тег нельзя удалить, пока устройство изолировано.

> Если вы добавите этот тег вручную, устройство не будет изолировано от сети.

Тег ISOLATED FROM NETWORK позволяет обнаружить изолированные устройства. Подробнее см. в разделе Просмотр списка изолированных устройств.

Информацию об управлении сетевой изоляцией в Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0 включительно) и Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Endpoint Agent и справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Поиск IOC

Индикатор компрометации (Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к устройству (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему.

Для поиска IOC используются IOC-файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие алертом.

В Kaspersky Industrial CyberSecurity for Nodes предусмотрена задача *Поиск IOC* – групповая или локальная задача, которая использует IOC-файлы. В случае обнаружения совпадения с индикаторами компрометации приложение выполняет заданное в свойствах задачи *Поиск IOC* действие. Доступны следующие действия по реагированию на обнаруженные IOC:

- Изолировать устройство от сети.
- Запустить проверку важных областей.
- Копию объекта поместить на карантин, объект удалить.

Вы можете создавать задачу *Поиск IOC* следующими способами:

- Из деталей алерта.
- **В Web Console.**

  1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

     Откроется список задач.

  2. Нажмите на кнопку **Добавить**.

     Запустится мастер создания задачи.

  3. Настройте параметры задачи:

     a. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.

     b. В раскрывающемся списке **Тип задачи** выберите **Поиск IOC**.

     c. В поле **Название задачи**, если необходимо, скорректируйте название задачи.

     d. В блоке **Устройства, которым будет назначена задача** выберите область действия задачи.

  4. Выберите устройства в соответствии с выбранным вариантом области действия задачи.

  5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу под системной учетной записью SYSTEM.

У системной учетной записи SYSTEM отсутствуют права на выполнение задачи *Поиск IOC* на сетевых дисках. Если вы хотите выполнить задачу на сетевом диске, выберите учетную запись пользователя, у которого есть доступ к этому диску.

6. Завершите работу мастера.

   В списке задач отобразится созданная задача.

7. Нажмите на имя созданной задачи.

   Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Перейдите в раздел **Настройки поиска IOC**.

10. Загрузите IOC-файлы для поиска индикаторов компрометации.

    Не рекомендуем добавлять или удалять IOC-файлы после запуска задачи. Это может привести к некорректному отображению результатов поиска IOC для предыдущих запусков задачи. Для поиска индикаторов компрометации по новым IOC-файлам рекомендуем создавать новые задачи.

11. Если необходимо, настройте ретроспективный поиск IOC. Режим работы задачи *Поиск IOC*, при котором Kaspersky Industrial CyberSecurity for Nodes выполняет поиск индикаторов компрометации в данных защищаемых устройств, полученных за указанный интервал времени. Приложение анализирует данные в журналах операционной системы и браузеров, установленных на защищаемом компьютере.

    Для работы задачи в режиме *Ретроспективный поиск IOC* необходимо, чтобы были загружены IOC-файлы для поиска индикаторов компрометации, включающие в себя один или несколько терминов из списка: *FileItem/**, *Network/**, *PortItem/**, *ProcessItem/**, *RegistryItem/**, *UrlHistoryItem/**.

    Выполните следующие действия:

    a. Установите флажок **Включить Ретроспективный поиск IOC**.

    b. Укажите период времени в днях, за который будет выполняться поиск. Максимальное значение – 14 дней.

       Во время выполнения задачи приложение анализирует данные, собранные за указанный вами период времени, начиная с момента запуска задачи.

       Значение по умолчанию – 1 день.

    c. В разделе **Дополнительно** свойств задачи проверьте, что установлены флажки напротив всех типов данных, упомянутых в загруженном IOC-файле.

    d. Если загруженный IOC-файл содержит индикатор компрометации с термином *Network/**, установите флажок напротив типа данных *Сетевые данные - NetworkItem*, который по умолчанию снят.

Задача *Поиск IOC* запустится в режиме ретроспективного поиска. В этом режиме приложение публикует для каждого файла результаты выполнения задачи в обычном режиме и результаты ретроспективного поиска IOC.

Kaspersky Industrial CyberSecurity for Nodes отображает поля PID и UPID только для результатов ретроспективного поиска. Также при выключенном расширенном сборе телеметрии ретроспективный поиск IOC имеет следующие ограничения:

- Приложение не заполняет поля Created, Modified, Changed, Accessed, FileAttributes для записей FileItem.
- Для существующих файлов, которые не запускались, значения полей Md5sum, Sha256sum, SizeInBytes в результатах ретроспективного сканирования равны 0.
- Для обнаруженных файлов, которые были удалены, приложение не рассчитывает хеш.

12. Если необходимо, настройте действия, которые выполняет Kaspersky Industrial CyberSecurity for Nodes при обнаружении индикатора компрометации:

    a. Установите флажок **Применять действия по реагированию при обнаружении IOC**.

    b. Установите флажки напротив действий, которые выполняет Kaspersky Industrial CyberSecurity for Nodes при обнаружении индикатора компрометации:

    - **Изолировать компьютер от сети**. Если выбран этот вариант действия, то Kaspersky Industrial CyberSecurity for Nodes изолирует компьютер от сети для предотвращения распространения угрозы. Вы можете настроить время изоляции в параметрах компонента Endpoint Detection and Response (KSC).
    - **Копию поместить на карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Industrial CyberSecurity for Nodes удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Industrial CyberSecurity for Nodes формирует его резервную копию и помещает ее на карантин.
    - **Запускать проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Industrial CyberSecurity for Nodes запускает предустановленную задачу *Проверка важных областей*.

13. Перейдите в раздел **Дополнительно**.

14. Выберите типы данных (IOC-документы), которые необходимо анализировать во время выполнения задачи.

    Kaspersky Industrial CyberSecurity for Nodes автоматически выбирает типы данных (IOC-документы) для задачи *Поиск IOC* в соответствии с содержанием загруженных IOC-файлов. Не рекомендуем самостоятельно отменять выбор типов данных.

    Для типа данных *Реестр Windows - RegistryItem* Kaspersky Industrial CyberSecurity for Nodes анализирует предустановленный набор разделов реестра.

15. Если необходимо, настройте дополнительные параметры для типа данных Файлы - FileItem:

    a. Нажмите на кнопку **IOC-документы**.

    Откроется окно **Настройки проверки файлов – FileItem**.

b. В блоке **Искать IOC в следующих областях** выберите данные, которые необходимо анализировать во время выполнения задачи.

c. В блоке **Проверять указанные области** выберите области на дисках защищаемого устройства, в которых необходимо искать индикаторы компрометации.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes выполняет поиск IOC только в важных областях компьютера, таких как папки Загрузки, Рабочий стол, папка с временными файлами операционной системы и другие. Вы можете указать пути до нужных областей самостоятельно.

d. Нажмите на кнопку **OK**.

16. Если необходимо, настройте дополнительные параметры для типа данных Журналы событий Windows - EventLogItem:

a. Нажмите на кнопку **Журналы и даты**.

Откроется окно **Настройки проверки журнала событий Windows – EventLogItem**.

b. Чтобы во время выполнения задачи не учитывать события, зафиксированные ранее определенного момента, установите флажок **Проверять только события, зафиксированные в течение указанного периода** и укажите дату и время.

c. В блоке **Проверять события, относящиеся к следующим каналам** выберите журналы событий Windows, которые необходимо анализировать во время выполнения задачи.

d. Нажмите на кнопку **OK**.

> При указании значения IOC-термина EventLogItem\source вам необходимо использовать значение параметра **Provider Name** из XML-схемы события.

17. Настройте расписание запуска задачи на вкладке **Расписание**.

18. Сохраните внесенные изменения.

19. Установите флажок напротив задачи.

20. Нажмите на кнопку **Запустить**.

- Из командной строки.

Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**. Информацию об обнаруженных индикаторах компрометации вы можете посмотреть в свойствах задачи **Параметры приложения → Результаты поиска IOC**.

Kaspersky Industrial CyberSecurity for Nodes выполняет поиск дубликатов среди записей, полученных по одному IOC-файлу, и сохраняет в результатах задачи только уникальные записи. Дубликатами считаются записи одного типа, у которых совпадают значения всех сравниваемых полей. Также приложение может не создавать записи при отсутствии у них значений **одного или нескольких полей.**

Тип	Сравниваемые поля	Условие, при котором запись не создается
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• У записи отсутствуют значения полей FullPath, Md5sum, Sha256sum. • У записей отсутствует значение поля FullPath и совпадают значения полей Md5sum, Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	У записи отсутствует значение какого-либо из следующих полей: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	У записи отсутствуют значения полей startTime или PID.

В окне **Детали алерта** могут присутствовать записи RegistryItem с одинаковыми значениями полей. Данные записи не являются дубликатами, так как различаются значением поля Text, не отображающегося в интерфейсе.

Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Industrial CyberSecurity for Nodes автоматически удаляет старые записи.

Поиск IOC прерывается при обнаружении 128 совпадений с индикаторами компрометации, описанными в IOC-файлах. Это необходимо для ограничения количества записей в отчете задачи *Поиск IOC* для удобства его анализа и защиты отчета от переполнения из-за неточно сформулированных индикаторов компрометации, для которых совпадений может быть очень много.

Подробнее о создании задачи поиска IOC в Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0) и Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Endpoint Agent и справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Требования к IOC-файлам

При создании задач поиска IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Приложение поддерживает IOC-файлы с расширением ioc и xml открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1.
- После загрузки IOC-файлов вы можете вручную изменять содержание файлов во встроенном редакторе прямо в свойствах задачи. Kaspersky Industrial CyberSecurity for Nodes поддерживает изменение содержания IOC-файлов, которые соответствуют стандарту OpenIOC версии 1.1. Изменить содержание IOC-файлов, соответствующих стандарту OpenIOC версии 1.0, невозможно.

- Если при создании задачи *Поиск IOC* из командной строки вы загрузите IOC-файлы, часть из которых не поддерживается, то при запуске задачи приложение будет использовать только поддерживаемые IOC-файлы. Если при создании задачи *Поиск IOC* из командной строки все загруженные вами IOC-файлы не поддерживаются, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации. Загрузить IOC-файлы, которые не поддерживаются, в Web Console или Cloud Console невозможно.

- Семантические ошибки и неподдерживаемые IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов приложение фиксирует отсутствие совпадения.

- Идентификаторы всех IOC-файлов, которые используются в одной задаче поиска IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.

- Размер одного IOC-файла не должен превышать 2 МБ. Использование файлов большего размера приводит к завершению задач поиска IOC с ошибкой. Суммарный размер всех добавляемых файлов в IOC-коллекции не должен превышать 10 МБ. Если размер всех файлов превышает 10 МБ, вам нужно разделить IOC-коллекцию и создать несколько задач *Поиск IOC*.

- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи *Поиск IOC*.

В файле, который можно загрузить по ссылке ниже, приведена таблица с полным списком IOC-терминов стандарта OpenIOC.

ЗАГРУЗИТЬ ФАЙЛ IOC_TERMS.XLSX

Особенности и ограничения поддержки стандарта OpenIOC приложением приведены в следующей таблице.

Особенности и ограничения поддержки стандарта OpenIOC версий 1.0 и 1.1.

Поддерживаемые условия	OpenIOC 1.0:
	
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Поддерживаемые атрибуты условий	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Поддерживаемые операторы	`AND` `OR`
Поддерживаемые типы данных	`"date"`: дата (применимые условия: `is`, `greater-than`, `less-than`) `"int"`: целое число (применимые условия: `is`, `greater-than`, `less-than`) `"string"`: строка (применимые условия: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: продолжительность в секундах (применимые условия: `is`, `greater-than`, `less-than`)

Особенности интерпретации типов данных	Типы данных `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` интерпретируются как строка (string).
	
	Приложение поддерживает интерпретацию параметра `Content` для типов данных `int` и `date`, заданного в виде промежутков:
	
	OpenIOC 1.0:
	С использованием оператора `TO` в поле `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	С помощью условий `greater-than` и `less-than`
	С использованием оператора `TO` в поле `Content`
	Приложение поддерживает интерпретацию типов данных `date` и `duration`, если индикаторы заданы в формате `ISO 8601, Zulu time zone, UTC`.

Расширенный сбор телеметрии для поиска IOC

Для ретроспективного поиска IOC рекомендуется включить расширенный сбор телеметрии на компьютере. Расширенный сбор телеметрии позволяет более точно определять индикаторы компрометации, но требует больше ресурсов компьютера.

Расширенный сбор телеметрии дополнительно включает в себя поддержку следующих терминов:

- FileItem/Md5sum;
- FileItem/Sha256sum;
- FileItem/SizeInBytes;
- FileItem/Created;
- FileItem/Modified;
- FileItem/Changed;
- FileItem/Accessed;
- FileItem/FileAttributes.

Если расширенный сбор телеметрии выключен, то Kaspersky Industrial CyberSecurity for Nodes может выполнять ротацию данных об обнаруженных индикаторах компрометации.

Чтобы включить расширенный сбор телеметрии, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Серверы сбора телеметрии** → **Endpoint Detection and Response (Industrial CyberSecurity)** и нажмите **Настроить**.

5. Установите флажок **Включить расширенное логирование активности в системе**.

6. Сохраните внесенные изменения.

Область поиска IOC в реестре (RegistryItem)

При добавлении типа данных RegistryItem в область поиска IOC, Kaspersky Industrial CyberSecurity for Nodes анализирует следующие разделы реестра:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Запуск проверки важных областей

Одно из возможных действий по реагированию при обнаружении угрозы – запуск проверки важных областей на устройстве.

Вы можете запустить проверку важных областей вручную или задать автоматический запуск проверки в качестве ответных действий на алерты.

Подробнее о проверке важных областей в Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0) и Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Endpoint Agent и справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Запрет запуска объектов

Запрет запуска объектов позволяет контролировать запуск исполняемых файлов и скриптов, а также открытие файлов офисного формата. Таким образом, вы можете, например, запретить запуск приложений, использование которых считаете небезопасным. В результате распространение угрозы может быть остановлено. Запрет запуска объектов поддерживает определенный **набор расширений файлов офисного формата** и определенный **набор интерпретаторов скриптов**

Запрет запуска объектов поддерживает следующие интерпретаторы скриптов:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe

- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Запрет запуска объектов поддерживает работу с Java-приложениями в среде выполнения Java (процессы java.exe и javaw.exe).

Kaspersky Industrial CyberSecurity for Nodes поддерживает запрет открытия файлов офисного формата через определенные приложения. Информация о поддерживаемых расширениях имен файлов и приложений приведена в следующей таблице.

Поддерживаемые расширения файлов для Запрета запуска объектов

Имя приложения	Исполняемый файл	Расширение имени файла
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Яндекс.Браузер Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

Правило запрета запуска

Запрет запуска объектов управляет доступом пользователей к файлам с помощью правил запрета запуска. *Правило запрета запуска* – это набор критериев, которые приложение учитывает при реагировании на запуск объекта, например, при блокировании запуска объекта. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Вы можете создавать правила запрета запуска следующими способами:

- В деталях алерта.

  Это действие недоступно на компьютерах под управлением ОС семейства Linux с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5.

- С помощью групповой политики или локальных параметров приложения.

  Вам нужно ввести путь к файлу или хеш файла (SHA256 или MD5), или путь к файлу и хеш файла.

Запрет запуска объектов имеет следующие ограничения:

1. Правила запрета не распространяются на файлы, расположенные на компакт-дисках или в ISO-образах. Приложение не будет блокировать исполнение или открытие этих файлов.
2. Невозможно запретить запуск критически важных системных объектов (англ. System Critical Object, SCO). К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Industrial CyberSecurity for Nodes.
3. Не рекомендуется создавать более 5000 правил запрета запуска, поскольку это может привести к нестабильности системы.

Режимы применения правил запрета запуска

Запрет запуска объектов может работать в двух режимах:

- **Информировать**

  В этом режиме Kaspersky Industrial CyberSecurity for Nodes публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

- **Блокировать**

  В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска объектов или открытия документов.

Управление запретом запуска объектов

Вы можете настроить параметры компонента только в Kaspersky Security Center Web Console или локально с помощью командной строки.

Как запретить запуск объектов в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Серверы сбора телеметрии → Endpoint Detection and Response (Industrial CyberSecurity)** и нажмите **Настроить**.

5. Установите флажок **Включить Запрет запуска объектов**.

6. В блоке **Действие при запуске или открытии объекта** выберите режим работы компонента:

   - **Блокировать**. В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Windows и Kaspersky Security Center событие о попытках запуска объектов или открытия документов.

   - **Информировать**. В этом режиме Kaspersky Industrial CyberSecurity for Nodes публикует в Журнал событий Windows и Kaspersky Security Center событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

7. Сформируйте список правил запрета запуска:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне введите имя правила запрета запуска.

   c. В раскрывающемся списке **Тип** выберите объект, который вы хотите заблокировать: **Исполняемый файл**, **Скрипт**, **Файл Microsoft Office**.

   Если вы выберите неверный тип объекта, Kaspersky Industrial CyberSecurity for Nodes не заблокирует файл или скрипт.

   d. Для добавления файла вам нужно ввести хеш файла (SHA256 или MD5) или полный путь к файлу, или хеш файла и путь к файлу.

   Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, Kaspersky Industrial CyberSecurity for Nodes не заблокирует файл или скрипт.

   e. Нажмите на кнопку **OK**.

8. Сохраните внесенные изменения.

В результате Kaspersky Industrial CyberSecurity for Nodes будет блокировать запуск объектов: запуск исполняемых файлов, скриптов и открытие файлов офисного формата. При этом вы можете, например, открыть файл скрипта в текстовом редакторе, даже если запуск скрипта запрещен. При блокировании запуска объекта Kaspersky Industrial CyberSecurity for Nodes покажет пользователю стандартное уведомление приложения, если уведомления включены в настройках приложения.

Информацию о настройке запрета запуска объектов в Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0) и Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Endpoint Agent и справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Запуск процесса

Вы можете удаленно запускать файлы с помощью задачи *Запуск процесса*. Например, вы можете удаленно запускать утилиту, которая создает файл с конфигурацией компьютера. Далее с помощью задачи *Получение файла*, вы можете получить созданный файл в Kaspersky Security Center Web Console.

Чтобы создать задачу Запуск процесса, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.

   b. В раскрывающемся списке **Тип задачи** выберите **Запуск процесса**.

   c. В поле **Название задачи** введите короткое описание задачи и нажмите **Далее**.

4. В разделе **Область действия задачи** выберите управляемые устройства и нажмите **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача.

7. Нажмите на новую задачу. Откроется окно свойств задачи.

8. Выберите закладку **Параметры приложения**.

9. Выберите раздел **Настройки запуска** и введите команду запуска процесса:

   Например, вы хотите запустить утилиту (`utility.exe`), которая сохраняет информацию о конфигурации компьютера в файл `conf.txt` в текущую папку (по умолчанию). Утилита расположена в папке `C:\Users\admin\Diagnostic\`. Конфигурационный файл необходимо сохранить в папке `C:\Users\admin\Documents\Configuration`. Введите следующие значения:

   - **Исполняемая команда** – `C:\Users\admin\Diagnostic\utility.exe`
   - **Аргументы командной строки (необязательно)** – `/R conf.txt`
   - **Путь к рабочей папке (необязательно)** – `C:\Users\admin\Documents\Configuration`

10. В окне свойств задачи выберите закладку **Расписание**.

11. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

12. Нажмите на кнопку **Сохранить**.

13. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

    В результате Kaspersky Industrial CyberSecurity for Nodes выполнит команду в тихом режиме и запустит процесс. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты выполнения**.

Подробную информацию о запуске задачи *Запуск процесса* в Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0) и Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Endpoint Agent и справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Завершение процесса

Вы можете удаленно завершать процессы с помощью задачи *Завершение процесса*. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи *Запуск процесса*.

Если вы хотите запретить запуск файла, вы можете настроить запрет запуска объектов. Вы можете запретить запуск исполняемых файлов, скриптов, файлов офисного формата.

Завершить процессы критически важных системных объектов (англ. System Critical Object, SCO) невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Industrial CyberSecurity for Nodes.

Чтобы создать задачу Завершение процесса, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.

   b. В раскрывающемся списке **Тип задачи** выберите **Завершение процесса**.

   c. В поле **Название задачи** введите короткое описание задачи и нажмите **Далее**.

4. В разделе **Область действия задачи** выберите управляемые устройства и нажмите **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача.

7. Нажмите на новую задачу. Откроется окно свойств задачи.

8. Выберите закладку **Параметры приложения**.

9. Для завершения процесса вам нужно выбрать файл, работу которого вы хотите завершить. Вы можете выбрать файл следующими способами:

   - Введите полный путь к файлу.
   - Введите хеш файла и путь к файлу.
   - Введите идентификатор процесса PID (только для локальных задач).

   Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

10. В окне свойств задачи выберите закладку **Расписание**.

11. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

12. Нажмите на кнопку **Сохранить**.

13. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

    В результате Kaspersky Industrial CyberSecurity for Nodes завершит процесс на компьютере. Например, если на компьютере запущено приложение GAME и вы завершили процесс game.exe, приложение будет закрыто без сохранения данных. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**.

Подробную информацию о запуске задачи *Завершение процесса* в Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0) и Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Endpoint Agent и справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Получение файла

Вы можете получать файлы с компьютеров пользователей. Например, вы можете настроить получение файла журнала событий, который создает стороннее приложение. Для получения файла вам нужно создать специальную задачу. В результате выполнения задачи файл будет сохранен в карантине. Вы можете загрузить этот файл на компьютер из карантина в Web Console. При этом на компьютере пользователя файл остается в исходной папке.

Для успешного выполнения задачи размер получаемого файла должен быть менее 2 ГБ.

Чтобы создать задачу Получение файла:

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.

   b. В раскрывающемся списке **Тип задачи** выберите **Получение файла**.

   c. В поле **Название задачи** введите короткое описание задачи и нажмите **Далее**.

4. В разделе **Область действия задачи** выберите управляемые устройства и нажмите **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача.

7. Нажмите на новую задачу. Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. В списке файлов нажмите на кнопку **Добавить**. Запустится мастер добавления файла.

10. Для добавления файла вам нужно ввести полный путь к файлу или контрольную сумму и путь к папке.

    Если файл расположен на сетевом диске, введите путь к файлу начиная с символов `\\`, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

11. В окне свойств задачи выберите вкладку **Расписание**. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

12. Нажмите на кнопку **Сохранить**.

13. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

В результате Kaspersky Industrial CyberSecurity for Nodes создаст копию файла и поместит копию в карантин.

Для получения копии файла в Kaspersky Endpoint Agent вам нужно создать задачу **Поместить файл на карантин** и в блоке параметров **Действия после помещения файла на карантин** указать, что файл не нужно удалять при помещении на карантин. Подробнее см. в справке Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0).

Для получения копии файла в Kaspersky Industrial CyberSecurity for Linux Nodes вам нужно создать задачу с типом **Получение файла с устройства**. Подробнее см. в справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Если вы используете приложение Kaspersky Endpoint Security 12.1 для Linux, то в результате выполнения задачи файл помещается в папку резервного хранилища Kaspersky Security Center.

Удаление файла

При интеграции Kaspersky Industrial CyberSecurity for Nodes с решением Kaspersky Industrial CyberSecurity Endpoint Detection and Response вы можете удалять файлы с защищаемого устройства с помощью задачи удаления файла.

Критически важные системные объекты (англ. System Critical Object, SCO) удалить невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Industrial CyberSecurity for Nodes.

Чтобы создать задачу Удаление файла:

1. В главном окне Web Console выберите **Управление активами** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.

   b. В раскрывающемся списке **Тип задачи** выберите **Удаление файла**.

   c. В поле **Название задачи** введите короткое описание задачи и нажмите **Далее**.

4. В разделе **Область действия задачи** выберите управляемые устройства и нажмите **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача.

7. Нажмите на новую задачу. Откроется окно свойств задачи.

8. Выберите вкладку **Параметры приложения**.

9. Для удаления файла вам нужно ввести полный путь к файлу или контрольную сумму и путь к папке.

   Если файл расположен на сетевом диске, введите путь к файлу начиная с символов \\, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку *Файл не найден*.

10. В окне свойств задачи выберите вкладку **Расписание**. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

11. Нажмите на кнопку **Сохранить**.

12. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

    В результате Kaspersky Industrial CyberSecurity for Nodes удалит файл с компьютера. Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Задача *Удаление файла* может быть завершена с ошибкой *Доступ запрещен*, если вы пытаетесь удалить запущенный исполняемый файл. Создайте задачу завершения процесса для этого файла, а затем повторите попытку.

Подробнее об удалении файлов в Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0) и Kaspersky Industrial CyberSecurity for Linux Nodes см. в справке Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0) и справке Kaspersky Industrial CyberSecurity for Linux Nodes.

Помещение файла на карантин

Одно из возможных действий по реагированию при обнаружении угрозы – помещение файла на карантин.

Карантин – это специальное локальное хранилище на устройстве с Kaspersky Industrial CyberSecurity Endpoint Detection and Response, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения. Вы можете настраивать параметры карантина. Файлы на карантине хранятся на защищаемом устройстве в зашифрованном виде и не угрожают безопасности устройства.

Вы можете поместить файл на карантин вручную или задать помещение на карантин автоматически в качестве ответных действий на алерты. Вы также можете поместить файл на карантин из окна деталей алерта.

Это действие недоступно на компьютерах под управлением ОС семейства Linux с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5.

Расширенная функциональность Kaspersky Industrial CyberSecurity Endpoint Detection and Response позволяет отправить файл, помещенный на карантин, на анализ в Kaspersky TIP. Чтобы использовать эту функцию, необходимо настроить интеграцию с Kaspersky TIP. Подробнее см. в справке Kaspersky Security Center.

Лицензия Kaspersky Security для бизнеса Профессиональный включает ограниченное количество запросов к Kaspersky TIP.

Подробнее о работе с карантином см. в справках приложений "Лаборатории Касперского":

- Справка Kaspersky Security Center.
- Справка Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0 включительно).
- Справка Kaspersky Industrial CyberSecurity for Linux Nodes.

Просмотр файлов на карантине

Чтобы просмотреть список файлов на карантине, выполните следующие действия:

в главном окне Web Console выберите **Операции** → **Хранилища** → **Карантин**.

Проверка объектов, помещенных на карантин в рамках работы Kaspersky Industrial CyberSecurity Endpoint Detection and Response, недоступна.

Объекты помещаются на карантин под системной учетной записью. При использовании Kaspersky Endpoint Agent при восстановлении из карантина файл помещается не в исходное расположение, а в специальную папку на устройстве, из которой вы сможете вручную переместить его в папку назначения.

Отправка файла из карантина в Kaspersky TIP

Лицензия Kaspersky Security для бизнеса Профессиональный включает ограниченное количество запросов к Kaspersky TIP.

Чтобы отправить файл из карантина в Kaspersky TIP:

1. В главном окне Web Console выберите **Операции** → **Хранилища** → **Карантин**.
2. Выберите файл.

   Одновременно можно отправить на анализ только один файл.
3. На панели инструментов нажмите на кнопку **Отправить на анализ угроз**.

   Kaspersky Security Center отправляет файл с управляемого устройства в Kaspersky TIP. Для этого управляемое устройство должно быть видимым в сети.

Файл отправляется в Kaspersky TIP. Чтобы увидеть результат анализа, нажмите кнопку **Просмотреть в Kaspersky TIP** в уведомлении, а затем войдите в Kaspersky TIP.

Kaspersky Security Center не сохраняет результат анализа Kaspersky TIP.

Cloud Sandbox

Cloud Sandbox – облачная технология, позволяющая обнаруживать сложные угрозы на компьютерах пользователей. Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Linux Nodes автоматически отправляют требующие проверки файлы в Cloud Sandbox для анализа. Cloud Sandbox запускает эти файлы в изолированной среде для выявления вредоносной активности и принимает решение о репутации этих файлов. Далее данные об этих файлах отправляются в Kaspersky Security Network.

Для работы Cloud Sandbox требуется включить использование Kaspersky Security Network.

Если вы используете Kaspersky Private Security Network, технология Cloud Sandbox недоступна.

Для использования технологии Cloud Sandbox на устройствах под управлением Linux требуется выполнение следующих условий:

- На устройстве установлено приложение Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 или более поздней.
- В Kaspersky Industrial CyberSecurity for Linux Nodes версии 2.0 или более поздней включена поддержка KSN.

Дополнительные сведения о поддержке Cloud Sandbox см. в справке *Kaspersky Industrial CyberSecurity for Linux Nodes*.

В Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 и более поздних версиях вы можете включить отдельный счетчик для угроз, обнаруженных с помощью Cloud Sandbox. Вы можете использовать этот счетчик для составления статистики при анализе обнаруженных угроз.

Чтобы просмотреть отчеты об алертах, обнаруженных технологией Cloud Sandbox (**Отчет об угрозах** → вкладка **Подробнее** → столбец **Обнаружено технологией Cloud Sandbox**), требуется Kaspersky Security Center Windows версии 14.2 или более поздней, Kaspersky Security Center Linux версии 15.1 или более поздней или Kaspersky Security Center Cloud Console.

Работа с деталями алерта

Этот раздел содержит информацию о действиях, которые можно выполнять непосредственно из окна деталей алерта.

О деталях алерта

Детали алерта содержат всю доступную информацию об обнаруженной угрозе и позволяют управлять действиями по реагированию на обнаружение.

В деталях алерта приведена следующая информация:

- **Граф цепочки развития угрозы**. Предоставляет жизненный цикл атаки на конечное устройство. В карточке деталей алерта отображаются два графа: сокращенный и полный.
  - Сокращенный граф содержит следующие ключевые элементы:
    - **Актив** – устройство, на котором был зарегистрирован алерт.
    - **Пользователь** – пользователь, связанный с алертом.
    - **Первопричина** – первопричина события.
    - **Обнаруженный объект** – название угрозы.
    - **Решение** – решение, принятое EPP-программой в отношении угрозы.
    - Результат выполнения действия.
  - Полный граф содержит всю цепочку событий, связанных с атакой, показывает путь эскалации атаки, процессы, задействованные в атаке, а также действия этих процессов.
- **Рекомендации**. Рекомендации по реагированию на алерт.

  Рекомендации доступны в Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5 и выше.

- **Детали алерта**. Общая информация об алерте, включая результат обработки, категорию, режим обнаружения (например, обнаружение при проверке по требованию или при автоматической проверке).
- **Устройство**. Информация о защищаемом устройстве, на котором произошло обнаружение. Например, имя устройства, IP-адрес, MAC-адрес, операционная система.
- **Процесс**. Информация о процессе, который был признан вредоносным.
- **Файл**. Информация об обнаруженном объекте.
- **Загрузка**. Информация о процессе, который обратился к сетевому ресурсу и вызвал алерт.

- **Данные из Kaspersky TIP**. Информация о репутации файла, включая группу доверия, цифровую подпись, данные о распространении файла и ссылку на аналитику алерта.

  Эта информация доступна, если в приложении Kaspersky Industrial CyberSecurity for Linux Nodes на момент регистрации алерта включена функция Kaspersky Security Network.

  > Перечисленные данные указаны на момент обнаружения угрозы. Решение не обновляет перечисленные данные, поэтому они могут отличаться от данных, отображаемых на Kaspersky Threat Intelligence Portal. Для просмотра актуальных данных воспользуйтесь ссылками на данные Kaspersky Threat Intelligence Portal в деталях алерта.

Дополнительная информация о действиях по реагированию, примененных к объектам, входящим в цепочку развития угрозы, приводится в случаях, если совместно с Kaspersky Security Center используются оба следующих приложения:

- Kaspersky Industrial CyberSecurity for Nodes версии 4.5 или более поздней.
- Веб-плагин Endpoint Detection and Response 15.4 или более поздней версии.

Из деталей алерта вы можете выполнить следующие действия по реагированию:

- Изолировать устройство, на котором произошел алерт.
- Поместить файл на карантин.

  > Это действие недоступно на компьютерах под управлением ОС семейства Linux с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5.

- Создать задачу поиска IOC.
- Запретить запуск обнаруженного файла.

  > Это действие недоступно на компьютерах под управлением ОС семейства Linux с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5.

EPP-приложения создают алерты в зависимости от событий, связанных с обнаружением угроз, и результатов обработки данных угроз. Интервал хранения событий можно настроить в EPP-программе.

> По умолчанию EPP-приложение хранит детали алертов в течение 30 дней. По истечении этого периода детали алерта автоматически удаляются.

В списке **Алерты** отображаются алерты за последние 30 дней.

Просмотр деталей алерта

Детали алерта доступны в окне со списком алертов. Список алертов доступен в отчете **Отчет об угрозах** или в подразделе **Алерты** в разделе **Мониторинг** в Kaspersky Security Center Web Console.

Если вы добавите лицензионный ключ для Kaspersky Industrial CyberSecurity Endpoint Detection and Response, подраздел **Алерты** автоматически отобразится в главном меню в разделе **Мониторинг**. Вы также можете настроить отображение подраздела **Алерты** в свойствах интерфейса в Kaspersky Security Center.

Чтобы просмотреть детали алерта, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Мониторинг → Алерты**.

   С помощью расширенной функциональности Kaspersky Industrial CyberSecurity Endpoint Detection and Response вы можете группировать похожие алерты с помощью переключателя **Агрегация алертов**.

2. Выберите алерт и нажмите на ссылку **Обогащенный**.

   Отобразятся детали алерта.

Чтобы просмотреть детали алерта в отчете об угрозах:

1. В главном окне Kaspersky Security Center Web Console перейдите в раздел **Мониторинг → Отчеты**.
2. Выберите отчет шаблона **Отчет об угрозах** и нажмите на кнопку **Показать отчет**.
3. В окне отчета на вкладке **Подробнее** выберите алерт и нажмите на ссылку **Открыть детали алерта**.

   Отобразятся детали алерта.

Чтобы открыть детали алерта, Kaspersky Industrial CyberSecurity Endpoint Detection and Response требуется получить данные с устройства, на котором произошел алерт. Если данные или устройство недоступны, отобразится сообщение об ошибке. Время ожидания ответа от устройства может занять несколько минут.

Применение и снятие сетевой изоляции

Чтобы изолировать устройство от сети из окна деталей алерта:

1. Откройте окно деталей алерта.
2. В блоке **Устройство** в раскрывающемся списке **Действия по реагированию** выберите **Изолировать устройство от сети**.

   В Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и выше можно настраивать параметры включения сетевой изоляции устройства.

3. Если вы хотите указать свой интервал сетевой изоляции, снимите флажок **Использовать параметры разблокировки по умолчанию**, а затем в поле **Разблокировать через (ч)** введите нужное количество часов.

4. Нажмите **Изолировать**.

5. Подтвердите действие.

Приложение изолирует устройство и присвоит ему тег ISOLATED FROM NETWORK.

Чтобы снять сетевую изоляцию устройства:

1. Откройте окно деталей алерта.

2. В блоке **Устройство** в раскрывающемся списке **Действия по реагированию** выберите **Снова включить устройство в сети**.

   Кнопка **Снова включить устройство в сети** доступна, если алерт получен от Kaspersky Industrial CyberSecurity for Nodes версии 4.5 или более поздней или Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5 или более поздней.

3. Подтвердите действие.

Сетевая изоляция устройства будет снята, а тег ISOLATED FROM NETWORK для него будет удален.

Подробнее о включении и выключении сетевой изоляции на устройстве и о настройке исключений из сетевой изоляции см. в следующих разделах:

- Справка Kaspersky Endpoint Agent (при использовании Kaspersky Industrial CyberSecurity for Nodes версии от 3.1 до 4.0 включительно).
- Справка Kaspersky Industrial CyberSecurity for Linux Nodes.

Помещение файла на карантин из деталей алерта

Чтобы поместить файл на карантин из деталей алерта:

1. Откройте детали алерта.

2. В блоке **Файл** в раскрывающемся списке **Действия по реагированию** нажмите на кнопку **Поместить на карантин**.

   Файл будет удален с устройства, а его копия будет помещена на карантин.

Это действие недоступно на компьютерах под управлением ОС семейства Linux с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5.

Создание задачи поиска IOC из деталей алерта

Чтобы создать задачу поиска IOC из деталей алерта:

1. Откройте детали алерта.
2. На вкладке **Все события алерта** выберите элементы списка, на основе которых вы хотите создать задачу поиска IOC.
3. Нажмите на кнопку **Создать IOC**.
4. Выберите условие срабатывания индикатора компрометации:
   - Если вы хотите, чтобы IOC срабатывал при обнаружении любого из выбранных объектов, в правой части экрана выберите **ИЛИ (любой IOC обнаружен)**.
   - Если вы хотите, чтобы IOC срабатывал только при обнаружении всех выбранных объектов, в правой части экрана выберите **И (все IOC обнаружены)**.
5. Выберите действия, которые требуется применять при срабатывании IOC:
   - Изолировать устройство от сети.
   - Запускать проверку важных областей.
   - Копию поместить на карантин, объект удалить.
6. Нажмите на кнопку **Создать задачу**.

Вы можете просмотреть созданные задачи в разделе **Устройства** → **Задачи**.

При создании задачи поиска IOC из деталей алерта для выбранного объекта (файла или процесса) будет автоматически создан IOC с термином FileItem.

Запрет запуска объекта из деталей алерта

Чтобы правила запрета запуска объекта могли применяться на устройстве, на котором произошел алерт, к этому устройству должна быть применена активная политика Kaspersky Industrial CyberSecurity for Nodes. Если устройство, на котором произошел алерт, не находится под управлением активной политики, то правило запрета запуска не будет создано.

Чтобы запретить запуск объекта из деталей алерта:

1. Откройте детали алерта.
2. В блоке **Файл** нажмите на кнопку **Запретить запуск**.

   Запуск объекта будет запрещен. Правило запрета запуска будет добавлено в политику для группы, в которую входит устройство.

Это действие недоступно на компьютерах под управлением ОС семейства Linux с установленным приложением Kaspersky Industrial CyberSecurity for Linux Nodes версии 1.5.

Действия по реагированию для пользователей Active Directory из деталей алерта

Расширенная функциональность Kaspersky Industrial CyberSecurity Endpoint Detection and Response позволяет выполнять действия по реагированию для пользователей Active Directory, затронутых или вовлеченных в алерт. Вы можете выполнять следующие действия по реагированию:

- Сброс пароля пользователя.
- Блокировка учетной записи пользователя.
- Добавление пользователя в группу безопасности.
- Удаление пользователя из группы безопасности.

Данные действия по реагированию доступны только на защищаемых устройствах с Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и выше.

Чтобы использовать эту функцию, необходимо настроить интеграцию с Active Directory. Подробнее см. в справке Kaspersky Security Center.

Сброс пароля пользователя

Для пользователя, у которого в свойствах учетной записи в Active Directory включен параметр **Пользователь не может изменять пароль**, действие по реагированию **Сбросить пароль** в Active Directory не будет выполнено.

Чтобы сбросить пароль пользователя Active Directory из деталей алерта, выполните следующие действия:

1. Откройте детали алерта.
2. Перейдите в **Детали алерта** → в группу параметров **Файл**, а затем в строке **Владелец** выберите в раскрывающемся списке пункт **Сбросить пароль**.

   Пароль пользователя в Active Directory будет сброшен.

Если в свойствах учетной записи пользователя в Active Directory включен параметр **Срок действия пароля не истекает**, после выполнения действия по реагированию **Сбросить пароль** параметр **Срок действия пароля не истекает** будет отключен, и пользователю потребуется изменить пароль домена при следующем входе в систему.

Блокировка учетной записи пользователя

Чтобы заблокировать учетную запись пользователя Active Directory из деталей алерта:

1. Откройте детали алерта.
2. Перейдите в **Детали алерта** → в группу параметров **Файл**, а затем в строке **Владелец** выберите в раскрывающемся списке пункт **Заблокировать учетную запись**.

   Учетная запись пользователя Active Directory будет заблокирована.

Добавление пользователя в группу безопасности

Чтобы добавить пользователя Active Directory в группу безопасности из деталей алерта:

1. Откройте детали алерта.
2. Перейдите в **Детали алерта** → в группу параметров **Файл**, а затем в строке **Владелец** выберите в раскрывающемся списке пункт **Добавить пользователя в группу безопасности**.

   Откроется окно **Добавить пользователя в группу безопасности**.
3. Введите полный путь к группе безопасности.
4. Нажмите на кнопку **Добавить**.

   Пользователь будет добавлен в группу безопасности. Обновление информации о группе безопасности пользователя может занять до 12 часов.

Удаление пользователя из группы безопасности

Чтобы удалить пользователя Active Directory из группы безопасности из деталей алерта:

1. Откройте детали алерта.
2. Перейдите в **Детали алерта** → в группу параметров **Файл**, а затем в строке **Владелец** выберите в раскрывающемся списке пункт **Удалить пользователя из группы безопасности**.

   Откроется окно **Удалить пользователя из группы безопасности**.

3. Введите полный путь к группе безопасности.

4. Нажмите на кнопку **Удалить**.

Пользователь будет удален из группы безопасности. Обновление информации о группе безопасности пользователя может занять до 12 часов.

Назначение учебных курсов Kaspersky ASAP пользователям из деталей алерта

Расширенная функциональность Kaspersky Industrial CyberSecurity Endpoint Detection and Response позволяет назначать из деталей алерта обучающие курсы Kaspersky Automated Security Awareness Platform для пользователей, работающих с алертами.

Чтобы использовать эту функцию, необходимо настроить интеграцию с Active Directory и Kaspersky ASAP. Дополнительную информацию можно найти в следующих статьях справки Kaspersky Security Center: Настройка интеграции с Active Directory, Настройка интеграции с Kaspersky Automated Security Awareness Platform.

Чтобы назначить учебные курсы Kaspersky ASAP из деталей алерта:

1. Откройте детали алерта.

2. Перейдите в **Детали алерта** → в группу параметров **Файл**, а затем в строке **Владелец** выберите в раскрывающемся списке пункт **Назначить курс KASAP**.

   Откроется окно **Информация о пользователе**.

3. В раскрывающемся списке **Назначить KASAP-группу** выберите для пользователя группу обучения.

Для пользователя будет назначена выбранная группа.

Вы можете просмотреть назначенный курс обучения в окне **Информация о пользователе**, в разделе **Назначенные курсы**.

Мониторинг и отчеты

Для мониторинга работы решения Kaspersky Industrial CyberSecurity Endpoint Detection and Response доступны следующие возможности:

- виджет EDR-алертов;
- список алертов;
- отчеты и выборки Kaspersky Security Center.

Просмотр списка алертов

Чтобы просмотреть все алерты в виде списка,

в Web Console перейдите в раздел **Мониторинг** → **Алерты**.

Раздел **Алерты** появляется автоматически при активации решения Kaspersky Industrial CyberSecurity Endpoint Detection and Response. Вы также можете включить отображение этого раздела в Kaspersky Security Center.

Из списка алертов вы можете перейти в детали выбранного алерта.

Просмотр информации о срабатывании правил запрета запуска

Функциональность Kaspersky Security Center позволяет получить информацию о приложениях, запуск которых был заблокирован решением Kaspersky Industrial CyberSecurity Endpoint Detection and Response в результате срабатывания правила запрета запуска объектов.

Чтобы просмотреть отчет о приложениях, запуск которых был запрещен:

1. В Web Console перейдите в раздел **Мониторинг** → **Отчеты**.
2. В списке отчетов выберите нужный отчет:
   - **Отчет о запрещенных приложениях** – чтобы просмотреть информацию о приложениях, запуск которых был запрещен в режиме блокирования и записи в отчет.
   - **Отчет о запрещенных приложениях в тестовом режиме** – чтобы просмотреть информацию о приложениях, запуск которых был запрещен в режиме только записи событий в отчет.

Просмотр списка изолированных устройств

Функциональность Kaspersky Security Center позволяет получить информацию об устройствах, к которым была применена сетевая изоляция.

Вы можете получить эту информацию, построив выборку устройств по тегу ISOLATED FROM NETWORK.

В Kaspersky Security Center Web Console вы можете построить выборку изолированных устройств на физическом Сервере администрирования только после того, как на нем хотя бы один раз была применена сетевая изоляция.

Чтобы просмотреть список устройств, изолированных от сети:

1. Перейдите в раздел **Управление активами** → **Теги** → **Теги устройств**.
2. В строке тега ISOLATED FROM NETWORK нажмите кнопку **Просмотреть устройства**.

Откроется список изолированных устройств.

Чтобы построить выборку устройств, изолированных от сети:

1. В Kaspersky Security Center Web Console перейдите в раздел **Управление активами** → **Выборки устройств**.
2. Нажмите на кнопку **Добавить**, чтобы создать выборку устройств.
3. Создайте новое условие и выберите вкладку **Теги**.
4. Нажмите **Добавить**.
5. В окне **Добавить тег** выберите **Все устройства, имеющие этот тег,** а в раскрывающемся списке **Тег** выберите значение ISOLATED FROM NETWORK.
6. Нажмите **Сохранить** во всех открытых окнах.
7. Подтвердите открытие созданной выборки.

Новая выборка отобразит список устройств, изолированных от сети.

Режим Endpoint Agent

Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent позволяет развернуть решения Detection and Response от "Лаборатории Касперского" совместно с EPP-приложениями от сторонних поставщиков. Конфигурация Endpoint Agent устанавливается на отдельные рабочие станции и серверы IT-инфраструктуры организации и осуществляет постоянное наблюдение за процессами, запущенными на компьютерах, открытыми сетевыми соединениями и изменяемыми файлами. В этом режиме компоненты защиты и контроля Kaspersky Industrial CyberSecurity for Nodes недоступны.

Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent обеспечивает работу следующих решений "Лаборатории Касперского":

- Kaspersky Managed Detection and Response;
- Kaspersky Anti Targeted Attack Platform.
- Kaspersky Endpoint Detection and Response Expert (on-premise).

Кроме того, режим Endpoint Agent включает интеграцию с приложением Kaspersky Industrial CyberSecurity for Networks и функциональность обнаружения аномалий с помощью SIGMA-правил.

Установка Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent

Установка Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent не отличается от установки Kaspersky Industrial CyberSecurity for Nodes, в параметрах инсталляционного пакета или мастере установки приложения на этапе выбора компонентов приложения для установки выберите Endpoint Agent.

После установки Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent доступна Консоль приложения, а также значок приложения в области уведомлений .

В Консоли администрирования Kaspersky Security Center компьютер с установленным приложением в режиме Endpoint Agent будет иметь статус *Критический* – . Компьютер имеет такой статус из-за отсутствия компонента Постоянная защита файлов. Никаких дополнительных действий предпринимать не требуется.

Если вам не удалось установить Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent на компьютер со сторонним EPP-приложением из-за того, что установщик обнаружил на компьютере несовместимое ПО, вы можете выключить проверку на наличие несовместимого ПО при установке приложения.

Совместимость со сторонними EPP-приложениями

Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent совместимо с EPP-приложениями от следующих поставщиков:

- **Bitdefender**

  Bitdefender Endpoint Security Tools версии 8.26.7.647.

- **Dallas Lock**

  СЗИ Dallas Lock 8.0-C версии 843.2.

- **ESET**

  ESET Endpoint Security версии 13.0.2044.0 и ESET Management Agent версии 13.2.1189.0.

- **Secret Net Studio**

  СЗИ Secret Net Studio версии 8.11 (20851).

  Невозможно установить приложение на компьютер, на котором развернуто программное обеспечение Secret Net Studio с компонентом Антивирус. Для совместной работы приложений вам нужно удалить компонент Антивирус из состава Secret Net Studio.

- **Sophos**

  Sophos Intercept X версии 2024.1.2 и выше (включая Endpoint Agent и Sophos Core Agent версии 2026.2.1.3).

- **Trend Micro**

  Trend Micro Vision One Apex One (включая Security Agent 14.0.20731).

  Trend Micro Deep Security версии 20.0.3-18160 (включая Security Agent).

- **Microsoft**

  Microsoft Defender Antivirus из состава решения Безопасность Windows (ранее – Windows Defender).

Следует устанавливать приложения в следующем порядке: сначала установите EPP-приложение, затем Агент администрирования Kaspersky Security Center, далее Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent. Это связано с тем, что установщик EPP-приложения может определить Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent и Агент администрирования как несовместимое ПО и удалить приложения. Также следует проверять работу приложения в режиме Endpoint Agent и Агента администрирования после обновления стороннего EPP-приложения, так как установщик повторно проверяет компьютер на несовместимое ПО и может удалить приложения.

Managed Detection and Response

Kaspersky Industrial CyberSecurity for Nodes поддерживает работу с решением Managed Detection and Response.

Kaspersky Managed Detection and Response (далее также MDR) обеспечивает круглосуточную защиту от растущего количества угроз, способных обойти автоматические средства защиты, для организаций, которым сложно найти квалифицированных специалистов или у которых ограничены внутренние ресурсы. В отличие от аналогичных предложений на рынке, решение использует успешный опыт эффективного исследования целевых атак для обеспечения непрерывной защиты даже от самых сложных угроз. Решение помогает повысить устойчивость компании к киберугрозам и освободить сотрудников, чтобы они могли сосредоточиться на других задачах.

MDR использует данные телеметрии, полученные от конечных точек, и машинное обучение. Данные об инцидентах MDR передает экспертам "Лаборатории Касперского". Далее эксперты могут самостоятельно обработать инцидент и, например, добавить новую запись в антивирусные базы. Или эксперты могут дать рекомендации по обработке инцидента и, например, предложить изолировать компьютер от сети. Подробную информацию о работе решения см. в справке Kaspersky Managed Detection and Response.

Конфигурации Kaspersky Industrial CyberSecurity for Nodes для работы с MDR

Для работы с MDR предусмотрены следующие конфигурации:

- **[KICS+встроенный агент]**. В этой конфигурации Kaspersky Industrial CyberSecurity for Nodes является и приложением, которое обеспечивает безопасность компьютера, и приложением для работы с MDR. Встроенный агент доступен в Kaspersky Industrial CyberSecurity for Nodes начиная с версии 4.5.

- **[стороннее EPP+KICS в режиме Endpoint Agent]**. В этой конфигурации безопасность IT-инфраструктуры обеспечивает система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Работу с MDR обеспечивает Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent. Режим Endpoint Agent доступен в Kaspersky Industrial CyberSecurity for Nodes начиная с версии 4.5.

Настройка интеграции с MDR

Интеграция с Kaspersky Managed Detection and Response состоит из следующих этапов:

1. **Установка компонента Managed Detection and Response (Industrial CyberSecurity)**

   Для интеграции Kaspersky Industrial CyberSecurity for Nodes с решением Managed Detection and Response используется компонент Managed Detection and Response (Industrial CyberSecurity). Для установки компонента в параметрах инсталляционного пакета или мастере установки приложения, а при изменении состава компонентов приложения через Панель управления Windows, выберите:

   - **Полная функциональность → Endpoint Agent → Managed Detection and Response (Industrial CyberSecurity)** для встроенного агента;
   - **Endpoint Agent → Managed Detection and Response (Industrial CyberSecurity)** для конфигурации Endpoint Agent.

   Также вы можете установить компонент с помощью задачи *Изменение состава компонентов Kaspersky Industrial CyberSecurity for Nodes*.

   > Для установки компонента Managed Detection and Response (Industrial CyberSecurity) без перезагрузки компьютера с помощью задачи *Изменение состава компонентов Kaspersky Industrial CyberSecurity for Nodes* вам необходимо выключить функцию **Проверять на наличие несовместимых приложений сторонних производителей** в настройках задачи.

2. **Настройка Kaspersky Private Security Network**

   Начиная с обновления от июля 2025 года решение Managed Detection and Response поддерживает работу без конфигурационного файла KPSN. Подробнее об использовании Kaspersky Security Network решением MDR см. справке Kaspersky Managed Detection and Response.

   Если ваша конфигурация не соответствует требованиям для работы без конфигурационных файлов KPSN, загрузите конфигурационный файл KPSN в свойствах Сервера администрирования. Конфигурационный файл KPSN находится в ZIP-архиве конфигурационного файла MDR. Также вы можете загрузить конфигурационный файл KPSN из командной строки.

   Подробнее о настройке Kaspersky Private Security Network см. в справке Kaspersky Security Center.

3. **Активация Kaspersky Managed Detection and Response**

   > При обновлении Kaspersky Industrial CyberSecurity for Nodes одной из предыдущих версий до версии 4.5 и выше решение Managed Detection and Response, активированное ранее с помощью конфигурационного файла MDR (BLOB-файла), не будет активировано автоматически. Вам необходимо повторно активировать решение Managed Detection and Response с помощью файла ключа или кода активации.

   Для активации решения Managed Detection and Response в Kaspersky Industrial CyberSecurity for Nodes вам необходима отдельная лицензия Kaspersky Managed Detection and Response for Industrial CyberSecurity Add-on.

   > Kaspersky Industrial CyberSecurity for Nodes начиная с версии 4.5 не поддерживает активацию решения Managed Detection and Response с помощью только конфигурационного файла MDR (BLOB-файла).

Если вы используете MDR-тенанты, вам нужно перед применением кода активации загрузить BLOB-файл для нужного тенанта, даже если срок действия файла истек.

Если вы не используете и никогда не создавали MDR-тенанты, загружать BLOB-файл не требуется.

Подробнее об активации решения см. в справке Kaspersky Managed Detection and Response.

4. **Включение компонента Managed Detection and Response (Industrial CyberSecurity)**

Как включить компонент Managed Detection and Response (Industrial CyberSecurity) в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. Выберите раздел **Серверы сбора телеметрии**.
4. В блоке **Managed Detection and Response (Industrial CyberSecurity)** нажмите на кнопку **Настройка**.

   Откроется окно **Managed Detection and Response (Industrial CyberSecurity)**.
5. Установите флажок **Managed Detection and Response**.
6. Если необходимо, загрузите конфигурационный файл MDR с помощью кнопки **Загрузить**. Подробную информацию о конфигурационном файле MDR см. в справке Kaspersky Managed Detection and Response.

   Загружая конфигурационный файл Managed Detection and Response, вы соглашаетесь автоматически передавать указанные данные с устройства с установленным приложением Kaspersky Industrial CyberSecurity for Nodes в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку указанных данных.
7. Сохраните внесенные изменения.

Как включить компонент Managed Detection and Response (Industrial CyberSecurity) в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Серверы сбора телеметрии**.
5. В блоке **Managed Detection and Response (Industrial CyberSecurity)** нажмите на кнопку **Настройка**.

   Откроется окно **Managed Detection and Response (Industrial CyberSecurity)**.
6. Установите флажок **Managed Detection and Response (Industrial CyberSecurity) ВЫКЛЮЧЕН**.

7. Если необходимо, загрузите конфигурационный файл MDR с помощью кнопки **Загрузить**. Подробную информацию о конфигурационном файле MDR см. в справке Kaspersky Managed Detection and Response.

   Загружая конфигурационный файл Managed Detection and Response, вы соглашаетесь автоматически передавать указанные данные с устройства с установленным приложением Kaspersky Industrial CyberSecurity for Nodes в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку указанных данных.

8. Сохраните внесенные изменения.

Как включить компонент Managed Detection and Response (Industrial CyberSecurity) в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Серверы сбора телеметрии** → **Managed Detection and Response (Industrial CyberSecurity)**.
2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Managed Detection and Response (Industrial CyberSecurity)** на вкладке **Общие**.
3. Установите флажок **Managed Detection and Response**.
4. Если необходимо, загрузите конфигурационный файл MDR с помощью кнопки **Загрузить**. Подробную информацию о конфигурационном файле MDR см. в справке Kaspersky Managed Detection and Response.

   Загружая конфигурационный файл Managed Detection and Response, вы соглашаетесь автоматически передавать указанные данные с устройства с установленным приложением Kaspersky Industrial CyberSecurity for Nodes в "Лабораторию Касперского" для обработки. Не загружайте конфигурационный файл, если вы не согласны на обработку указанных данных.

5. Сохраните внесенные изменения.

Также вы можете включить компонент Managed Detection and Response (Industrial CyberSecurity) из командной строки.

5 **Настройка других компонентов приложения для получения телеметрии**

Для работы Kaspersky Managed Detection and Response должны быть включены следующие компоненты:

- Kaspersky Security Network (расширенный режим).
- Постоянная защита файлов.
- AMSI-защита.
- Защита от шифрования.
- Защита от эксплойтов.
- Защита от сетевых угроз.
- Сетевой экран.
- Проверка по требованию.

Также для работы Kaspersky Managed Detection and Response с Сервером администрирования через Web Console Kaspersky Security Center вам нужно установить новое безопасное соединение – *фоновое соединение*. Kaspersky Managed Detection and Response предлагает установить фоновое соединение при развертывании решения. Убедитесь, что фоновое соединение установлено.

Как установить фоновое соединение в Web Console Kaspersky Security Center

1. В главном окне Web Console выберите **Параметры** → **Интеграция**.
2. Перейдите в раздел **Интеграция**.
3. Включите переключатель **Фоновое соединение для интеграции Включено**.
4. Сохраните внесенные изменения.

Kaspersky Anti Targeted Attack Platform

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

Решение Kaspersky Anti Targeted Attack Platform включает в себя три функциональных блока:

- Kaspersky Anti Targeted Attack, обеспечивающий защиту периметра IT-инфраструктуры предприятия.
- Kaspersky Endpoint Detection and Response (далее также KEDR), обеспечивающий защиту компьютеров локальной сети организации.
- Network Detection and Response, обеспечивающий защиту внутренней сети предприятия.

Подробнее о решении см. в справке Kaspersky Anti Targeted Attack Platform.

Принцип работы решения

Приложение Kaspersky Industrial CyberSecurity for Nodes устанавливается на отдельных компьютерах под управлением операционных систем Windows, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере, об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз отправляются на сервер с компонентом Central Node.

Настройка интеграции с KEDR (KATA) выполняется в Консоли администрирования Kaspersky Security Center или Kaspersky Security Center Web Console. Дальнейшее управление встроенным агентом или приложением в режиме Endpoint Agent осуществляется в консоли Kaspersky Anti Targeted Attack Platform, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Конфигурации Kaspersky Industrial CyberSecurity for Nodes для работы с Kaspersky Anti Targeted Attack Platform

Kaspersky Industrial CyberSecurity for Nodes интегрируется с Kaspersky Endpoint Detection and Response в составе решения Kaspersky Anti Targeted Attack Platform. Предусмотрены следующие конфигурации:

- **[KICS+встроенный агент]**. В этой конфигурации Kaspersky Industrial CyberSecurity for Nodes является и приложением, которое обеспечивает безопасность компьютера, и приложением для работы с KEDR. Встроенный агент доступен в Kaspersky Industrial CyberSecurity for Nodes начиная с версии 4.5.

- **[стороннее EPP+KICS в режиме Endpoint Agent]**. В этой конфигурации безопасность IT-инфраструктуры обеспечивает система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Работу с KEDR обеспечивает Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent. Режим Endpoint Agent доступен в Kaspersky Industrial CyberSecurity for Nodes начиная с версии 4.5.

Поддержка предыдущих версий Kaspersky Industrial CyberSecurity for Nodes

Приложение Kaspersky Industrial CyberSecurity for Nodes версии 4.5 поддерживает работу с решением Kaspersky Anti Targeted Attack Platform (EDR) с помощью встроенного агента или режима Endpoint Agent, устанавливать Kaspersky Endpoint Agent не требуется.

Если вы используете Kaspersky Industrial CyberSecurity for Nodes версии ниже 4.5 для взаимодействия с Kaspersky Anti Targeted Attack Platform (EDR), вам нужно установить Kaspersky Endpoint Agent отдельно.

Настройка интеграции с KATA

Начиная с Kaspersky Industrial CyberSecurity for Nodes версии 4.5 компонент Интеграция с KATA переименован в Endpoint Detection and Response Expert (on-premises). В этой версии приложения компонент совместим с Kaspersky Anti Targeted Attack Platform версии 7.1 и ниже и Kaspersky Endpoint Detection and Response Expert (on-premises).

Компоненты Endpoint Detection and Response (Industrial CyberSecurity) и Endpoint Detection and Response Expert (on-premises) несовместимы между собой.

Для интеграции встроенного агента Kaspersky Industrial CyberSecurity for Nodes с KATA должны быть выполнены следующие условия:

- В IT-инфраструктуре организации развернуто решение Kaspersky Anti Targeted Attack Platform версии 5.0 или выше.
- В IT-инфраструктуре организации развернуто Kaspersky Security Center версии 14.2 или выше.
- Включены и работают компоненты приложения, которые обеспечивают передачу данных в KATA:
  - Постоянная защита файлов.
  - Защита от эксплойтов.

- Защита от шифрования.
- AMSI-защита.
- Kaspersky Security Network.

Для интеграции конфигурации Endpoint Agent с KATA в IT-инфраструктуре организации должны быть развернуты:

- Kaspersky Anti Targeted Attack Platform версии 5.0 или выше.
- Kaspersky Security Center версии 14.2 или выше.

Интеграция с KATA состоит из следующих этапов:

1. **Установка компонента Endpoint Detection and Response Expert (on-premises)**

   В параметрах инсталляционного пакета или мастере установки приложения, а также с помощью изменения состава компонентов приложения через Панель управления Windows, на этапе выбора компонентов приложения для установки выберите:

   - **Полная функциональность → Endpoint Agent → Endpoint Detection and Response Expert (on-premises)** для встроенного агента;
   - **Endpoint Agent → Endpoint Detection and Response Expert (on-premises)** для конфигурации Endpoint Agent.

   Для завершения изменения состава компонентов приложения необходимо перезагрузить компьютер.

2. **Активация Endpoint Detection and Response Expert (on-premises)**

   Вам нужно приобрести отдельную лицензию на использование KATA (например, Kaspersky Endpoint Detection and Response (KATA) Add-on).

   Лицензирование отдельной функциональности Endpoint Detection and Response Expert (on-premises) не отличается от лицензирования Kaspersky Industrial CyberSecurity for Nodes. Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response (KATA). В результате на компьютере будет добавлено два ключа: ключ для Kaspersky Industrial CyberSecurity for Nodes и ключ для Endpoint Detection and Response Expert (on-premises).

   Убедитесь, что функциональность Endpoint Detection and Response Expert (on-premises) включена в лицензию.

3. **Подключение к Central Node**

   Для работы Kaspersky Anti Targeted Attack Platform вы можете установить доверенное соединение между Kaspersky Industrial CyberSecurity for Nodes и компонентом Central Node. Для настройки доверенного соединения вам нужен TLS-сертификат. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). Далее вам нужно добавить TLS-сертификат в Kaspersky Industrial CyberSecurity for Nodes (см. инструкцию ниже).

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes проверяет только TLS-сертификат Central Node. Чтобы сделать соединение более безопасным, вы можете включить дополнительную проверку компьютера в Central Node. Для включения такой проверки вам нужно включить двустороннюю аутентификацию в параметрах Central Node и Kaspersky Industrial CyberSecurity for Nodes. Также для двусторонней аутентификации вам нужен криптоконтейнер. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

Как подключить компьютер с Kaspersky Industrial CyberSecurity for Nodes к Central Node в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику для управления приложением и откройте окно ее параметров двойным щелчком мыши.
4. Выберите раздел **Серверы сбора телеметрии**.
5. В блоке **Endpoint Detection and Response Expert (on-premises)** нажмите на кнопку **Настройка**.

   Откроется окно **Endpoint Detection and Response Expert (on-premises)**.
6. Установите флажок **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.
7. В блоке **Настройки подключения** с помощью кнопки **Добавить** добавьте один или несколько серверов Central Node. Для каждого сервера укажите адрес сервера (IPv4, IPv6) и порт подключения к серверу.

   Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение через второй IP-адрес и так далее по списку.
8. Нажмите на кнопку **Настройки подключения к серверам**.
9. В открывшемся окне настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Industrial CyberSecurity for Nodes пытается подключиться к другому серверу Central Node.
   - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).
   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Central Node. Для использования двусторонней аутентификации вам нужно в параметрах Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.
10. Нажмите на кнопку **OK**.

11. Если требуется, настройте параметры отправки телеметрии.

12. Сохраните внесенные изменения.

Как подключить компьютер с Kaspersky Industrial CyberSecurity for Nodes к Central Node в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Серверы сбора телеметрии → Endpoint Detection and Response Expert (on-premises)**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Свойства: Endpoint Detection and Response Expert (on-premises)** на вкладке **Общие**.

3. Установите флажок **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.

4. В блоке **Настройки подключения** с помощью кнопки **Добавить** добавьте один или несколько серверов Central Node. Для каждого сервера укажите адрес сервера (IPv4, IPv6) и порт подключения к серверу.

   Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение через второй IP-адрес и так далее по списку.

5. Нажмите на кнопку **Настройки подключения к серверам**.

6. В открывшемся окне настройте параметры подключения к серверам:

   - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Industrial CyberSecurity for Nodes пытается подключиться к другому серверу Central Node.

   - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).

   - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Central Node. Для использования двусторонней аутентификации вам нужно в параметрах Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

     Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

7. Нажмите на кнопку **OK**.

8. Если требуется, настройте параметры отправки телеметрии.

9. Сохраните внесенные изменения.

Как подключить компьютер с Kaspersky Industrial CyberSecurity for Nodes к Central Node в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Серверы сбора телеметрии**.
5. В блоке **Endpoint Detection and Response Expert (on-premises)** нажмите на кнопку **Настроить**.

   Откроется окно **Endpoint Detection and Response Expert (on-premises)**.
6. Установите флажок **Включить Endpoint Detection and Response Expert (on-premises)**.
7. Выберите режим **Endpoint Detection and Response Expert (версия 7.1 и ниже)**.
8. В блоке **Настройки подключения** с помощью кнопки **Добавить** добавьте один или несколько серверов Central Node. Для каждого сервера укажите адрес сервера (IPv4, IPv6) и порт подключения к серверу.

   Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение через второй IP-адрес и так далее по списку.
9. Нажмите на кнопку **Настройки подключения**.
10. В открывшемся окне настройте параметры подключения к серверам:

    - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера Central Node. По истечению времени ожидания Kaspersky Industrial CyberSecurity for Nodes пытается подключиться к другому серверу Central Node.
    - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Central Node. Вы можете получить TLS-сертификат в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform).
    - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Central Node. Для использования двусторонней аутентификации вам нужно в параметрах Central Node включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в консоли Kaspersky Anti Targeted Attack Platform (см. инструкцию в справке Kaspersky Anti Targeted Attack Platform). После настройки параметров Central Node вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

      Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.
11. Нажмите на кнопку **OK**.

12. Если требуется, настройте параметры отправки телеметрии.

13. Сохраните внесенные изменения.

В результате компьютер с установленным приложением Kaspersky Industrial CyberSecurity for Nodes будет добавлен в консоли Kaspersky Anti Targeted Attack Platform.

Настройка отправки телеметрии

Телеметрия – список событий, которые произошли на защищаемом компьютере. Kaspersky Industrial CyberSecurity for Nodes анализирует данные телеметрии и отправляет их на серверы Kaspersky Anti Targeted Attack Platform во время синхронизации. События телеметрии поступают на сервер почти непрерывно. Kaspersky Industrial CyberSecurity for Nodes выполняет синхронизацию с сервером при выполнении любого из следующих условий:

- Истек период синхронизации.
- Количество событий в буфере превысило максимальное значение.

Вы можете настроить параметры синхронизации в политике Kaspersky Industrial CyberSecurity for Nodes и выбрать оптимальные значения исходя из нагрузки на сеть.

Если соединение между Kaspersky Industrial CyberSecurity for Nodes и сервером отсутствует, то приложение ставит новые события в очередь. При восстановлении соединения Kaspersky Industrial CyberSecurity for Nodes отправляет события из очереди на сервер по порядку. При этом, чтобы не перегрузить сервер, Kaspersky Industrial CyberSecurity for Nodes может отправлять не все события. Для этого вы можете оптимизировать параметры отправки событий и, например, задать максимальное количество событий в час.

Если вы используете Kaspersky Anti Targeted Attack Platform совместно с другим решением, которое также использует телеметрию, вы можете выключить отправку телеметрии для KATA. Это позволит оптимизировать нагрузку на серверы для этих решений. Например, если у вас развернуты решения Managed Detection and Response и Kaspersky Anti Targeted Attack Platform, вы можете использовать телеметрию Managed Detection and Response, а создавать задачи реагирования на угрозы в Kaspersky Anti Targeted Attack Platform.

Как настроить параметры отправки телеметрии в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли откройте папку **Политики**.
3. Выберите нужную политику для управления приложением и откройте окно ее параметров двойным щелчком мыши.
4. Выберите раздел **Серверы сбора телеметрии**.
5. В блоке **Endpoint Detection and Response Expert (on-premises)** нажмите на кнопку **Настройка**.
6. В открывшемся окне настройте параметр **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)**. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Industrial CyberSecurity for Nodes передает данные об изменениях в параметрах приложения и задачах.

7. Убедитесь, что в блоке **Настройка передачи данных** установлен флажок **Отправлять телеметрию в KATA**.

8. Если требуется, настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Industrial CyberSecurity for Nodes повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. По умолчанию установлено значение 30 секунд.

9. Если требуется, настройте параметр **Максимальное количество пакетов событий**. Параметр регулирует максимальное количество пакетов, которое можно передать в рамках одной транзакции. По умолчанию установлено значение 1024.

10. Если требуется, в блоке **Регулирование количества запросов** установите флажок **Включить регулирование количества запросов**.

    Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

11. Настройте параметры оптимизации отправки событий на сервер:

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15%.

12. Сохраните внесенные изменения.

Как настроить параметры отправки телеметрии в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Серверы сбора телеметрии → Endpoint Detection and Response Expert (on-premises)**.

2. В панели результатов перейдите по ссылке **Свойства**.

3. В открывшемся окне настройте параметр **Отправлять запрос на синхронизацию на сервер KATA каждые (мин.)**. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Industrial CyberSecurity for Nodes передает данные об изменениях в параметрах приложения и задачах.

4. Убедитесь, что в блоке **Настройка передачи данных** установлен флажок **Отправлять телеметрию в KATA**.

5. Если требуется, настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Industrial CyberSecurity for Nodes повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. По умолчанию установлено значение 30 секунд.

6. Если требуется, настройте параметр **Максимальное количество пакетов событий**. Параметр регулирует максимальное количество пакетов, которое можно передать в рамках одной транзакции. По умолчанию установлено значение 1024.

7. Если требуется, в блоке **Регулирование количества запросов** установите флажок **Включить регулирование количества запросов**.

   Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

8. Настройте параметры оптимизации отправки событий на сервер:

   - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

   - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15%.

9. Сохраните внесенные изменения.

Как настроить параметры отправки телеметрии в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Серверы сбора телеметрии**.

5. В блоке **Endpoint Detection and Response Expert (on-premises)** нажмите на кнопку **Настроить**.

6. В открывшемся окне настройте параметр **Отправлять запрос на синхронизацию на сервер каждые (мин.)**. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Industrial CyberSecurity for Nodes передает данные об изменениях в параметрах приложения и задачах.

7. Убедитесь, что в блоке **Настройка передачи данных** установлен флажок **Отправлять телеметрию в KATA**.

8. Если требуется, настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Industrial CyberSecurity for Nodes повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. По умолчанию установлено значение 30 секунд.

9. Если требуется, настройте параметр **Максимальное количество пакетов событий**. Параметр регулирует максимальное количество пакетов, которое можно передать в рамках одной транзакции. По умолчанию установлено значение 1024.

10. Если требуется, в блоке **Троттлинг** установите флажок **Включить троттлинг**.

    Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

11. Настройте параметры оптимизации отправки событий на сервер:

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15%.

12. Сохраните внесенные изменения.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Industrial CyberSecurity for Nodes поддерживает работу с решением Kaspersky Endpoint Detection and Response Expert (on-premises). Kaspersky Endpoint Detection and Response Expert (on-premises) – решение для кибербезопасности бизнеса, которое включает в себя приложения "Лаборатории Касперского", с помощью которых организация получает возможность защититься от большинства киберрисков и покрыть основные сценарии распространения угроз. Компоненты EDR Expert (on-premises) развернуты на единой платформе управления Open Single Management Platform (OSMP). Платформа обеспечивает выполнение кросс-программных сценариев в рамках единого интерфейса и позволяет интегрировать приложения "Лаборатории Касперского" и приложения сторонних производителей в единую систему безопасности.

Один из центральных элементов решения – *SIEM*. SIEM позволяет отслеживать события, полученные от всех компонентов, и выполняет взаимную корреляцию этих событий с помощью готовых и пользовательских правил. На основании журналов и телеметрии, полученных от инфраструктуры организации, EDR Expert (on-premises) автоматически выявляет атаки и позволяет проводить расследование инцидентов с помощью единого графа расследования, который комбинирует все собираемые в EDR Expert (on-premises) события – как от приложений "Лаборатории Касперского", так и от сторонних ИБ-продуктов.

Для реагирования на сложные инциденты EDR Expert (on-premises) использует предустановленные и пользовательские сценарии. Также доступны действия по реагированию от приложений сторонних производителей и сценарии реагирования, в которых задействовано несколько приложений.

Средства анализа угроз

Kaspersky Endpoint Detection and Response использует следующие средства анализа угроз (Threat Intelligence):

- Интеграция с Kaspersky Threat Intelligence Portal, который содержит и отображает информацию о репутации файлов и веб-адресов.
- База угроз "Лаборатории Касперского" Kaspersky Threats.
- Инфраструктура облачных служб Kaspersky Security Network, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Принцип работы решения

Приложение Kaspersky Industrial CyberSecurity for Nodes устанавливается на отдельных компьютерах под управлением операционных систем Windows, входящих в IT-инфраструктуру организации, и осуществляет постоянное наблюдение за процессами, открытыми сетевыми соединениями и изменяемыми файлами. Данные о событиях на компьютере, об угрозах, обнаруженных приложением, и данные о результатах обработки этих угроз отправляются на сервер EDR Expert (on-premises).

Настройка интеграции с EDR Expert (on-premises) выполняется в Kaspersky Security Center Web Console. Дальнейшее управление встроенным агентом или приложением в режиме Endpoint Agent осуществляется в единой платформе управления OSMP, включая запуск задач, управление объектами на карантине, просмотр отчетов и другие действия.

Конфигурации Kaspersky Industrial CyberSecurity for Nodes для работы с Kaspersky Anti Targeted Attack Platform

Для работы с EDR Expert (on-premises) предусмотрены следующие конфигурации:

- **[KICS+встроенный агент]**. В этой конфигурации Kaspersky Industrial CyberSecurity for Nodes является и приложением, которое обеспечивает безопасность компьютера, и приложением для работы с EDR Expert (on-premises). Встроенный агент поддерживает работу с EDR Expert (on-premises) начиная с версии 4.5.
- **[стороннее EPP+KICS в режиме Endpoint Agent]**. В этой конфигурации безопасность IT-инфраструктуры обеспечивает система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Работу с EDR Expert (on-premises) обеспечивает Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent. Режим Endpoint Agent поддерживает работу с EDR Expert (on-premises) начиная с версии 4.5.

Настройка интеграции с EDR Expert (on-premises)

Компоненты Endpoint Detection and Response (Industrial CyberSecurity) и Endpoint Detection and Response Expert (on-premises) несовместимы между собой.

Для работы Endpoint Detection and Response Expert (on-premises) должны быть выполнены следующие условия:

- Установлена единая платформа управления OSMP (Open Single Management Platform).
- Приложение активировано и функциональность входит в лицензию.
- Компонент Endpoint Detection and Response Expert (on-premises) включен.
- Компоненты приложения, которые обеспечивают работу EDR Expert (on-premises), включены и работают. Работу EDR Expert (on-premises) обеспечивают следующие компоненты:
  - Постоянная защита файлов.
  - Защита от эксплойтов.
  - Защита от шифрования.
  - AMSI-защита.
  - Kaspersky Security Network.

Интеграция с EDR Expert (on-premises) состоит из следующих этапов:

1. **Установка компонента Endpoint Detection and Response Expert (on-premises)**

   В параметрах инсталляционного пакета или мастере установки приложения, а также с помощью изменения состава компонентов приложения через Панель управления Windows, на этапе выбора компонентов приложения для установки выберите:

   - **Полная функциональность → Endpoint Agent → Endpoint Detection and Response Expert (on-premises)** для встроенного агента;
   - **Endpoint Agent → Endpoint Detection and Response Expert (on-premises)** для конфигурации Endpoint Agent.

   > Для завершения изменения состава компонентов приложения необходимо перезагрузить компьютер.

2. **Активация Endpoint Detection and Response Expert (on-premises)**

   Вам нужно приобрести отдельную лицензию на использование EDR Expert (on-premises) (Kaspersky Endpoint Detection and Response Expert (on-premises) Add-on).

   Лицензирование отдельной функциональности Endpoint Detection and Response Expert (on-premises) не отличается от лицензирования Kaspersky Industrial CyberSecurity for Nodes. Функциональность будет доступна после добавления отдельного ключа Kaspersky Endpoint Detection and Response (on-premises). В результате на компьютере будет добавлено два ключа: ключ для Kaspersky Industrial CyberSecurity for Nodes и ключ для Endpoint Detection and Response Expert (on-premises).

   Убедитесь, что функциональность Endpoint Detection and Response Expert (on-premises) включена в лицензию.

3. **Подключение к серверу сбора телеметрии и серверу реагирования**

Для работы Kaspersky Endpoint Detection and Response Expert (on-premises) необходимо установить доверенное соединение между Kaspersky Industrial CyberSecurity for Nodes и двумя серверами:

- *Сервер сбора телеметрии* – сервер, входящий в состав SIEM, который предназначен для сбора, нормализации, корреляции, анализа и хранения данных о событиях на компьютере.

- *Сервер реагирования* – сервер, который предназначен для приема и проверки данных, исследования поведения объектов, а также публикации результатов исследования.

Для настройки доверенного соединения вам нужен TLS-сертификат. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)). Далее вам нужно добавить TLS-сертификат в Kaspersky Industrial CyberSecurity for Nodes (см. инструкцию ниже).

По умолчанию Kaspersky Industrial CyberSecurity for Nodes проверяет только TLS-сертификат серверов. Чтобы сделать соединение более безопасным, вы можете включить дополнительную проверку компьютера на сервере (двусторонняя аутентификация). Для включения такой проверки вам нужно включить двустороннюю аутентификацию в параметрах сервера и Kaspersky Industrial CyberSecurity for Nodes. Также для двусторонней аутентификации вам нужен криптоконтейнер. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

Как подключить компьютер с Kaspersky Industrial CyberSecurity for Nodes к EDR Expert (on-premises) в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Серверы сбора телеметрии**.

5. В блоке **Endpoint Detection and Response Expert (on-premises)** нажмите на кнопку **Настроить**.

   Откроется окно **Endpoint Detection and Response Expert (on-premises)**.

6. Установите флажок **Включить Endpoint Detection and Response Expert (on-premises)**.

7. Выберите режим **Endpoint Detection and Response Expert (версия 8.0 и выше)**.

8. Настройте параметры подключения к серверам сбора телеметрии:

   a. В блоке **Подключение к серверам сбора телеметрии** перейдите по ссылке **Настройки подключения**.

   b. В открывшемся окне настройте параметры подключения к серверам сбора телеметрии:

      - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Industrial CyberSecurity for Nodes пытается подключиться к другому серверу.

      - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и сервером. Для использования двусторонней аутентификации вам нужно в параметрах сервера включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)). После настройки параметров сервера вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

  Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

c. Нажмите на кнопку **OK**.

d. Добавьте серверы сбора телеметрии. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

   Вы можете добавить несколько адресов сервера сбора телеметрии. Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение через второй IP-адрес и так далее по списку.

e. Если требуется, настройте параметры отправки телеметрии.

9. Настройте подключение к серверам реагирования:

a. В блоке **Подключение к серверам реагирования** настройте параметр **Отправлять запрос на синхронизацию на сервер каждые (мин.)**. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Industrial CyberSecurity for Nodes получает задачи по реагированию на угрозы и отправляет результаты выполнения задач.

b. Перейдите по ссылке **Настройки подключения**.

c. В открывшемся окне настройте параметры подключения к серверам реагирования:

- **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Industrial CyberSecurity for Nodes пытается подключиться к другому серверу.

- **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером. Вы можете получить TLS-сертификат в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и сервером. Для использования двусторонней аутентификации вам нужно в параметрах сервера включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. Вы можете получить криптоконтейнер в единой платформе управления OSMP (см. инструкцию в справке Kaspersky Endpoint Detection and Response Expert (on-premises)). После настройки параметров сервера вам нужно в параметрах Kaspersky Endpoint Security также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

  Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

d. Нажмите на кнопку **OK**.

e. Добавьте серверы реагирования. Для этого укажите адрес сервера (IPv4, IPv6), а также порт подключения к серверу.

   Вы можете добавить несколько адресов сервера сбора телеметрии. Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение с сервером через первый IP-адрес. Если установить соединение не удалось, Kaspersky Industrial CyberSecurity for Nodes пытается установить соединение через второй IP-адрес и так далее по списку.

10. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

В результате компьютер будет добавлен единой платформе управления OSMP.

Настройка отправки телеметрии EDR Expert (on-premises)

Телеметрия – список событий, которые произошли на защищаемом компьютере. Kaspersky Industrial CyberSecurity for Nodes анализирует данные телеметрии и отправляет их на серверы сбора телеметрии во время синхронизации. Подробную информацию об отправляемых событиях телеметрии см. в справке Kaspersky Endpoint Detection and Response Expert (on-premises).

События телеметрии поступают на сервер почти непрерывно. Kaspersky Industrial CyberSecurity for Nodes выполняет синхронизацию с сервером при выполнении любого из следующих условий:

- Истек период синхронизации.
- Количество событий в буфере превысило максимальное значение.

Таким образом, по умолчанию приложение выполняет синхронизацию каждые 30 секунд или при накоплении в буфере 1024 события. Вы можете настроить параметры синхронизации в политике Kaspersky Industrial CyberSecurity for Nodes и выбрать оптимальные значения исходя из нагрузки на сеть (см. инструкцию ниже).

Если соединение между Kaspersky Industrial CyberSecurity for Nodes и сервером отсутствует, то приложение ставит новые события в очередь. При восстановлении соединения Kaspersky Industrial CyberSecurity for Nodes отправляет события из очереди на сервер по порядку. При этом, чтобы не перегрузить сервер, Kaspersky Industrial CyberSecurity for Nodes может отправлять не все события. Для этого вы можете оптимизировать параметры отправки событий и, например, задать максимальное количество событий в час (см. инструкцию ниже).

Чтобы настроить параметры отправки телеметрии, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Серверы сбора телеметрии**.
5. В блоке **Endpoint Detection and Response Expert (on-premises)** нажмите на кнопку **Настроить**.

   Откроется окно **Endpoint Detection and Response Expert (on-premises)**.
6. В блоке **Настройка передачи данных** убедитесь, что установлен флажок **Отправлять телеметрию на серверы сбора телеметрии**.
7. Если требуется, установите флажок **Отправлять телеметрию только с IOA**. *Индикатор атак (Indicator of Attack, IOA)* – правило, содержащее описание подозрительного поведения в системе, которое может являться признаком целевой атаки. Приложение сравнивает текущее поведение в системе с этими правилами и регистрирует события, характерные для целевой атаки. Приложение использует технологию потоковой проверки, которая позволяет отслеживать такие события в режиме реального времени.
8. Если требуется, в блоке **Настройка передачи данных** настройте параметры синхронизации с сервером:

   - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечению периода синхронизации. По умолчанию установлено значение 30 секунд.
   - **Управлять количеством пакетов событий, передаваемых в рамках транзакции**. Приложение выполняет синхронизацию с сервером при заполнении буфера событиями. По умолчанию установлено значение 1024 события.
9. Если требуется, в блоке **Троттлинг** снимите флажок **Включить троттлинг**.

   Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события. По умолчанию функция включена.
10. Настройте параметры оптимизации отправки событий на сервер:

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечению часа. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.
    - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. По умолчанию установлено значение 15 %.

11. В блоке **Подключение к серверам реагирования** введите значение для параметра **Отправлять запрос на синхронизацию на сервер каждые (мин.)**.

12. Период отправки запросов на синхронизацию с сервером. Во время синхронизации Kaspersky Industrial CyberSecurity for Nodes передает данные об изменениях в параметрах приложения и задачах.

13. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Исключения из телеметрии EDR Expert (on-premises)

Для повышения производительности и оптимизации отправки данных на Сервер сбора телеметрии вы можете настроить исключения из телеметрии. Например, вы можете отменить обработку данных о сетевых коммуникациях для отдельных приложений.

Kaspersky Industrial CyberSecurity for Nodes поддерживает суммарно не более 10 000 включающих и исключающих правил фильтрации событий EDR Expert (on-premises).

Правила фильтрации событий EDR Expert (on-premises) не будут переданы из политики на управляемые устройства с Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и ниже в случае превышения поддерживаемого объема хранимых правил фильтрации. Приложение отобразит соответствующее предупреждение.

Чтобы создать исключение из телеметрии в Web Console:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Дополнительные возможности**.

5. В блоке **Настройки телеметрии** нажмите на кнопку **Настроить**.

6. Выберите вкладку **Телеметрия EDR Expert (on-premises)**.

7. В блоке **Общие исключения** нажмите на кнопку **Добавить**.

   Откроется окно **Добавление правила исключения**.

8. При необходимости измените статус правила. По умолчанию правило включено.

9. Введите имя правила.

10. Выберите действие, которое будет выполнено при срабатывании правила:

    - **Не собирать**. Отфильтрованное событие будет исключено из отправляемой телеметрии.

    - **Исключить IOA**. Из отправляемой телеметрии будет исключено событие о срабатывании IOA-правила.

11. Если выбран вариант **Исключить IOA**, укажите IOA-правила, которые необходимо добавить в исключения:

    - **Исключить все**. При выполнении заданного условия приложение будет исключать из телеметрии события, формируемые на основе всех IOA-правил.

    - **Исключить по GUID**. Укажите GUID IOA-правила. Вы можете указать несколько GUID через `,`. Подробную информацию об IOA-правилах см. в справке EDR Expert (on-premises).

12. Задайте условие фильтрации:

    a. Выберите название поля, по которому будет выполняться фильтрация.

    b. Выберите оператор (см. таблицу ниже), и укажите значение, с которым будет сравниваться значение поля из события.

Перечень операторов условий

Оператор	Описание
<	Если значение поля меньше значения, заданного в условии, событие будет отфильтровано.
≤	Если значение поля меньше или равно значению, заданному в условии, событие будет отфильтровано.
=	Если значение поля равно значению, заданному в условии, событие будет отфильтровано.
≥	Если значение поля больше или равно значению, заданному в условии, событие будет отфильтровано.
>	Если значение поля больше значения, заданного в условии, событие будет отфильтровано.
≠	Если значение поля не равно значению, заданному в условии, событие будет отфильтровано.
похоже	Если значение поля подходит под маску, указанную в условии, событие будет отфильтровано. Приложение поддерживает символы `*` и `?` для ввода маски.
не похоже	Если значение поля не подходит под маску, указанную в условии, событие будет отфильтровано. Приложение поддерживает символы `*` и `?` для ввода маски.
одно из	Если значение поля совпадает с одним из значений из заданного в условии списка, событие считается отфильтрованным.
ни одного из	Если значение поля не совпадает ни с одним из значений из заданного в условии списка, событие считается отфильтрованным.
похоже на одно из	Если значение поля подходит под одну из масок, заданных в условии, событие будет отфильтровано. Приложение поддерживает символы * и ? для ввода маски.
не похоже ни на одно из	Если значение поля не подходит ни под одну из масок, заданных в условии, событие будет отфильтровано. Приложение поддерживает символы * и ? для ввода маски.
существует	Если указанное в условии поле содержится в событии, событие будет отфильтровано.
не существует	Если указанное в условии поле не содержится в событии, событие будет отфильтровано.
содержит	Если значение, заданное в условии, содержится в значении поля, событие будет отфильтровано.
равно	Если значение поля равно значению, заданному в условии, событие будет отфильтровано. Проверка выполняется без учета регистра.
побитовое "И"	Если результат операции "Побитовое И" (&) для значения поля и значения, указанного в условии, равен 1, событие будет отфильтровано.

13. При необходимости вы можете формировать сложные критерии фильтрации, добавляя несколько условий фильтрации и групп условий. Также в группу условий вы можете добавлять вложенные условия и группы условий. Вы можете использовать следующие операторы:

    - **И** – фильтр отбирает события, которые соответствуют всем указанным условиям.
    - **ИЛИ** – фильтр отбирает события, которые соответствуют одному из указанных условий.
    - **НЕ** (для использования данного оператора выберите вариант **Добавить НЕ перед**) – фильтр отбирает события, которые не соответствуют всем указанным условиям.

    Условия и группы условий первого уровня объединены с помощью оператора **И**.

14. Если компьютер находится под управлением OSMP, вам доступна проверка созданного правила фильтрации. Для выполнения проверки нажмите на кнопку **Проверить правило**.

    В открывшемся окне отобразится таблица событий, отфильтрованных с помощью созданного правила. Подробнее см. в справке EDR Expert (on-premises).

15. Если требуется, в блоке **Все типы событий** добавьте исключения из телеметрии по типу событий:

    a. Нажмите на название типа события.

    b. В открывшемся окне нажмите на кнопку **Настроить вручную**.

    c. При необходимости настройте отправку телеметрии по выбранному типу событий с помощью переключателя **Отправлять событие**. По умолчанию включена отправка телеметрии по всем типам событий.

    d. В блоке **Правила исключения** нажмите на кнопку **Добавить**.

    Откроется окно **Добавление правила исключения**.

    e. Выполните действия, описанные в шагах 7-13, для каждого добавляемого правила.

16. Для некоторых типов событий вы также можете добавить правила включения для расширения собираемой телеметрии:

    a. В блоке **Правила исключения** нажмите на кнопку **Добавить**.

    Откроется окно **Добавление правила включения**.

    b. Введите имя правила.

    c. В блоке **Условие** введите значения для отображаемых полей. Тип доступных полей зависит от выбранного события.

    Правила исключения имеют приоритет над правилами включения.

17. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Экспорт и импорт фильтров событий EDR Expert (on-premises)

Kaspersky Industrial CyberSecurity for Nodes поддерживает суммарно не более 10 000 включающих и исключающих правил фильтрации событий EDR Expert (on-premises).

Правила фильтрации событий EDR Expert (on-premises) не будут переданы из политики на управляемые устройства с Kaspersky Industrial CyberSecurity for Nodes версии 4.5 и ниже в случае превышения поддерживаемого объема хранимых правил фильтрации. Приложение отобразит соответствующее предупреждение.

Вы можете экспортировать список исключений в файл формата JSON. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество идентификаторов событий. Также вы можете использовать функцию экспорта/импорта для резервного копирования фильтров событий или для миграции списка на другой сервер.

Как экспортировать/импортировать фильтры событий в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Дополнительные возможности**.
4. В блоке **Настройки телеметрии EDR Expert (on-premises)** нажмите на кнопку **Настройка**.
5. Для экспорта настроек телеметрии EDR Expert (on-premises) выполните следующие действия:
   a. Нажмите на кнопку **Экспорт**.
   b. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать настройки, а также выберите папку, в которой вы хотите сохранить этот файл.
   c. Сохраните файл.

   Kaspersky Industrial CyberSecurity for Nodes экспортирует настройки в JSON-файл.
6. Для импорта настроек телеметрии выполните следующие действия:
   a. Нажмите на кнопку **Импорт**.
   b. Выберите JSON-файл, из которого вы хотите импортировать фильтры событий.
   c. Откройте файл.
   d. В открывшемся диалоговом окне подтвердите изменение настроек телеметрии EDR Expert (on-premises).
7. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как экспортировать/импортировать фильтры событий в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Дополнительные возможности**.
5. В блоке **Настройки телеметрии** нажмите на кнопку **Настроить**.
6. Выберите вкладку **Телеметрия EDR Expert (on-premises)**.
7. Для экспорта настроек телеметрии EDR Expert (on-premises) нажмите на кнопку **Экспорт**.

   Kaspersky Industrial CyberSecurity for Nodes сохранит в стандартной папке загрузок файл filterExport.json.
8. Для импорта настроек телеметрии выполните следующие действия:

   a. Нажмите на кнопку **Импорт**.

   b. Выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

   c. Откройте файл.

   d. Выберите способ импорта правил фильтрации событий: добавить к существующим правилам или заменить существующие правила на новые.

   e. Сохраните внесенные изменения.

   Правила, содержащиеся в JSON-файле, отобразятся в списке.

Как экспортировать/импортировать фильтры событий в Консоли приложения

1. В дереве Консоли приложения выберите узел **Настройки телеметрии**.
2. В блоке **Настройки телеметрии EDR Expert (on-premises)** нажмите на кнопку **Настройка**.
3. Для экспорта настроек телеметрии EDR Expert (on-premises) выполните следующие действия:

   a. Нажмите на кнопку **Экспортировать**.

   b. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать настройки, а также выберите папку, в которой вы хотите сохранить этот файл.

   c. Сохраните файл.

   Kaspersky Industrial CyberSecurity for Nodes экспортирует настройки в JSON-файл.
4. Для импорта настроек телеметрии выполните следующие действия:

   a. Нажмите на кнопку **Импортировать**.

   b. Выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

c. Откройте файл.

d. В открывшемся диалоговом окне подтвердите изменение настроек телеметрии EDR Expert (on-premises).

5. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Также вы можете экспортировать и импортировать фильтры событий из командной строки.

YARA-проверка

YARA-проверка – это процесс, в ходе выполнения которого Kaspersky Industrial CyberSecurity for Nodes использует YARA-файлы для поиска сигнатур вредоносной активности на устройствах. Проверка выполняется рекурсивно на локальных дисках. Сканирование сетевых, подключаемых и облачных ресурсов не поддерживается.

Для выполнения YARA-проверки необходима действующая лицензия на использование EDR Expert (on-premise).

YARA-файлы – это файлы с расширением .YARA или .YAR, которые содержат YARA-правила. *YARA-правила* представляют собой описание сигнатур целевых атак и вторжений в IT-инфраструктуру организации. По этим правилам Kaspersky Industrial CyberSecurity for Nodes производит проверку объектов. Если правило выполняется, анализатор выносит заключение о заражении с соответствующими подробностями в журнале.

Учитывайте следующие требования и ограничения, связанные с YARA-файлами:

- Kaspersky Industrial CyberSecurity for Nodes поддерживает YARA-файлы с расширением .YARA или .YAR открытого стандарта описания индикаторов компрометации YARA версии 4.2.3.
- Если вы запустите YARA-проверку с использованием YARA-файлов, которые не поддерживаются Kaspersky Industrial CyberSecurity for Nodes или содержат синтаксические ошибки, проверка будет прервана с соответствующим уведомлением об ошибке.
- Идентификаторы YARA-файлов, которые используются в одной задаче YARA-проверка, должны быть уникальными. Наличие YARA-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.
- YARA-проверка прерывается при обнаружении 128 совпадений с маркерами, описанными в YARA-правилах. Это необходимо для ограничения количества записей в отчете YARA-проверки для удобства его анализа и защиты отчета от переполнения из-за неточно сформулированных YARA-правил, для которых совпадений может быть очень много.

Мы рекомендуем создавать по одному правилу в одном YARA-файле. Такой подход облегчает чтение результатов YARA-проверки.

Запуск YARA-проверки возможен только через интерфейс командной строки.

YARA-проверка может занять продолжительное время. В зависимости от размера диска, параметров задачи, количества объектов на диске YARA-проверка может длиться от нескольких минут до нескольких часов. При этом приложение не показывает индикатор выполнения. Прервать или отменить YARA-проверку невозможно. Рекомендуем дождаться результатов YARA-проверки.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Industrial CyberSecurity for Nodes выводит в командную строку следующие данные о результатах выполнения задачи:

`Started at <time>` `Finished at <time>`	Время начала и завершения сканирования.
`Host name: <computer name>`	Имя компьютера, на котором обнаружен объект.
`Result: <error>`	Код ошибки, которая возникла при выполнении задачи. Если ошибки нет, приложение выводит `0x00000000`.
`Comment: <comment text>`	Описание ошибки, которая возникла при выполнении задачи. Например, `Operation timeout`.
`Object Name:` или `Process:` (при проверке памяти процессов)	Имя объекта/процесса, на котором сработало YARA-правило.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Хеши объекта, на котором сработало YARA-правило.
`Rule Name`	Имя сработавшего YARA-правила.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Метаданные, которые указаны в YARA-правиле.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Найденные совпадения внутри объекта, которые соответствуют условиям YARA-правила:
	• Смещение в памяти процесса / в файле, где обнаружено совпадение (`Offset`).
	• Имя строки в YARA-правиле, с которой произошло совпадение (`String name`).
	• Совпавшая строка в памяти процесса / в файле (`String data`).

Исключения EDR-телеметрии

Для повышения производительности и оптимизации отправки данных на сервер сбора телеметрии вы можете настроить исключения из телеметрии. Например, вы можете отменить обработку данных о сетевых коммуникациях для отдельных приложений.

Создание исключений для EDR-телеметрии в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Дополнительные возможности → Настройки телеметрии Интеграции с KATA / Интеграции с KICS for Networks** и нажмите на кнопку **Настройка**.
4. В открывшемся окне настройте исключения из телеметрии (см. таблицу ниже).
5. Сохраните внесенные изменения.

Создание исключений для EDR-телеметрии в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Дополнительные возможности → Настройки телеметрии Интеграции с KATA / Интеграции с KICS for Networks** и нажмите на кнопку **Настроить**.

5. В открывшемся окне настройте исключения из телеметрии (см. таблицу ниже).

6. Сохраните внесенные изменения.

Создание исключений для EDR-телеметрии в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и в контекстном меню узла выберите пункт **Настройки телеметрии Интеграции с KATA / Интеграции с KICS for Networks**.

2. В открывшемся окне настройте исключения из телеметрии (см. таблицу ниже).

3. Сохраните внесенные изменения.

Параметр	Описание
Исключенные процессы	**Оптимизировать объем отправляемой телеметрии**. Kaspersky Industrial CyberSecurity for Nodes позволяет оптимизировать объем отправляемых данных и исключить из телеметрии события с кодами 102 (базовые коммуникации) и 8 (сетевая активность процесса) для протокола Microsoft SMB, службы WinRM и процесса Агента администрирования klnagent.exe, а также расширенную информацию о типе сетевых пакетов для всех типов сетевых протоколов. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И. **Информация о процессе** и **Информация о родительском процессе**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **Использовать для следующих типов событий**: • **Изменение файла**. • **Сетевые события**. • **Интерактивный ввод команд в консоли**. • **Модуль загружен**. • **Изменение в реестре**. • **Логи DNS**. • **Доступ к процессу**. • **Внедрение в код**. • **Запрос WMI**. • **Канал**. • **LDAP**. • **AMSI**.
Исключенные сетевые коммуникации	• **Название правила**. Имя правила. • **Направление**. Входящие или исходящие события. • **Протокол**. Тип протокола. • **Сырой сокет**. Параметр, определяющий, использовать ли сырой сокет. • **Номер протокола**. Номер протокола. • **TLS-сертификат**. Цифровой сертификат, который используется для обеспечения защищенного соединения между клиентом и сервером с помощью протокола TLS. • **Локальный порт или диапазон**. Конкретный порт или диапазон возможных значений локальных портов. • **Удаленный порт или диапазон**. Конкретный порт или диапазон возможных значений удаленных портов. • **Локальный адрес**. Сетевой адрес компьютера, для которого Kaspersky Industrial CyberSecurity for Nodes исключает телеметрию из сетевого трафика. • **Удаленный адрес**. Сетевой адрес компьютера, для которого Kaspersky Industrial CyberSecurity for Nodes исключает телеметрию из сетевого трафика. Для IP-адресов поддерживается только формат IPv4. • **Приложения**. Список исполняемых файлов приложений, для которых Kaspersky Industrial CyberSecurity for Nodes исключает EDR-телеметрию из сетевого трафика.
Исключенные операции с файлами	• **Название правила**. Имя правила. • **Имя или маска файла**. Имя или маска имени файла или папки, при доступе к которым Kaspersky Industrial CyberSecurity for Nodes применяет правило исключения. Kaspersky Industrial CyberSecurity for Nodes поддерживает символы `*` и `?` для ввода маски. • **Тип операции**. Тип операций с файлами, например, создание файла или изменение атрибутов файла. • **Предыдущий путь**. Предыдущий путь к файлу. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И.

Параметр	Описание
	Информация о процессе и **Информация о родительском процессе**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Родительский путь**. Путь до папки, в которой находится файл. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные операции с DNS	• **Название правила**. Имя правила. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И. **Информация о процессе** и **Информация о родительском процессе**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы. **DNS**: • **IP-адрес DNS-сервера**. Адрес сервера, обрабатывающего DNS-запросы. • **Настройки запроса**. Параметры, регулирующие формат и условия DNS-запроса. • **Статус**. Текущее состояние операции с DNS. • **Имя домена**. Доменное имя, для которого выполняется запрос. • **ID типа настроек**. Уникальный идентификатор типа DNS-настроек. • **Ответная информация**. Данные, возвращаемые сервером в ответ на DNS-запрос.
Исключенные операции с LDAP	• **Название правила**. Имя правила. • **Область поиска LDAP**. Область, в которой выполняется поиск в LDAP. • **Фильтр**. Критерии поиска для фильтрации LDAP-объектов. • **Отличительное имя для поиска объектов в LDAP**. Уникальное имя объекта для поиска в LDAP. • **Атрибуты объекта**. Характеристики объектов, которые будут извлечены в LDAP-запросе. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И. **Информация о процессе** и **Информация о родительском процессе**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256.

Параметр	Описание
	Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.

Параметр	Описание
Исключенные запросы доступа к процессу	**Название правила**. Имя правила. **Тип операции**. Тип операции доступа к процессу, например, "любой" или "открыть". **Запрошенный доступ к процессу**. Уровень доступа к процессу. **Трассировка стека вызовов**. Информация о последовательности вызовов функций, связанная с доступом к процессу. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И. **Информация о процессе**, **Информация о родительском процессе**, **Файл целевого процесса**, **Дескриптор исходного процесса** и **Дескриптор целевого процесса**. • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные внедрения в код	• **Название правила**. Имя правила. • **Метод доступа**. Метод доступа, использованный для внедрения в код. • **Стек вызовов**. Последовательность вызовов функций, связанная с внедрением в код. • **Измененная командная строка**. Командная строка, которая была изменена в процессе внедрения. • **Адрес внедрения**. Место в памяти, где произошло внедрение. • **Имя внедряемой библиотеки DLL**. Название динамически подключаемой библиотеки (DLL), использованной для внедрения. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И. **Информация о процессе** и **Информация о родительском процессе**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные запросы WMI	• **Название правила**. Имя правила. • **Тип операции WMI**. Вид операции, выполняемой с использованием WMI. • **Удаленный запрос**. Информация о том, был ли запрос WMI выполнен удаленно. • **Имя компьютера, с которого выполнена команда WMI**. Название компьютера, инициировавшего запрос. • **Учетная запись пользователя WMI**. Учетная запись пользователя, использованная для запроса WMI. • **Выполненная команда WMI**. Конкретная команда, выполненная через WMI. • **Пространство имен WMI**. Пространство имен, в котором была выполнена операция WMI. • **Фильтр потребителя событий WMI**. Фильтр, используемый для обработки событий в WMI. • **Имя созданного потребителя событий WMI**. Имя потребителя событий, созданного с помощью WMI. • **Исходный код потребителя событий WMI**. Код, использованный для создания потребителя событий WMI. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И.

Параметр	Описание
	Информация о процессе и **Информация о родительском процессе:** • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные операции с каналами	• **Название правила**. Имя правила. • **Имя канала**. Название канала. • **Тип операции**. Тип операций с каналами, например, создание или подключение. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И. **Информация о процессе** и **Информация о родительском процессе**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256. Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные изменения реестра	• **Название правила**. Имя правила. • **Тип операции**. Вид операции, выполняемой с реестром, например, добавление, удаление, изменение. • **Путь**. Путь к ключу или разделу реестра, в котором произошли изменения. • **Имя значения**. Название значения в реестре, которое было изменено. • **Значение**. Новое или измененное значение в реестре. • **Полное имя файла реестра**. Полный путь к файлу реестра, в котором были внесены изменения. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И. **Информация о процессе** и **Информация о родительском процессе**: • **Полный путь**. Полный путь к файлу, включая его имя и расширение. Kaspersky Industrial CyberSecurity for Nodes поддерживает переменные среды и символы `*` и `?` для ввода маски. • **Текст командной строки**. Команда для запуска файла. • **Описание**. Значение параметра FileDescription из ресурса типа RT_VERSION (VersionInfo). • **Исходное имя файла**. Значение параметра OriginalFilename из ресурса типа RT_VERSION (VersionInfo). • **Версия**. Значение параметра FileVersion из ресурса типа RT_VERSION (VersionInfo). • **Контрольные суммы файла**. MD5 и SHA256.

Параметр	Описание
	Вы также можете выбрать файл вручную, и приложение автоматически заполнит поля из выбранного файла. В 64-разрядных операционных системах параметры 64-разрядной версии исполняемого файла процесса из папки `C:\windows\system32` необходимо вводить вручную, так как приложение заполняет параметры исполняемого файла процесса из свойств 32-разрядной версии этого же исполняемого файла, расположенного в папке `C:\windows\syswow64`. Например, если вы выберете файл `C:\windows\system32\cmd.exe`, то плагин отобразит параметры файла `C:\windows\syswow64\cmd.exe`. Такое поведение связано с особенностями операционной системы.
Исключенные операции с устройствами	• **Название правила**. Имя правила. • **Тип устройства**. Тип устройства: локальный принтер, съемный диск, CD/DVD-привод и так далее. Более подробно см. в разделе О правилах доступа к устройствам. • **Идентификатор устройства**. Уникальный идентификатор, с помощью которого можно определить конкретный экземпляр устройства. • **Название устройства**. Имя устройства. Kaspersky Industrial CyberSecurity for Nodes применяет критерии срабатывания по правилу логического И.

Интеграция с Kaspersky Industrial CyberSecurity for Networks

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

Приложение Kaspersky Industrial CyberSecurity for Nodes поддерживает интеграцию с Kaspersky Industrial CyberSecurity for Networks. Данные о событиях на устройстве, полученные Kaspersky Industrial CyberSecurity for Nodes, отправляются на сервер Kaspersky Industrial CyberSecurity for Networks. Интеграция между приложениями расширяет возможности Kaspersky Industrial CyberSecurity for Networks по расследованию и реагированию на угрозы в сетях промышленных предприятий.

Конфигурации Kaspersky Industrial CyberSecurity for Nodes для интеграции с Kaspersky Industrial CyberSecurity for Networks

Предусмотрены следующие конфигурации:

- **[KICS+встроенный агент]**. В этой конфигурации Kaspersky Industrial CyberSecurity for Nodes является и приложением, которое обеспечивает безопасность компьютера, и приложением для работы с Kaspersky Industrial CyberSecurity for Networks. Встроенный агент доступен в Kaspersky Industrial CyberSecurity for Nodes начиная с версии 4.5.

- **[стороннее EPP+KICS в режиме Endpoint Agent]**. В этой конфигурации безопасность компьютера обеспечивает система защиты конечных точек (англ. Endpoint Protection Platform, EPP) от сторонних поставщиков. Работу с Kaspersky Industrial CyberSecurity for Networks обеспечивает Kaspersky Industrial CyberSecurity for Nodes в режиме Endpoint Agent. Режим Endpoint Agent доступен в Kaspersky Industrial CyberSecurity for Nodes начиная с версии 4.5.

Для интеграции встроенного агента Kaspersky Industrial CyberSecurity for Nodes с Kaspersky Industrial CyberSecurity for Networks должны быть выполнены следующие условия:

- Развернуто приложение Kaspersky Industrial CyberSecurity for Networks.
- Развернуто приложение Kaspersky Security Center версии 14.2 или выше.
- Включены и работают следующие компоненты защиты: Защита от эксплойтов, Откат вредоносных действий, Защита от шифрования.

Для интеграции конфигурации Endpoint Agent с Kaspersky Industrial CyberSecurity for Networks должны быть развернуты:

- Kaspersky Industrial CyberSecurity for Networks.
- Kaspersky Security Center версии 14.2 или выше.

Поддержка предыдущих версий Kaspersky Industrial CyberSecurity for Nodes

Приложение Kaspersky Industrial CyberSecurity for Nodes версии 4.5 поддерживает работу с Kaspersky Industrial CyberSecurity for Networks с помощью встроенного агента или режима Endpoint Agent, устанавливать Kaspersky Endpoint Agent не требуется.

Если вы используете Kaspersky Industrial CyberSecurity for Nodes версии ниже 4.5 для взаимодействия с Kaspersky Industrial CyberSecurity for Networks, вам нужно установить Kaspersky Endpoint Agent отдельно.

Настройка интеграции с Kaspersky Industrial CyberSecurity for Networks

Интеграция с Kaspersky Industrial CyberSecurity for Networks состоит из следующих этапов:

1. **Установка компонента Интеграция с Kaspersky Industrial CyberSecurity for Networks**

   В параметрах инсталляционного пакета или мастере установки приложения, а также с помощью изменения состава компонентов приложения через Панель управления Windows, на этапе выбора компонентов приложения для установки выберите:

   - **Полная функциональность** → **Endpoint Agent** → **Интеграция с KICS for Networks** для встроенного агента;
   - **Endpoint Agent** → **Интеграция с KICS for Networks** для режима Endpoint Agent.

   > Для завершения изменения состава компонентов приложения необходимо перезагрузить компьютер.

2. **Активация компонента Интеграция с Kaspersky Industrial CyberSecurity for Networks**

   Убедитесь, что функциональность Интеграция с Kaspersky Industrial CyberSecurity for Networks включена в лицензию.

3. **Включение и настройка компонента Интеграция с Kaspersky Industrial CyberSecurity for Networks**

   Kaspersky Industrial CyberSecurity for Nodes поддерживает протоколы TCP и UDP для отправки телеметрии на сервер KICS for Networks. В зависимости от параметров сервера интеграции KICS for Networks, к которому будет выполняться подключение, вам нужно выбрать соответствующий протокол и указать настройки подключения. Подробнее о параметрах серверов интеграции см. в справке KICS for Networks.

Также приложение поддерживает интеграцию с KICS for Networks в сети с установленным диодом данных. Диод данных – это однонаправленный шлюз для передачи данных между защищенными сегментами сети и внешними устройствами. Приложение может отправлять телеметрию через диод данных по следующим протоколам:

- MQTT;
- UDP.

Подробнее о передаче данных телеметрии в KICS for Networks через диоды данных см. в справке KICS for Networks.

Kaspersky Industrial CyberSecurity for Nodes поддерживает программные MQTT-серверы (например, Mosquitto) в качестве MQTT-брокера. Вы можете использовать приложение как в режиме подписчика, так и в режиме издателя. Приложение в режиме MQTT-издателя отправляет телеметрию через диод данных в адрес MQTT-брокера.

Телеметрия, отправленная на сервер MQTT-брокера, может содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту телеметрии.

Как настроить интеграцию с Kaspersky Industrial CyberSecurity for Networks в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. Выберите раздел **Серверы сбора телеметрии**.
4. В блоке **Интеграция с KICS for Networks** нажмите на кнопку **Настройка**.

   Откроется окно **Интеграция с KICS for Networks**.
5. Установите флажок **Интеграция с KICS for Networks**.
6. На вкладке **Общие** выберите режим отправки телеметрии:

   - **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию напрямую на сервер Kaspersky Industrial CyberSecurity for Networks по протоколу TCP.
   - **Отправлять телеметрию на диод данных в качестве MQTT-издателя**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию на сервер MQTT-брокера, встроенный в программный диод данных.
   - **Отправлять телеметрию на сервер KICS for Networks по протоколу UDP**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию на сервер Kaspersky Industrial CyberSecurity for Networks через диод данных по протоколу UDP.

7. Для режима **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP** вам нужно настроить следующие параметры:

   - **Адрес** и **Порт**. IP-адрес сервера Kaspersky Industrial CyberSecurity for Networks, в адрес которого отправляется телеметрия, и порт для подключения. Диапазон возможных значений порта: 1–65535. Значение порта по умолчанию – 8081.

   - **Интервал между запросами (мин.)**. Интервал между запросами на сервер Kaspersky Industrial CyberSecurity for Networks в минутах. При работе Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-издателя данный параметр задает интервал между запросами к MQTT-брокеру в случае потери соединения с брокером. Диапазон доступных значений: 1–60 мин. Значение по умолчанию – 1 мин.

   - **Настройки подключения к серверам**. Настройте следующие параметры:

     - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Industrial CyberSecurity for Nodes повторно подключается к серверу. Диапазон доступных значений: 1–60 000 сек. Значение по умолчанию – 10 сек.

     - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Kaspersky Industrial CyberSecurity for Networks. Вы можете получить TLS-сертификат с помощью интерфейса управления Kaspersky Industrial CyberSecurity for Networks.

     - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks. Для использования двусторонней аутентификации вам нужно в параметрах Kaspersky Industrial CyberSecurity for Networks включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. После настройки параметров Kaspersky Industrial CyberSecurity for Networks вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

       Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

8. Для режима **Отправлять телеметрию на диод данных в качестве MQTT-издателя** вам нужно настроить следующие параметры:

   a. Нажмите на кнопку **Настройки подключения к серверам**.

   b. Введите учетные данные для аутентификации на сервере MQTT-брокера.

   c. Введите IP-адрес и порт сервера MQTT-брокера.

9. Для режима **Отправлять телеметрию на сервер KICS for Networks по протоколу UDP** настройте следующие параметры:

   a. Введите IP-адрес и порт сервера.

   b. Для включения шифрования данных нажмите на кнопку **Настройки подключения к серверам** и установите флажок **Использовать шифрование при передаче данных по протоколу UDP**.

   > Вам необходимо самостоятельно определить необходимость шифрования передаваемых данных.

   c. Введите пароль от ключа шифрования и загрузите файл ключа шифрования с расширением .PEM.

10. Перейдите на вкладку **Передача данных**.

11. Настройте параметры передачи данных:

    - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечении указанного времени. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.

      > При использовании Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика не рекомендуется настраивать получение данных телеметрии более чем от 250 устройств с Kaspersky Industrial CyberSecurity for Nodes, настроенном в качестве MQTT-издателя, в случае, если в настройках MQTT-издателей задано минимальное значение параметра **Максимальная задержка отправки событий (сек.)** – 1 сек. Если значение параметра равно 30 сек. и более, не рекомендуется настраивать получение данных более чем от 1000 MQTT-издателей.

    - **Включить регулирование количества запросов**. Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечении часа. Диапазон доступных значений: 10–65 535. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. Диапазон доступных значений: 5–100%. Значение по умолчанию – 15%.

Если необходимо, настройте неизбирательный режим сбора телеметрии. По умолчанию Kaspersky Industrial CyberSecurity for Nodes собирает сетевой трафик, поступающий на сетевые интерфейсы компьютера и предназначенный компьютеру, на котором установлено приложение. В неизбирательном режиме приложение собирает сетевой трафик для сетевых интерфейсов компьютера с установленным приложением со всех доступных подсетей. На основе собранного сетевого трафика приложение формирует расширенную телеметрию.

Не все сетевые адаптеры поддерживают неизбирательный режим сбора телеметрии (англ. Promiscuous mode). На этих сетевых адаптерах сбор расширенной телеметрии не работает.

a. На вкладке **Сбор телеметрии** установите флажок **Включить неизбирательный режим для приложения и сетевых интерфейсов узла**, если хотите, чтобы для всех сетевых интерфейсов компьютера с установленным приложением был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

b. Установите флажок **Использовать в неизбирательном режиме только сетевые интерфейсы узла, настроенные на указанные подсети**, если хотите, чтобы для сетевых интерфейсов компьютера с установленным приложением, настроенных на подсети из списка ниже, был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

c. Если необходимо, сформируйте список подсетей.

12. Сохраните внесенные изменения.

Как настроить интеграцию с Kaspersky Industrial CyberSecurity for Networks в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Серверы сбора телеметрии**.
5. В блоке **Интеграция с KICS for Networks** нажмите на кнопку **Настроить**.

   Откроется окно **Интеграция с KICS for Networks**.
6. Установите флажок **Включить Интеграцию с KICS for Networks**.
7. В блоке **Настройка подключения** выберите режим отправки телеметрии:

   - **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию напрямую на сервер Kaspersky Industrial CyberSecurity for Networks по протоколу TCP.
   - **Отправлять телеметрию на диод данных в качестве MQTT-издателя**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию на сервер MQTT-брокера, встроенный в программный диод данных.
   - **Отправлять телеметрию на сервер KICS for Networks по протоколу UDP**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию на сервер Kaspersky Industrial CyberSecurity for Networks через диод данных по протоколу UDP.

8. Для режима **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP** вам нужно настроить следующие параметры:

   - **Адрес** и **Порт**. IP-адрес сервера Kaspersky Industrial CyberSecurity for Networks, в адрес которого отправляется телеметрия, и порт для подключения. Диапазон возможных значений порта: 1–65535. Значение порта по умолчанию – 8081.

   - **Интервал между запросами (мин.)**. Интервал между запросами на сервер Kaspersky Industrial CyberSecurity for Networks в минутах. При работе Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-издателя данный параметр задает интервал между запросами к MQTT-брокеру в случае потери соединения с брокером. Диапазон доступных значений: 1–60 мин. Значение по умолчанию – 1 мин.

   - **Настройки подключения к серверам**. Настройте следующие параметры:

     - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Industrial CyberSecurity for Nodes повторно подключается к серверу. Диапазон доступных значений: 1–60 000 сек. Значение по умолчанию – 10 сек.

     - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Kaspersky Industrial CyberSecurity for Networks. Вы можете получить TLS-сертификат с помощью интерфейса управления Kaspersky Industrial CyberSecurity for Networks.

     - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks. Для использования двусторонней аутентификации вам нужно в параметрах Kaspersky Industrial CyberSecurity for Networks включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. После настройки параметров Kaspersky Industrial CyberSecurity for Networks вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

       Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

9. Для режима **Отправлять телеметрию на диод данных в качестве MQTT-издателя** вам нужно настроить следующие параметры:

   a. Введите учетные данные для аутентификации на сервере MQTT-брокера.

   b. Введите IP-адрес и порт сервера MQTT-брокера.

10. Для режима **Отправлять телеметрию на сервер KICS for Networks по протоколу UDP** настройте следующие параметры:

    a. Введите IP-адрес и порт сервера.

    b. Для включения шифрования данных нажмите на кнопку **Настройки подключения к серверам** и установите флажок **Использовать шифрование при передаче данных по протоколу UDP**.

    > Вам необходимо самостоятельно определить необходимость шифрования передаваемых данных.

    c. Введите пароль от ключа шифрования и загрузите файл ключа шифрования с расширением .PEM.

11. Настройте параметры передачи данных:

    - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечении указанного времени. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.

      > При использовании Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика не рекомендуется настраивать получение данных телеметрии более чем от 250 устройств с Kaspersky Industrial CyberSecurity for Nodes, настроенном в качестве MQTT-издателя, в случае, если в настройках MQTT-издателей задано минимальное значение параметра **Максимальная задержка отправки событий (сек.)** – 1 сек. Если значение параметра равно 30 сек. и более, не рекомендуется настраивать получение данных более чем от 1000 MQTT-издателей.

    - **Включить регулирование количества запросов**. Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечении часа. Диапазон доступных значений: 10–65 535. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. Диапазон доступных значений: 5–100%. Значение по умолчанию – 15%.

    Если необходимо, настройте неизбирательный режим сбора телеметрии. По умолчанию Kaspersky Industrial CyberSecurity for Nodes собирает сетевой трафик, поступающий на сетевые интерфейсы компьютера и предназначенный компьютеру, на котором установлено приложение. В неизбирательном режиме приложение собирает сетевой трафик для сетевых интерфейсов компьютера с установленным приложением со всех доступных подсетей. На основе собранного сетевого трафика приложение формирует расширенную телеметрию.

Не все сетевые адаптеры поддерживают неизбирательный режим сбора телеметрии (англ. Promiscuous mode). На этих сетевых адаптерах сбор расширенной телеметрии не работает.

a. Установите флажок **Включить неизбирательный режим для приложения и сетевых интерфейсов узла**, если хотите, чтобы для всех сетевых интерфейсов компьютера с установленным приложением был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

b. Установите флажок **Использовать в неизбирательном режиме только сетевые интерфейсы узла, настроенные на указанные подсети**, если хотите, чтобы для сетевых интерфейсов компьютера с установленным приложением, настроенных на подсети из списка ниже, был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

c. Если необходимо, сформируйте список подсетей.

12. Сохраните внесенные изменения.

Как настроить интеграцию с Kaspersky Industrial CyberSecurity for Networks в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Серверы сбора телеметрии → Интеграция с KICS for Networks**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Свойства: Интеграция с KICS for Networks** на вкладке **Общие**.

3. Установите флажок **Интеграция с KICS for Networks**.

4. На вкладке **Общие** выберите режим отправки телеметрии:

   - **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию напрямую на сервер Kaspersky Industrial CyberSecurity for Networks по протоколу TCP.

   - **Отправлять телеметрию на диод данных в качестве MQTT-издателя**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию на сервер MQTT-брокера, встроенный в программный диод данных.

   - **Отправлять телеметрию на сервер KICS for Networks по протоколу UDP**. Kaspersky Industrial CyberSecurity for Nodes отправляет телеметрию на сервер Kaspersky Industrial CyberSecurity for Networks через диод данных по протоколу UDP.

5. Для режима **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP** вам нужно настроить следующие параметры:

   - **Адрес** и **Порт**. IP-адрес сервера Kaspersky Industrial CyberSecurity for Networks, в адрес которого отправляется телеметрия, и порт для подключения. Диапазон возможных значений порта: 1–65535. Значение порта по умолчанию – 8081.

   - **Интервал между запросами (мин.)**. Интервал между запросами на сервер Kaspersky Industrial CyberSecurity for Networks в минутах. При работе Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-издателя данный параметр задает интервал между запросами к MQTT-брокеру в случае потери соединения с брокером. Диапазон доступных значений: 1–60 мин. Значение по умолчанию – 1 мин.

- **Настройки подключения к серверам**. Настройте следующие параметры:

  - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечению времени ожидания Kaspersky Industrial CyberSecurity for Nodes повторно подключается к серверу. Диапазон доступных значений: 1–60 000 сек. Значение по умолчанию – 10 сек.

  - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Kaspersky Industrial CyberSecurity for Networks. Вы можете получить TLS-сертификат с помощью интерфейса управления Kaspersky Industrial CyberSecurity for Networks.

  - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks. Для использования двусторонней аутентификации вам нужно в параметрах Kaspersky Industrial CyberSecurity for Networks включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. После настройки параметров Kaspersky Industrial CyberSecurity for Networks вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

    Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

6. Для режима **Отправлять телеметрию на диод данных в качестве MQTT-издателя** вам нужно настроить следующие параметры:

   a. Нажмите на кнопку **Настройки подключения к серверам**.

   b. Введите учетные данные для аутентификации на сервере MQTT-брокера.

   c. Введите IP-адрес и порт сервера MQTT-брокера.

7. Для режима **Отправлять телеметрию на сервер KICS for Networks по протоколу UDP** настройте следующие параметры:

   a. Введите IP-адрес и порт сервера.

   b. Для включения шифрования данных нажмите на кнопку **Настройки подключения к серверам** и установите флажок **Использовать шифрование при передаче данных по протоколу UDP**.

   > Вам необходимо самостоятельно определить необходимость шифрования передаваемых данных.

   c. Введите пароль от ключа шифрования и загрузите файл ключа шифрования с расширением .PEM.

8. Перейдите на вкладку **Передача данных**.

9. Настройте параметры передачи данных:

- **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечении указанного времени. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.

  При использовании Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика не рекомендуется настраивать получение данных телеметрии более чем от 250 устройств с Kaspersky Industrial CyberSecurity for Nodes, настроенном в качестве MQTT-издателя, в случае, если в настройках MQTT-издателей задано минимальное значение параметра **Максимальная задержка отправки событий (сек.)** – 1 сек. Если значение параметра равно 30 сек. и более, не рекомендуется настраивать получение данных более чем от 1000 MQTT-издателей.

- **Включить регулирование количества запросов**. Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

- **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечении часа. Диапазон доступных значений: 10–65 535. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

- **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. Диапазон доступных значений: 5–100%. Значение по умолчанию – 15%.

Если необходимо, настройте неизбирательный режим сбора телеметрии. По умолчанию Kaspersky Industrial CyberSecurity for Nodes собирает сетевой трафик, поступающий на сетевые интерфейсы компьютера и предназначенный компьютеру, на котором установлено приложение. В неизбирательном режиме приложение собирает сетевой трафик для сетевых интерфейсов компьютера с установленным приложением со всех доступных подсетей. На основе собранного сетевого трафика приложение формирует расширенную телеметрию.

Не все сетевые адаптеры поддерживают неизбирательный режим сбора телеметрии (англ. Promiscuous mode). На этих сетевых адаптерах сбор расширенной телеметрии не работает.

a. На вкладке **Сбор телеметрии** установите флажок **Включить неизбирательный режим для приложения и сетевых интерфейсов узла**, если хотите, чтобы для всех сетевых интерфейсов компьютера с установленным приложением был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

b. Установите флажок **Использовать в неизбирательном режиме только сетевые интерфейсы узла, настроенные на указанные подсети**, если хотите, чтобы для сетевых интерфейсов компьютера с установленным приложением, настроенных на подсети из списка ниже, был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

c. Если необходимо, сформируйте список подсетей.

10. Сохраните внесенные изменения.

Также вы можете настроить Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика. В таком режиме приложение получает телеметрию от MQTT-брокера через диод данных для дальнейшей отправки телеметрии в KICS for Networks.

Как настроить приложение в качестве MQTT-подписчика в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит компьютер.

2. В панели результатов перейдите на вкладку **Устройства**.

3. Откройте окно свойств компьютера двойным щелчком мыши.

4. Перейдите в раздел **Приложения**.

5. В списке установленных на компьютере приложений "Лаборатории Касперского" выберите Kaspersky Industrial CyberSecurity for Nodes и откройте свойства приложения двойным щелчком мыши.

6. Выберите раздел **Серверы сбора телеметрии**.

7. В блоке **Интеграция с KICS for Networks** нажмите на кнопку **Настройка**.

   Откроется окно **Интеграция с KICS for Networks**.

8. Установите флажок **Интеграция с KICS for Networks**.

9. На вкладке **Общие** выберите **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP**.

10. Настройте следующие параметры:

- **Адрес** и **Порт**. IP-адрес сервера Kaspersky Industrial CyberSecurity for Networks, в адрес которого отправляется телеметрия, и порт для подключения.

- **Интервал между запросами (мин.)**. Интервал между запросами на сервер Kaspersky Industrial CyberSecurity for Networks в минутах. При работе Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-издателя данный параметр задает интервал между запросами к MQTT-брокеру в случае потери соединения с брокером. Диапазон доступных значений: 1–60 мин. Значение по умолчанию – 1 мин.

- **Настройки подключения к серверам**. Настройте следующие параметры:

  - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечении времени ожидания Kaspersky Industrial CyberSecurity for Nodes повторно подключается к серверу. Диапазон доступных значений: 1–60 000 сек. Значение по умолчанию – 10 сек.

  - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Kaspersky Industrial CyberSecurity for Networks. Вы можете получить TLS-сертификат с помощью интерфейса управления Kaspersky Industrial CyberSecurity for Networks.

  - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks. Для использования двусторонней аутентификации вам нужно в параметрах Kaspersky Industrial CyberSecurity for Networks включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. После настройки параметров Kaspersky Industrial CyberSecurity for Networks вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

    Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

- Установите флажок **Получать телеметрию с диода данных в качестве MQTT-подписчика**.

- Введите учетные данные для аутентификации на сервере MQTT-брокера.

- Введите IP-адрес и порт сервера MQTT-брокера.

11. Перейдите на вкладку **Передача данных**.

12. Настройте параметры передачи данных:

    - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечении указанного времени. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.

      При использовании Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика не рекомендуется настраивать получение данных телеметрии более чем от 250 устройств с Kaspersky Industrial CyberSecurity for Nodes, настроенном в качестве MQTT-издателя, в случае, если в настройках MQTT-издателей задано минимальное значение параметра **Максимальная задержка отправки событий (сек.)** – 1 сек. Если значение параметра равно 30 сек. и более, не рекомендуется настраивать получение данных более чем от 1000 MQTT-издателей.

    - **Включить регулирование количества запросов**. Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

    - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечении часа. Диапазон доступных значений: 10–65 535. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

    - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. Диапазон доступных значений: 5–100%. Значение по умолчанию – 15%.

13. Если необходимо, настройте неизбирательный режим сбора телеметрии.

    По умолчанию Kaspersky Industrial CyberSecurity for Nodes собирает сетевой трафик, поступающий на сетевые интерфейсы компьютера и предназначенный компьютеру, на котором установлено приложение. В неизбирательном режиме приложение собирает сетевой трафик для сетевых интерфейсов компьютера с установленным приложением со всех доступных подсетей. На основе собранного сетевого трафика приложение формирует расширенную телеметрию.

Не все сетевые адаптеры поддерживают неизбирательный режим сбора телеметрии (англ. Promiscuous mode). На этих сетевых адаптерах сбор расширенной телеметрии не работает.

a. На вкладке **Сбор телеметрии** установите флажок **Включить неизбирательный режим для приложения и сетевых интерфейсов узла**, если хотите, чтобы для всех сетевых интерфейсов компьютера с установленным приложением был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

b. Установите флажок **Использовать в неизбирательном режиме только сетевые интерфейсы узла, настроенные на указанные подсети**, если хотите, чтобы для сетевых интерфейсов компьютера с установленным приложением, настроенных на подсети из списка ниже, был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

c. Если необходимо, сформируйте список подсетей.

14. Сохраните внесенные изменения.

Как настроить приложение в качестве MQTT-подписчика в Web Console

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.
2. Нажмите на нужное имя компьютера.
3. В открывшемся окне свойств компьютера выберите вкладку **Приложения**.
4. Нажмите на **Kaspersky Industrial CyberSecurity for Nodes (5.0.0)**.
5. Выберите вкладку **Параметры приложения**.
6. Выберите раздел **Серверы сбора телеметрии**.
7. В блоке **Интеграция с KICS for Networks** нажмите на кнопку **Настроить**.

   Откроется окно **Интеграция с KICS for Networks**.
8. Установите флажок **Интеграция с KICS for Networks**.
9. На вкладке **Общие** выберите **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP**.
10. Настройте следующие параметры:

    - **Адрес** и **Порт**. IP-адрес сервера Kaspersky Industrial CyberSecurity for Networks, в адрес которого отправляется телеметрия, и порт для подключения.
    - **Интервал между запросами (мин.)**. Интервал между запросами на сервер Kaspersky Industrial CyberSecurity for Networks в минутах. При работе Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-издателя данный параметр задает интервал между запросами к MQTT-брокеру в случае потери соединения с брокером. Диапазон доступных значений: 1–60 мин. Значение по умолчанию – 1 мин.

- **Настройки подключения к серверам**. Настройте следующие параметры:

  - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечении времени ожидания Kaspersky Industrial CyberSecurity for Nodes повторно подключается к серверу. Диапазон доступных значений: 1–60 000 сек. Значение по умолчанию – 10 сек.

  - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Kaspersky Industrial CyberSecurity for Networks. Вы можете получить TLS-сертификат с помощью интерфейса управления Kaspersky Industrial CyberSecurity for Networks.

  - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks. Для использования двусторонней аутентификации вам нужно в параметрах Kaspersky Industrial CyberSecurity for Networks включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. После настройки параметров Kaspersky Industrial CyberSecurity for Networks вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

    Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

- Установите флажок **Получать телеметрию с диода данных в качестве MQTT-подписчика**.

- Введите учетные данные для аутентификации на сервере MQTT-брокера.

- Введите IP-адрес и порт сервера MQTT-брокера.

11. Настройте параметры передачи данных:

- **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечении указанного времени. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.

  При использовании Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика не рекомендуется настраивать получение данных телеметрии более чем от 250 устройств с Kaspersky Industrial CyberSecurity for Nodes, настроенном в качестве MQTT-издателя, в случае, если в настройках MQTT-издателей задано минимальное значение параметра **Максимальная задержка отправки событий (сек.)** – 1 сек. Если значение параметра равно 30 сек. и более, не рекомендуется настраивать получение данных более чем от 1000 MQTT-издателей.

- **Включить регулирование количества запросов**. Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

- **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечении часа. Диапазон доступных значений: 10–65 535. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

- **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. Диапазон доступных значений: 5–100%. Значение по умолчанию – 15%.

12. Если необходимо, настройте неизбирательный режим сбора телеметрии.

    По умолчанию Kaspersky Industrial CyberSecurity for Nodes собирает сетевой трафик, поступающий на сетевые интерфейсы компьютера и предназначенный компьютеру, на котором установлено приложение. В неизбирательном режиме приложение собирает сетевой трафик для сетевых интерфейсов компьютера с установленным приложением со всех доступных подсетей. На основе собранного сетевого трафика приложение формирует расширенную телеметрию.

    > Не все сетевые адаптеры поддерживают неизбирательный режим сбора телеметрии (англ. Promiscuous mode). На этих сетевых адаптерах сбор расширенной телеметрии не работает.

    a. Установите флажок **Включить неизбирательный режим для приложения и сетевых интерфейсов узла**, если хотите, чтобы для всех сетевых интерфейсов компьютера с установленным приложением был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

    b. Установите флажок **Использовать в неизбирательном режиме только сетевые интерфейсы узла, настроенные на указанные подсети**, если хотите, чтобы для сетевых интерфейсов компьютера с установленным приложением, настроенных на подсети из списка ниже, был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

    c. Если необходимо, сформируйте список подсетей.

13. Сохраните внесенные изменения.

Как настроить приложение в качестве MQTT-подписчика в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Серверы сбора телеметрии → Интеграция с KICS for Networks**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Свойства: Интеграция с KICS for Networks** на вкладке **Общие**.

3. Установите флажок **Интеграция с KICS for Networks**.

4. На вкладке **Общие** выберите **Отправлять телеметрию на сервер KICS for Networks по протоколу TCP**.

5. Настройте следующие параметры:

- **Адрес** и **Порт**. IP-адрес сервера Kaspersky Industrial CyberSecurity for Networks, в адрес которого отправляется телеметрия, и порт для подключения.

- **Интервал между запросами (мин.)**. Интервал между запросами на сервер Kaspersky Industrial CyberSecurity for Networks в минутах. При работе Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-издателя данный параметр задает интервал между запросами к MQTT-брокеру в случае потери соединения с брокером. Диапазон доступных значений: 1–60 мин. Значение по умолчанию – 1 мин.

- **Настройки подключения к серверам**. Настройте следующие параметры:

  - **Время ожидания (сек.)**. Максимальное время ожидания ответа от сервера. По истечении времени ожидания Kaspersky Industrial CyberSecurity for Nodes повторно подключается к серверу. Диапазон доступных значений: 1–60 000 сек. Значение по умолчанию – 10 сек.

  - **TLS-сертификат сервера**. TLS-сертификат для установки доверенного соединения с сервером Kaspersky Industrial CyberSecurity for Networks. Вы можете получить TLS-сертификат с помощью интерфейса управления Kaspersky Industrial CyberSecurity for Networks.

  - **Использовать двустороннюю аутентификацию**. Двусторонняя аутентификация при установлении безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks. Для использования двусторонней аутентификации вам нужно в параметрах Kaspersky Industrial CyberSecurity for Networks включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. После настройки параметров Kaspersky Industrial CyberSecurity for Networks вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes также включить функцию двусторонней аутентификации и загрузить защищенный паролем криптоконтейнер.

    Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

- Установите флажок **Получать телеметрию с диода данных в качестве MQTT-подписчика**.

- Введите учетные данные для аутентификации на сервере MQTT-брокера.

- Введите IP-адрес и порт сервера MQTT-брокера.

6. Перейдите на вкладку **Передача данных**.

7. Настройте параметры передачи данных:

   - **Максимальная задержка отправки событий (сек.)**. Приложение выполняет синхронизацию с сервером для передачи событий по истечении указанного времени. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.

     При использовании Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика не рекомендуется настраивать получение данных телеметрии более чем от 250 устройств с Kaspersky Industrial CyberSecurity for Nodes, настроенном в качестве MQTT-издателя, в случае, если в настройках MQTT-издателей задано минимальное значение параметра **Максимальная задержка отправки событий (сек.)** – 1 сек. Если значение параметра равно 30 сек. и более, не рекомендуется настраивать получение данных более чем от 1000 MQTT-издателей.

   - **Включить регулирование количества запросов**. Функция позволяет оптимизировать нагрузку на сервер. Если флажок установлен, приложение будет ограничивать передачу событий. Если количество событий превышает установленные ограничения, Kaspersky Industrial CyberSecurity for Nodes прекращает отправлять события.

   - **Максимальное количество событий в час**. Приложение анализирует поток данных телеметрии и ограничивает передачу событий, если поток передаваемых событий превышает установленное ограничение в час. Kaspersky Industrial CyberSecurity for Nodes восстанавливает передачу событий по истечении часа. Диапазон доступных значений: 10–65 535. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.

   - **Процент превышения лимита событий**. Приложение сортирует события по типу (например, события изменений в реестре) и ограничивает передачу событий, если соотношение однотипных событий к общему количеству событий превышает установленное ограничение в процентах. Kaspersky Industrial CyberSecurity for Nodes восстанавливает отправку событий, когда соотношение других событий к общему количеству событий увеличится. Диапазон доступных значений: 5–100%. Значение по умолчанию – 15%.

8. Если необходимо, настройте неизбирательный режим сбора телеметрии.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes собирает сетевой трафик, поступающий на сетевые интерфейсы компьютера и предназначенный компьютеру, на котором установлено приложение. В неизбирательном режиме приложение собирает сетевой трафик для сетевых интерфейсов компьютера с установленным приложением со всех доступных подсетей. На основе собранного сетевого трафика приложение формирует расширенную телеметрию.

Не все сетевые адаптеры поддерживают неизбирательный режим сбора телеметрии (англ. Promiscuous mode). На этих сетевых адаптерах сбор расширенной телеметрии не работает.

a. На вкладке **Сбор телеметрии** установите флажок **Включить неизбирательный режим для приложения и сетевых интерфейсов узла**, если хотите, чтобы для всех сетевых интерфейсов компьютера с установленным приложением был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

b. Установите флажок **Использовать в неизбирательном режиме только сетевые интерфейсы узла, настроенные на указанные подсети**, если хотите, чтобы для сетевых интерфейсов компьютера с установленным приложением, настроенных на подсети из списка ниже, был включен неизбирательный режим получения сетевого трафика со всех доступных подсетей.

c. Если необходимо, сформируйте список подсетей.

9. Сохраните внесенные изменения.

При необходимости вы можете настроить интеграцию с Kaspersky Industrial CyberSecurity for Networks через интерфейс командной строки.

Особенности работы и ограничения интеграции с Kaspersky Industrial CyberSecurity for Networks

Изменение параметров политики аудита

Для корректной работы интеграции с Kaspersky Industrial CyberSecurity for Networks необходимо изменение параметров политики аудита. Поведение приложения различается в зависимости от того, входит устройство в домен или нет:

- Если устройство не входит в домен, приложение при необходимости автоматически изменяет параметры локальной политики.
- Если устройство входит в домен, приложение не меняет параметры групповой политики домена. Вы можете исключить данное устройство из домена или настроить параметры групповой политики домена самостоятельно:
  - Для подкатегории **Аудит управления учетными записями пользователей** (**Audit User Account Management**) активируйте параметр **Успех** (**Success**).
  - Для подкатегорий **Аудит входа в систему** (**Audit Logon**), **Аудит выхода из системы** (**Audit Logoff**) и **Аудит других событий входа и выхода** (**Audit Other Logon/Logoff Events**) активируйте параметры **Успех** (**Success**) и **Отказ** (**Failure**).

Ограничения интеграции с Kaspersky Industrial CyberSecurity for Networks

Функциональность интеграции с Kaspersky Industrial CyberSecurity for Networks имеет следующие ограничения:

- Отправка телеметрии на сервер MQTT-брокера недоступна на компьютерах под управлением Windows XP.
- Отсутствует гарантия доставки сообщений, полученных Kaspersky Industrial CyberSecurity for Nodes с диода данных во время отсутствия соединения с сервером Kaspersky Industrial CyberSecurity for Networks.
- Функционал мониторинга сетей Wi-Fi поддерживается в сетях, использующих протокол IPv4. Устройства с IPv6-адресами обнаружены не будут.
- Для Wi-Fi сетей со скрытым SSID недоступен сбор данных об используемых стандартах защиты и протоколах шифрования, а также стандартах роуминга.
- При сканировании сетей Wi-Fi приложение использует следующие протоколы: DHCP, ICMP, ARP, mDNS, UPnP, NetBIOS. Для корректной работы приложения вам нужно разрешить использование данных протоколов в вашей сети.
- На защищаемых устройствах под управлением Windows 11, Windows Server 2025 и выше для сбора данных о сетях Wi-Fi нужно включить службу определения местоположения в параметрах операционной системы. Если служба определения местоположения выключена, Kaspersky Industrial CyberSecurity for Nodes не собирает и не отправляет в Kaspersky Industrial CyberSecurity for Networks данные о сетях Wi-Fi.
- Сбор данных о сетях Wi-Fi недоступен на устройствах под управлением операционных систем версий ниже Windows Vista.

Настройка мониторинга сетей Wi-Fi

Вы можете настроить отправку на сервер Kaspersky Industrial CyberSecurity for Networks данных о сетях Wi-Fi, обнаруженных защищаемым устройством с установленным Kaspersky Industrial CyberSecurity for Nodes, и данных об устройствах, которые подключены к той же сети Wi-Fi, что и защищаемое устройство. Собранные данные Kaspersky Industrial CyberSecurity for Networks использует для централизованного мониторинга сетей Wi-Fi в вашей инфраструктуре. Подробнее см. в справке Kaspersky Industrial CyberSecurity for Networks.

Для снижения нагрузки на сетевую инфраструктуру рекомендуется включать сбор данных о сетях Wi-Fi только на тех устройствах, которые необходимы для обеспечения полноты собираемых данных.

Вы можете настроить сбор и отправку данных о сетях Wi-Fi только из Консоли администрирования Kaspersky Security Center и Web Console. В Консоли приложения доступен только просмотр текущих настроек.

Как настроить сбор и отправку данных о сетях Wi-Fi в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. Выберите раздел **Серверы сбора телеметрии**.

4. В блоке **Интеграция с KICS for Networks** нажмите на кнопку **Настройка**.

   Откроется окно **Интеграция с KICS for Networks**.

5. Перейдите на вкладку **Настройки контроля сетей и устройств**.

6. Настройте параметры контроля сетей Wi-Fi:

   - **Обнаруживать сети Wi-Fi**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes собирает и отправляет в Kaspersky Industrial CyberSecurity for Networks информацию о сетях Wi-Fi, доступных на защищаемом устройстве. По умолчанию функция выключена.

   - **Обнаруживать проводные и беспроводные устройства в подключенной сети**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes собирает и отправляет в Kaspersky Industrial CyberSecurity for Networks информацию об устройствах, подключенных к той же сети Wi-Fi, что и защищаемое устройство. По умолчанию функция выключена.

7. При необходимости измените заданные по умолчанию параметры сбора и отправки данных:

   - **Выполнять каждые (минут)**. Укажите период сканирования в минутах. Диапазон доступных значений: 1–150 мин. Значение по умолчанию – 5 минут.

   - **Отправлять данные на сервер каждые (минут)**. Укажите период отправки данных на сервер в минутах. Диапазон доступных значений: 1–150 мин. Значение по умолчанию – 10 минут.

     > Период сканирования должен быть меньше периода отправки данных.

     Если за один период отправки приложение выполняет несколько сканирований, собранные данные агрегируются по следующим правилам:

     - В агрегированных данных в качестве уникальных идентификаторов объектов сканирования используются MAC-адреса.

     - Для каждого объекта сканирования в агрегированные данные попадает информация, полученная при последнем за период сканировании.

     - Если сканирующее устройство переключалось между несколькими сетями W-Fi, в агрегированных данных будет содержаться только информация, собранная с последней за текущий период отправки сети.

     - Если объект сканирования перестает обнаруживаться, в агрегированные данные попадет последняя собранная о нем информация с отметкой о времени последнего обнаружения.

     - При смене SSID сети Wi-Fi данные, связанные с предыдущим SSID, не сохраняются. В агрегированных данных остается только информация, связанная с последним SSID.

8. Сохраните внесенные изменения.

Как настроить сбор и отправку данных о сетях Wi-Fi в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Серверы сбора телеметрии**.
5. В блоке **Интеграция с KICS for Networks** нажмите на кнопку **Настроить**.

   Откроется окно **Интеграция с KICS for Networks**.
6. В блоке **Настройки контроля сетей и устройств** настройте параметры контроля сетей Wi-Fi:

   - **Обнаруживать сети Wi-Fi**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes собирает и отправляет в Kaspersky Industrial CyberSecurity for Networks информацию о сетях Wi-Fi, доступных на защищаемом устройстве. По умолчанию функция выключена.
   - **Обнаруживать проводные и беспроводные устройства в подключенной сети**. Если функция включена, Kaspersky Industrial CyberSecurity for Nodes собирает и отправляет в Kaspersky Industrial CyberSecurity for Networks информацию об устройствах, подключенных к той же сети Wi-Fi, что и защищаемое устройство. По умолчанию функция выключена.
7. При необходимости измените заданные по умолчанию параметры сбора и отправки данных:

   - **Выполнять каждые (минут)**. Укажите период сканирования в минутах. Диапазон доступных значений: 1–150 мин. Значение по умолчанию – 5 минут.
   - **Отправлять данные на сервер каждые (минут)**. Укажите период отправки данных на сервер в минутах. Диапазон доступных значений: 1–150 мин. Значение по умолчанию – 10 минут.

     > Период сканирования должен быть меньше периода отправки данных.

     Если за один период отправки приложение выполняет несколько сканирований, собранные данные агрегируются по следующим правилам:

     - В агрегированных данных в качестве уникальных идентификаторов объектов сканирования используются MAC-адреса.
     - Для каждого объекта сканирования в агрегированные данные попадает информация, полученная при последнем за период сканировании.
     - Если сканирующее устройство переключалось между несколькими сетями W-Fi, в агрегированных данных будет содержаться только информация, собранная с последней за текущий период отправки сети.

- Если объект сканирования перестает обнаруживаться, в агрегированные данные попадет последняя собранная о нем информация с отметкой о времени последнего обнаружения.

- При смене SSID сети Wi-Fi данные, связанные с предыдущим SSID, не сохраняются. В агрегированных данных остается только информация, связанная с последним SSID.

8. Сохраните внесенные изменения.

Мониторинг EDR-действий

Единый центр мониторинга EDR-действий – это консоль, в которой представлена история реагирования на угрозы от всех решений Detection and Response от "Лаборатории Касперского". Если в вашей организации развернуто несколько решений Detection and Response, то Kaspersky Industrial CyberSecurity for Nodes покажет историю реагирования на угрозы для всех решений. Таким образом, вы сможете проанализировать работу решений Detection and Response на отдельном компьютере и оптимизировать параметры этих решений.

Центр мониторинга предоставляет следующие данные:

- информация о задачах по реагированию на угрозы (например, задача *Завершение процесса*);

- изменения правил компонентов Сетевой изоляции и Запрета запуска объектов.

Если в процессе реагирования на угрозу возникает ошибка, связанная с доступом к сетевой папке, такая ошибка не будет отображаться в истории реагирования на угрозы.

Чтобы открыть Единый центр мониторинга EDR-действий:

1. В главном окне Web Console выберите **Управление активами → Активы (Устройства)**.

2. Нажмите на имя компьютера, для которого вы хотите просмотреть историю реагирования на угрозы.

   Откроется окно свойств компьютера.

3. Выберите вкладку **Приложения**.

4. Нажмите на **Kaspersky Industrial CyberSecurity for Nodes (5.0.0)**.

   Откроются локальные параметры приложения.

5. Выберите вкладку **Параметры приложения**.

6. Перейдите в раздел **Серверы сбора телеметрии → История реагирования**.

   Откроется консоль Единого центра мониторинга EDR-действий. В консоли вы можете просмотреть статус задач по реагированию на угрозы, время выполнения этих задач, изменения в правилах, а также данные об инициаторе.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent обеспечивает взаимодействие приложения с другими решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, Kaspersky Anti Targeted Attack Platform). Решения "Лаборатории Касперского", которые поддерживает Kaspersky Endpoint Agent, зависят от версии Kaspersky Endpoint Agent.

Для работы Kaspersky Endpoint Agent в составе решений "Лаборатории Касперского" необходимо активировать эти решения соответствующим лицензионным ключом.

Kaspersky Endpoint Agent поддерживает взаимодействие со следующими решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, целевых атак):

- Kaspersky Industrial CyberSecurity Endpoint Detection and Response (поддерживает Kaspersky Endpoint Agent 3.9 и выше).
- Kaspersky Anti Targeted Attack Platform (поддерживает Kaspersky Endpoint Agent 3.8 и выше).
- Kaspersky Managed Detection and Response.

В комплект поставки Kaspersky Industrial CyberSecurity for Nodes версии 4.0 включено приложение Kaspersky Endpoint Agent, для более ранних версий приложения дистрибутив Kaspersky Endpoint Agent можно запрашивать у менеджера по технической поддержке (TAM). Начиная с версии 4.5 комплект поставки Kaspersky Industrial CyberSecurity for Nodes не содержит дистрибутив приложения Kaspersky Endpoint Agent. В Kaspersky Industrial CyberSecurity for Nodes версии 4.5 включен встроенный агент, с помощью которого приложение поддерживает работу с решениями Detection and Response. Установить оба приложения на одном компьютере невозможно.

Миграция конфигурации [KICS+KEA] на [KICS+встроенный Enpoint Agent]

Начиная с версии 4.5 Kaspersky Industrial CyberSecurity for Nodes включает в себя встроенный агент для работы решений Detection and Response. Теперь вам не нужно отдельное приложение Kaspersky Endpoint Agent для работы этих решений. При развертывании Kaspersky Industrial CyberSecurity for Nodes на компьютеры с установленным Kaspersky Endpoint Agent решения Detection and Response продолжат работу с Kaspersky Industrial CyberSecurity for Nodes, а приложение Kaspersky Endpoint Agent удаляется с компьютера.

Миграция конфигурации [KICS+KEA] на [KICS+встроенный агент] состоит из следующих этапов:

1. **Обновление Kaspersky Security Center**

   Обновите все компоненты Kaspersky Security Center до версии 14.2 или выше, включая Агент администрирования на компьютерах пользователей.

2. **Установка / Обновление приложения Kaspersky Industrial CyberSecurity for Nodes до версии 5.0**

   Если вы устанавливаете приложение, в параметрах инсталляционного пакета или мастере установки приложения вместе с другими необходимыми компонентами выберите для установки **Полная функциональность → Endpoint Agent**.

Если вы обновляете приложение, Kaspersky Industrial CyberSecurity for Nodes поддерживает автоматический выбор компонентов на компьютере с установленным приложением Kaspersky Endpoint Agent. Автоматический выбор компонентов зависит от прав учетной записи пользователя, который обновляет приложение.

Если вы обновляете Kaspersky Industrial CyberSecurity for Nodes с помощью EXE-файла или с помощью MSI-файла под системной учетной записью (SYSTEM), Kaspersky Industrial CyberSecurity for Nodes получает доступ к действующим лицензиям решений "Лаборатории Касперского". Таким образом, если на компьютере, например, установлено приложение Kaspersky Endpoint Agent и активировано решение EDR Optimum, установщик Kaspersky Industrial CyberSecurity for Nodes автоматически сконфигурирует набор компонентов и выберет компонент EDR Optimum. При этом Kaspersky Industrial CyberSecurity for Nodes перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent. Запуск установщика MSI под системной учетной записью (SYSTEM) обычно выполняется при обновлении через службу обновлений "Лаборатории Касперского" (SMU) или при развертывании инсталляционного пакета через Kaspersky Security Center.

Если вы обновляете Kaspersky Industrial CyberSecurity for Nodes с помощью MSI-файла под учетной записью непривилегированного пользователя, у Kaspersky Industrial CyberSecurity for Nodes отсутствует доступ к действующим лицензиям решений "Лаборатории Касперского". При этом Kaspersky Industrial CyberSecurity for Nodes автоматически выбирает компоненты на основании конфигурации Kaspersky Endpoint Agent. Далее Kaspersky Industrial CyberSecurity for Nodes перейдет на работу со встроенным агентом и удалит Kaspersky Endpoint Agent.

3. **Лицензирование функций**

   Если для активации Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Endpoint Agent у вас общая лицензия Kaspersky Endpoint Detection and Response Optimum, после обновления приложения до версии 5.0 активация функции EDR Optimum будет выполнена автоматически. Дополнительных действий не требуется.

   Если для активации функциональности EDR Optimum у вас отдельная лицензия EDR Optimum Add-on, вам нужно убедиться, что ключ EDR Optimum Add-on добавлен в хранилище Kaspersky Security Center и функция автоматического распространения лицензионного ключа включена. После обновления приложения до версии 5.0 активация функции EDR Optimum будет выполнена автоматически.

   Если для активации Kaspersky Endpoint Agent у вас лицензия Kaspersky Endpoint Detection and Response Optimum, а для активации Kaspersky Industrial CyberSecurity for Nodes у вас другая лицензия, вам нужно заменить ключ для Kaspersky Industrial CyberSecurity for Nodes на общий ключ Kaspersky Endpoint Detection and Response Optimum. Вы можете заменить ключ с помощью задачи *Добавление ключа*.

4. **Обновление Веб-плагина Kaspersky Industrial CyberSecurity for Nodes**

   В Kaspersky Security Center Web Console обновите Веб-плагин Kaspersky Industrial CyberSecurity for Nodes до версии 5.0.

5. **Миграция политики и задач**

   С помощью мастера миграции политик и задач перенесите параметры работы Kaspersky Endpoint Agent в приложение Kaspersky Industrial CyberSecurity for Nodes.

Миграция политик и задач конфигурации [KICS+KEA] на [KICS+встроенный агент]

С помощью мастера миграции политик и задач Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Endpoint Agent версий 4.0 и ниже до Kaspersky Industrial CyberSecurity for Nodes 5.0 со встроенным агентом вы можете перенести настройки политик и задач для следующих решений:

- Kaspersky Industrial CyberSecurity Endpoint Detection and Response;
- Kaspersky Anti Targeted Attack Platform (EDR).

Мастер миграции политик и задач доступен только в Web Console и Cloud Console.

Рекомендуем сначала выполнить миграцию политик и задач конфигурации [KICS+KEA] на [KICS+встроенный агент] на одном компьютере, затем на группе компьютеров и далее выполнить миграцию на всех компьютерах организации.

Чтобы перенести параметры политик и задач конфигурации [KICS+KEA] на [KICS+встроенный агент],

в главном окне Web Console или Cloud Console выберите **Операции → Миграция на Kaspersky Industrial CyberSecurity for Nodes 5.0.0**.

В результате запустится мастер миграции политик и задач. Следуйте его указаниям.

Шаг 1. Миграция политик

Выберите политики Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Endpoint Agent, параметры которых вы хотите объединить.

Убедитесь, что политики выбраны верно, и перейдите к следующему шагу.

Шаг 2. Миграция задач

В списке задач выберите задачи Kaspersky Industrial CyberSecurity for Nodes, которые вы хотите создать для Kaspersky Industrial CyberSecurity for Nodes 5.0.

Перейдите к следующему шагу.

Шаг 3. Завершение работы мастера

Завершите работу мастера. В результате работы мастера будут выполнены следующие действия:

- Созданы новые политики для Kaspersky Industrial CyberSecurity for Nodes 5.0.

В политиках объединены параметры Kaspersky Industrial CyberSecurity for Nodes предыдущих версий и Kaspersky Endpoint Agent. Названия новых политик повторяют названия политик Kaspersky Industrial CyberSecurity for Nodes до объединения с добавлением фразы "скопирована из KICS". Новые политики имеют статус *Неактивна*. Для продолжения работы активируйте новую объединенную политику.

При миграции с Kaspersky Endpoint Agent на Kaspersky Industrial CyberSecurity for Nodes для решения Kaspersky Anti Targeted Attack Platform (EDR) могут возникнуть ошибки подключения компьютера к серверам KATA. Это связано с тем, что мастер миграции пропускает и не переносит следующие настройки политики:

- Запрет на изменение настроек подключения ("замок").

  По умолчанию изменение настроек разрешено ("замок" открыт), поэтому настройки не будут применены на компьютере. Вам нужно запретить изменение настроек и закрыть "замок".

- Криптоконтейнер.

  Если вы используете двустороннюю аутентификацию для подключения к серверам KATA, нужно добавить криптоконтейнер повторно. TLS-сертификат сервера мастер миграции переносит корректно.

- Созданы новые задачи для Kaspersky Industrial CyberSecurity for Nodes 5.0.

  В новых задачах перенесены значения настроек из мигрированных задач Kaspersky Industrial CyberSecurity for Nodes и добавлены новые настройки, которые появились в Kaspersky Industrial CyberSecurity for Nodes 5.0. Названия новых задач повторяют названия задач Kaspersky Industrial CyberSecurity for Nodes до миграции с добавлением фразы "скопирована из KICS".

Интеграция с SIEM

Kaspersky Industrial CyberSecurity for Nodes позволяет подключаться к SIEM-системам, чтобы отправлять события для их анализа и последующего реагирования на потенциальные угрозы. SIEM-система позволяет обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб организации.

Интеграция с SIEM подразумевает, что приложение Kaspersky Industrial CyberSecurity for Nodes, установленное на защищаемых устройствах под управлением операционных систем Windows, может отправлять на SIEM-сервер следующие события Kaspersky Industrial CyberSecurity for Nodes:

- События безопасности. Поддерживается конвертация событий в форматы JSON Lines и Syslog (RFC 5424). Вы можете выбрать события, которые приложение будет отправлять на SIEM-сервер.
- События Журнала событий Windows (Windows Event Log). Приложение конвертирует события Windows Event Log в формат JSON Lines. При необходимости вы можете исключить события из отправляемой телеметрии с помощью правил фильтрации.

  Kaspersky Industrial CyberSecurity for Nodes, установленное на защищаемых устройствах под управлением Windows XP, не поддерживает отправку событий Windows Event Log.

Kaspersky Industrial CyberSecurity for Nodes поддерживает следующие протоколы для отправки событий на SIEM-серверы:

- TCP;
- UDP;
- HTTP/HTTPS (только для отправки событий Windows Event Log).

Интеграция с SIEM состоит из следующих этапов:

1. **Установка компонента Интеграция с SIEM**

   В параметрах инсталляционного пакета или мастере установки приложения, а также с помощью изменения состава компонентов приложения через Панель управления Windows, на этапе выбора компонентов приложения для установки выберите **Полная функциональность** → **Endpoint Agent** → **Интеграция с SIEM**.

2. **Включение и настройка компонента Интеграция с SIEM**

   Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры.

   Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к нескольким SIEM-серверам. Kaspersky Industrial CyberSecurity for Nodes подключается к первому серверу SIEM из списка. Если подключиться не удается, Kaspersky Industrial CyberSecurity for Nodes последовательно пытается установить соединение с другими серверами из списка. Также Kaspersky Industrial CyberSecurity for Nodes использует события системного аудита для уведомления о неудачных попытках подключения к SIEM-серверу и об ошибках отправки событий на SIEM-сервер.

   Как настроить интеграцию с SIEM в Консоли администрирования Kaspersky Security Center

   1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
   2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. Выберите раздел **Серверы сбора телеметрии**.

4. В блоке **Интеграция с SIEM** нажмите на кнопку **Настройка**.

   Откроется окно **Интеграция с SIEM**.

5. Установите флажок **Интеграция с SIEM**.

6. Настройте подключение к SIEM-серверам для отправки событий безопасности:

   a. Перейдите на вкладку **Настройки отправки событий безопасности**.

   b. Нажмите на кнопку **Добавить**.

   c. В открывшемся окне **Добавление сервера** введите адрес сервера SIEM (IPv4, DNS), порт и протокол подключения к серверу.

   d. Нажмите на кнопку **Настройки безопасности TCP-соединения**.

   e. В открывшемся окне **Настройки безопасности TCP-соединения** настройте параметры подключения к SIEM-серверам (см. таблицу ниже).

   f. Если требуется, в блоке **Настройки отправки событий на сервер SIEM** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**. Если флажок установлен, приложение удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах. Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально. По умолчанию флажок снят.

   > Приложение никогда не удаляет локальные версии журнала безопасности.

   g. В блоке **Формат событий** выберите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер:

   - **Конвертировать события в формат структурированных данных** (значение по умолчанию). Приложение будет отправлять события в формате Syslog (RFC 5424).
   - **Конвертировать события в формат JSON**. Приложение будет отправлять события в формате JSON Lines.

   Рекомендуется выбирать формат событий на основе конфигурации используемого SIEM-сервера.

7. Настройте подключение к SIEM-серверам для отправки событий Windows Event Log:

   a. Перейдите на вкладку **Настройки отправки событий Windows**.

   b. В блоке **Настройки подключения к серверам SIEM** установите флажок **Использовать шифрование TLS**, если необходимо включить шифрование соединения между Kaspersky Industrial CyberSecurity for Nodes и серверами SIEM.

   c. Нажмите на кнопку **Добавить**.

   d. В открывшемся окне **Сервер SIEM** введите адрес сервера SIEM (IPv4, DNS), порт и протокол подключения к серверу.

e. Нажмите на кнопку **Настройки подключения к серверам SIEM**.

f. В открывшемся окне **Настройки подключения к серверам SIEM** настройте параметры подключения к SIEM-серверам (см. таблицу ниже).

g. Если требуется, в блоке **Настройка передачи данных** настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Industrial CyberSecurity for Nodes повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. По умолчанию установлено значение 30 секунд.

Приложение будет отправлять события Windows Event Log на SIEM-сервер в формате JSON Lines.

8. Закройте замок для применения политики на компьютерах.

9. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как настроить интеграцию с SIEM в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Серверы сбора телеметрии**.

5. В блоке **Интеграция с SIEM** нажмите на кнопку **Настроить**.

Откроется окно **Интеграция с SIEM**.

6. Установите флажок **Включить Интеграцию с SIEM**.

7. Настройте подключение к SIEM-серверам для отправки событий безопасности:

a. Перейдите на вкладку **Настройки отправки событий безопасности**.

b. Нажмите на кнопку **Добавить**.

c. В открывшемся окне **Сервер SIEM** введите адрес сервера SIEM (IPv4, DNS), порт и протокол подключения к серверу.

d. В блоке **Защита соединения** нажмите на ссылку **Настройки подключения к серверам SIEM**.

e. В открывшемся окне **Настройки подключения к серверам SIEM** настройте параметры подключения к SIEM-серверам (см. таблицу ниже).

f. В разделе **Формат событий** выберите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер:

- **Конвертировать события в формат структурированных данных** (значение по умолчанию). Приложение будет отправлять события в формате Syslog (RFC 5424).

- **Конвертировать события в формат JSON**. Приложение будет отправлять события в формате JSON Lines.

Рекомендуется выбирать формат событий на основе конфигурации используемого SIEM-сервера.

g. Если требуется, в блоке **Настройки подключения** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**. Если флажок установлен, приложение удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах. Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально. По умолчанию флажок снят.

> Приложение никогда не удаляет локальные версии журнала безопасности.

8. Настройте подключение к SIEM-серверам для отправки событий Windows Event Log:

   a. Перейдите на вкладку **Настройки отправки событий Windows**.

   b. Нажмите на кнопку **Добавить**.

   c. В открывшемся окне **Сервер SIEM** введите адрес сервера SIEM (IPv4, DNS), порт и протокол подключения к серверу.

   d. В блоке **Защита соединения** нажмите на ссылку **Настройки подключения к серверам SIEM**.

   e. В открывшемся окне **Настройки подключения к серверам SIEM** настройте параметры подключения к SIEM-серверам (см. таблицу ниже).

   f. Если требуется, в блоке **Настройки подключения** настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Industrial CyberSecurity for Nodes повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. По умолчанию установлено значение 30 секунд.

   Приложение будет отправлять события Windows Event Log на SIEM-сервер в формате JSON Lines.

9. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Как настроить интеграцию с SIEM в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Телеметрия Endpoint Agent → Интеграция с SIEM**.

2. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Свойства: Интеграция с SIEM**.

3. Установите флажок **Интеграция с SIEM**.

4. Настройте подключение к SIEM-серверам для отправки событий безопасности:

   a. Перейдите на вкладку **Настройки отправки событий безопасности**.

   b. Нажмите на кнопку **Добавить**.

   c. В открывшемся окне **Добавление сервера** введите адрес сервера SIEM (IPv4, DNS), порт и протокол подключения к серверу.

   d. Нажмите на кнопку **Настройки безопасности TCP-соединения**.

e. В открывшемся окне **Настройки безопасности TCP-соединения** настройте параметры подключения к SIEM-серверам (см. таблицу ниже).

f. Если требуется, в блоке **Настройки отправки событий на сервер SIEM** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**. Если флажок установлен, приложение удаляет локальные копии событий после того, как они были успешно опубликованы на SIEM-сервере. Рекомендуется использовать этот режим на маломощных устройствах. Если флажок снят, программа только отправляет события на SIEM-сервер. Копии журналов продолжают храниться локально. По умолчанию флажок снят.

Приложение никогда не удаляет локальные версии журнала безопасности.

g. В блоке **Формат событий** выберите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер:

- **Конвертировать события в формат структурированных данных** (значение по умолчанию). Приложение будет отправлять события в формате Syslog (RFC 5424).
- **Конвертировать события в формат JSON**. Приложение будет отправлять события в формате JSON Lines.

Рекомендуется выбирать формат событий на основе конфигурации используемого SIEM-сервера.

5. Настройте подключение к SIEM-серверам для отправки событий Windows Event Log:

a. Перейдите на вкладку **Настройки отправки событий Windows**.

b. В блоке **Настройки подключения к серверам SIEM** установите флажок **Использовать шифрование TLS**, если необходимо включить шифрование соединения между Kaspersky Industrial CyberSecurity for Nodes и серверами SIEM.

c. Нажмите на кнопку **Добавить**.

d. В открывшемся окне **Сервер SIEM** введите адрес сервера SIEM (IPv4, DNS), порт и протокол подключения к серверу.

e. Нажмите на кнопку **Настройки подключения к серверам SIEM**.

f. В открывшемся окне **Настройки подключения к серверам SIEM** настройте параметры подключения к SIEM-серверам (см. таблицу ниже).

g. Если требуется, в блоке **Настройка передачи данных** настройте параметр **Максимальная задержка отправки событий (сек.)**. По истечении указанного времени Kaspersky Industrial CyberSecurity for Nodes повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. По умолчанию установлено значение 30 секунд.

Приложение будет отправлять события Windows Event Log на SIEM-сервер в формате JSON Lines.

6. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Параметры подключения к SIEM-серверам

Параметр	Описание
Время ожидания (сек.)	Максимальное время ожидания ответа от сервера SIEM. По истечении времени ожидания Kaspersky Industrial CyberSecurity for Nodes пытается подключиться к другому серверу SIEM.
TLS-сертификат сервера	TLS-сертификат для установки доверенного соединения с сервером SIEM. Вы можете получить TLS-сертификат с помощью интерфейса управления SIEM.
Использовать двустороннюю аутентификацию	Двусторонняя аутентификация при создании безопасного соединения между Kaspersky Industrial CyberSecurity for Nodes и SIEM. Для использования двусторонней аутентификации вам нужно в параметрах SIEM включить функцию двусторонней аутентификации, далее получить криптоконтейнер и установить пароль для защиты криптоконтейнера. *Криптоконтейнер* – PFX-архив с сертификатом и закрытым ключом агента. После настройки параметров SIEM вам нужно в параметрах Kaspersky Industrial CyberSecurity for Nodes включить функцию двусторонней аутентификации с помощью флажка и загрузить защищенный паролем криптоконтейнер. Криптоконтейнер должен быть защищен паролем. Добавить криптоконтейнер с пустым паролем невозможно.

Фильтрация событий для отправки в SIEM

Для повышения производительности и оптимизации отправки данных на сервер SIEM вы можете вручную добавить или исключить отдельные события Журнала событий Windows из телеметрии. Например, вы можете отменить отправку событий Sysmon.

Для корректной работы компонента Интеграция с SIEM вам необходимо включить отправку требуемых событий. По умолчанию отправка всех событий выключена.

Kaspersky Industrial CyberSecurity for Nodes поддерживает суммарно не более 1500 включающих и исключающих правил фильтрации событий WEL для телеметрии SIEM.

Как сформировать список событий для отправки в SIEM в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Дополнительные возможности**.
4. В блоке **Настройки телеметрии SIEM** нажмите на кнопку **Настройка**.
5. В открывшемся окне настройте фильтр событий для отправки в SIEM.

Вы можете настроить фильтрацию событий для стандартных журналов *Application*, *Security*, *System* или добавить другой журнал вручную:

a. Откройте свойства журнала или нажмите на кнопку **Добавить** и введите название журнала.

b. Выберите режим отправки событий:

- **Отправлять все события**. В этом режиме приложение отправляет все события журнала Windows кроме событий, добавленных в правила исключения.
- **Отправлять только выбранные события**. В этом режиме приложение отправляет только события, добавленные в правила включения.

c. Сформируйте списки правил исключения или правил включения для соответствующего режима отправки событий.

Для добавления правил необходимо указать идентификатор события в журнале событий Windows. Вы можете перечислить несколько идентификаторов событий в одном правиле. Для указания нескольких идентификаторов событий используйте символ `,`.

d. При необходимости включите отправку событий из журнала с помощью флажка рядом с названием журнала.

6. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Как сформировать список событий для отправки в SIEM в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Дополнительные возможности**.
5. В блоке **Настройки телеметрии** нажмите на кнопку **Настроить**.

   Откроется окно **Настройки телеметрии**.
6. Перейдите на вкладку **Телеметрия SIEM**.
7. Настройте фильтр событий для отправки в SIEM.

   Вы можете настроить фильтрацию событий для стандартных журналов *Application*, *Security*, *System* или добавить другой журнал вручную:

   a. Откройте свойства журнала или нажмите на кнопку **Добавить** и введите название журнала.

   b. Выберите режим отправки событий:

   - **Отправлять все события**. В этом режиме приложение отправляет все события журнала Windows кроме событий, добавленных в правила исключения.
   - **Отправлять только выбранные события**. В этом режиме приложение отправляет только события, добавленные в правила включения.

c. Сформируйте списки правил исключения или правил включения для соответствующего режима отправки событий.

Для добавления правил необходимо указать идентификатор события в журнале событий Windows. Вы можете перечислить несколько идентификаторов событий в одном правиле. Для указания нескольких идентификаторов событий используйте символ `,`.

d. При необходимости включите отправку событий из журнала с помощью переключателя рядом с названием журнала.

8. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки.

Экспорт и импорт правил фильтрации событий телеметрии

Kaspersky Industrial CyberSecurity for Nodes позволяет выполнять импорт и экспорт JSON-файлов с правилами фильтрации событий телеметрии.

Kaspersky Industrial CyberSecurity for Nodes поддерживает суммарно не более 1500 включающих и исключающих правил фильтрации событий WEL для телеметрии SIEM.

Если на компьютере уже есть правила фильтрации событий, Kaspersky Industrial CyberSecurity for Nodes заменит их при импорте.

Пример. Вы можете экспортировать список исключений в файл формата JSON. Далее вы можете вносить изменения в файл, чтобы, например, добавить большое количество идентификаторов событий. Также вы можете использовать функцию экспорта/импорта для резервного копирования фильтров событий или для миграции списка на другой сервер.

Как экспортировать/импортировать правила фильтрации событий в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Дополнительные возможности**.
4. В блоке **Телеметрия SIEM** нажмите на кнопку **Настройка**.
5. Для экспорта фильтров событий выполните следующие действия:
   a. Выберите журналы событий с фильтрами, которые вы хотите экспортировать.
   b. Нажмите на кнопку и в открывшемся контекстном меню выберите **Экспортировать**.
   c. В открывшемся окне введите имя файла, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.
   d. Сохраните файл.

Kaspersky Industrial CyberSecurity for Nodes экспортирует фильтры событий в JSON-файл.

6. Для импорта фильтров событий выполните следующие действия:

   a. Нажмите на кнопку и в открывшемся контекстном меню выберите **Импортировать**.

   b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

   c. Откройте файл.

7. Сохраните внесенные изменения. Для применения политики на компьютерах закройте замок .

Как экспортировать/импортировать правила фильтрации событий в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.
   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Дополнительные возможности**.
5. В блоке **Настройки телеметрии** нажмите на кнопку **Настроить**.
   Откроется окно **Настройки телеметрии**.
6. Перейдите на вкладку **Телеметрия SIEM.**
7. Для экспорта фильтров событий выполните следующие действия:

   a. Выберите журналы событий с фильтрами, которые вы хотите экспортировать.

   b. Нажмите на кнопку **Экспорт**.

   c. В открывшемся окне введите имя файла, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.

   d. Сохраните файл.

   Kaspersky Industrial CyberSecurity for Nodes экспортирует фильтры событий в JSON-файл.

8. Для импорта фильтров событий выполните следующие действия:

   a. Нажмите на кнопку **Импорт**.

   b. В открывшемся окне выберите JSON-файл, из которого вы хотите импортировать фильтры событий.

   c. Откройте файл.

9. Сохраните внесенные изменения. Для применения политики на компьютерах, закройте замки .

Как экспортировать/импортировать правила фильтрации событий в Консоли приложения Kaspersky Industrial CyberSecurity for Nodes

1. В дереве Консоли приложения выберите узел **Настройки телеметрии**.
2. В блоке **Телеметрия SIEM** нажмите на кнопку **Настройка**.
3. Для экспорта фильтров событий выполните следующие действия:
   a. Нажмите на кнопку **Экспортировать**.
   b. В открывшемся окне введите имя файла формата JSON, в который вы хотите экспортировать фильтры событий, а также выберите папку, в которой вы хотите сохранить этот файл.
   c. Сохраните файл.

   Kaspersky Industrial CyberSecurity for Nodes экспортирует фильтры событий в JSON-файл.
4. Для импорта фильтров событий выполните следующие действия:
   a. Нажмите на кнопку **Импортировать**.
   b. В открывшемся диалоговом окне подтвердите изменение настроек телеметрии SIEM.
   c. Выберите JSON-файл, из которого вы хотите импортировать фильтры событий.
   d. Откройте файл.
5. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Также вы можете экспортировать/импортировать правила фильтрации событий телеметрии через интерфейс командной строки.

Обнаружение аномалий с помощью Sigma-правил

Функциональность доступна на компьютерах, работающих под управлением операционных систем Windows 7 и выше или Windows Server 2008 R2 и выше при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes с лицензионными объектами EDR Optimum и ICS Telemetry.

Для работы обнаружения аномалий с помощью Sigma-правил необходимо, чтобы были включены следующие компоненты: Постоянная защита файлов, Защита от эксплойтов, Откат вредоносных действий.

Sigma – это формат описания правил для обнаружения аномалий, с помощью которых Kaspersky Industrial CyberSecurity for Nodes анализирует данные внутренних событий и журналов событий. Правила, написанные в формате Sigma, называются Sigma-правилами.

Sigma-правила пишутся на языке YAML и имеют унифицированную структуру. Это позволяет специально созданным конвертерам формировать правила в синтаксисе различных SIEM-систем на основе Sigma-правил. Каждое Sigma-правило хранится в отдельном YAML-файле.

Структура Sigma-правила

В таблице дана базовая информация об атрибутах и секциях Sigma-правила, которые интерпретирует Kaspersky Industrial CyberSecurity for Nodes. Более детальную информацию вы можете получить по ссылке.

Значения атрибутов чувствительны к регистру. Например, названия исполняемых файлов AnyDesk.exe и anyDesk.exe Kaspersky Industrial CyberSecurity for Nodes обрабатывает как разные.

<table>
<tr><th>Атрибут / Секция</th><th>Обязательный</th><th>Описание</th></tr>
<tr><td><code>logsource</code></td><td>Да</td><td>
В секции можно определить источник событий, в которых программа ищет аномалии. Основные атрибуты секции: <code>category</code>, <code>product</code>, <code>service</code>.
Источники событий, которые поддерживает Kaspersky Industrial CyberSecurity for Nodes
Поддерживаемые Kaspersky Industrial CyberSecurity for Nodes источники событий
<table>
<tr><th>Источник (logsource)</th><th>Событие</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события о запуске процесса, которое по содержанию соответствует событию EventID 1 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события о загрузке драйвера, которое по содержанию соответствует событию EventID 6 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 7 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутренних событий, которые по содержанию соответствуют событиям EventID 12, EventID 13 и EventID 14 в журнале Microsoft-Windows-Sysmon/Operational и дополнены полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 22 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию в журнале провайдера службы трассировки Windows Microsoft-Windows-Kernel-File и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 11 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/Application.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/Security.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/System.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутренних событий, связанных с нормализованными данными из журналов событий системы Emerson DeltaV.
События источника не связаны с внешними журналами событий.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала Windows PowerShell.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала Microsoft-Windows-PowerShell/Operational.</td></tr>
</table>
В операционной системе Microsoft Windows 7 для источников <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> отсутствуют некоторые внутренние события либо в событиях могут отсутствовать некоторые поля или необходимые данные. В результате Sigma-правила могут не срабатывать.
Подробнее читайте по ссылке.
</td></tr>
<tr><td><code>title</code></td><td>Да</td><td>Название правила, указывающее на то, что оно обнаруживает. Максимальная длина 256 символов.
Например:
<code>title: Creation of a new RAT service</code></td></tr>
<tr><td><code>id</code></td><td>Нет</td><td>Глобальный уникальный идентификатор правила. Например:
<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code></td></tr>
<tr><td><code>status</code></td><td>Нет</td><td>Статус правила. Возможные значения: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.
Например:
<code>status: test</code></td></tr>
</table>

`description`	Нет	Описание правила и вредоносной активности, которую можно обнаружить с его помощью. Максимальная длина 65 535 символов. Например: `description: Detects the installation of a new Remote Utilities host application service.`
`license`	Нет	Идентификатор лицензии согласно спецификации SPDX ID. Правило публикуется на условиях указанного типа лицензии.
`author`	Нет	Любой признак, указывающий на автора правила. Например, имя-фамилия, прозвище, идентификатор в социальной сети.
`reference`	Нет	Ссылка на источник, из которого было получено правило. Например, статья в блоге, технический документ.
`date`	Нет	Дата создания правила в формате ГГГГ/ММ/ДД.
`modified`	Нет	Дата в формате ГГГГ/ММ/ДД, когда был изменен один из атрибутов правила: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	Нет	Тег для категоризации правила. Подробнее читайте по ссылке.

`category`	Нет	Определяет категорию продуктов, в журналах событий которых программа ищет аномалии. Например: брандмауэр, интернет, антивирус или обобщенная категория.
		`logsource:`
		`  category: firewall`

`product`	Нет	Определяет программный продукт или операционную систему, в журналах событий которых программа ищет аномалии. Например:
		`logsource:`
		`  product: Windows`

`service`	Нет	Определяет службу, в журналах событий которой программа ищет аномалии. Например:
		`logsource:`
		`  service: AppLocker`

`definition`	Нет	Описание особенностей источника журналов событий, в которых программа ищет аномалии.
`detection`	Да	Секция содержит один или несколько критериев для поиска аномалий в журналах событий и условие срабатывания правила. В качестве критериев поиска могут быть списки, словари и их комбинация. Kaspersky Industrial CyberSecurity for Nodes не поддерживает модификатор значения `windash`.

список	Нет	Список из значений какого-либо параметра из журнала событий, объединенных логическим ИЛИ. Например:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		Согласно условию, будут искаться совпадения `OriginalFileName='AnyDesk.exe'` ИЛИ `OriginalFileName='TeamViewer.exe'`.

словарь	Нет	Пары типа *параметр журнала событий - значение*. Соединены логическим И. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		Согласно условию, будут искаться совпадения EventLog='Security' И Event ID=517.

комбинация списка и словаря	Нет	Список, состоящий из значений параметров журнала событий и словарей. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		Согласно условию, будут искаться совпадения EventLog='Security' И (Event ID=517 ИЛИ Event ID=1102)

`condition`	Да	Условие срабатывания правила. Например:
		
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	Нет	Строки из журнала событий, которые могут быть интересны аналитику для дальнейшего анализа события.

`falsepositives`	Нет	Список известных сценариев, которые могут привести к ложному срабатыванию правила. Например:
		
		`falsepositives:`
		`- Use of a utility by system administrators`

`level`	Нет	Показатель критичности аномалий, которые могут быть найдены с помощью правила. Возможные значения: `informational`, `low`, `medium`, `high`, `critical`.

Пример Sigma-правила

```
title: Downloading files using CertUtil.exe
id: 89346938-3b2f-46c7-bb38-b9f244e3fad0
status: test
description: Detects file downloads using CertUtil.exe.
references:
  - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
author: Kaspersky
date: 2024-05-22
tags:
  - attack.defense_evasion
  - attack.t1027
logsource:
  category: process_creation
  product: windows
detection:
  selection_image:
    - Image|endswith: '\certutil.exe'
    - OriginalFileName: 'CertUtil.exe'
  selection_http:
    CommandLine|contains: 'http'
condition: all of selection_*
falsepositives:
  - Legitimate actions of the system administrator.
level: low
```

Коллекция Sigma-правил – набор Sigma-правил, определяющих схожие события.

Kaspersky Industrial CyberSecurity for Nodes анализирует данные внутренних событий и журналов событий на предмет аномалий с помощью коллекций Sigma-правил, поставляемых АО "Лаборатория Касперского"с базами приложения, и создаваемых пользователем коллекций Sigma-правил.

В зависимости от версии приложения, Kaspersky Industrial CyberSecurity for Nodes поддерживает работу с предустановленными коллекциями Sigma-правил, приведенными в таблице ниже.

Предустановленные коллекции Sigma-правил

Коллекция Sigma-правил	Версия приложения	
	4.5	5.0
Обнаружение средств удаленного администрирования (RAT)	✓	✓
Обнаружение аномалий для Emerson DeltaV	✓	✓
Контроль учетных записей пользователей (UAC)	✓	✓
Обнаружение аномалий для Siemens SIMATIC WinCC, Siemens TIA Portal, Siemens SIMATIC STEP 7	✓	✓

Коллекция Sigma-правил	Версия приложения	
	4.5	5.0
Обнаружение аномалий для Yokogawa CENTUM VP	✓	✓
Аудит обмена файлами по сети и через съемные носители	–	✓

При использовании некоторых Sigma-правил приложение может вносить изменения в политику аудита безопасности защищаемого компьютера – части локальной политики безопасности Windows.

Особенности работы и ограничения обнаружения аномалий с помощью Sigma-правил

Для корректной работы некоторых коллекций Sigma-правил необходимо изменение параметров политик аудита. Поведение приложения различается в зависимости от того, входит компьютер в домен или нет:

- Если компьютер входит в домен, приложение не меняет параметры групповой политики домена. Вы можете исключить данный компьютер из домена или настроить параметры групповой политики домена самостоятельно.

- Если компьютер не входит в домен, приложение автоматически изменяет параметры локальной политики, если это требуется для корректной работы коллекции Sigma-правил.

  Для автоматического изменения параметров локальной политики должна быть включена функция Автоматически вносить изменения в локальную политику аудита безопасности. Если функция выключена, необходимо самостоятельно настроить параметры локальной политики для корректной работы Sigma-правил.

  Приложение не вносит изменения в параметры локальной политики для пользовательских коллекций Sigma-правил. Вам необходимо самостоятельно настроить параметры локальной политики для корректной работы пользовательских Sigma-правил.

  После выключения коллекции Sigma-правил приложение не возвращает параметры локальной политики в исходное состояние. При необходимости вы можете самостоятельно восстановить исходные параметры локальной политики.

Функциональность обнаружения аномалий с помощью Sigma-правил имеет следующие ограничения:

- Для работы Sigma-правила "Изменение или удаление журналов событий Windows на узле DeltaV" сразу после установки компонента Обнаружение аномалий с помощью Sigma-правил требуется перезагрузить компьютер или **остановить и заново запустить службу Журнал событий Windows**.

  1. Запустите приложение Windows Службы (services.msc).

  2. В списке служб найдите Журнал событий Windows.

3. В контекстном меню службы Журнал событий Windows выберите **Остановить**, чтобы остановить работу службы.

4. В контекстном меню службы Журнал событий Windows выберите **Запустить**, чтобы запустить службу.

- Не поддерживаются следующие модификаторы значений: `base64offset`, `cidr`, `lt`, `windash`.
- Не поддерживаются регулярные выражения.
- Не поддерживается экранирование подстановочных знаков.
- Подстановочный знак `?` обрабатывается приложением как `*`.
- Не поддерживается конструкция "`condition: not selection`", при этом поддерживается конструкция "`condition: selection and not filter`".
- Не поддерживаются правила, в которых в качестве критериев для поиска аномалий в журналах событий Windows не указано одно или несколько значений параметра `EventID`.
- Для Sigma-правил, описывающих операции с файлами, в отчете фиксируется первые 50 обнаружений. Счетчик обнаружений ведется отдельно для каждого процесса в случае, если процесс выполняет операции с файлами, у которых схожие пути.
- Приложение поддерживает работу Sigma-правил на компьютерах под управлением Windows XP и Windows Server 2003 с ограничениями. Открытие деталей алерта, обнаруженных на компьютерах под управлением этих ОС, может завершиться с ошибкой *Не удалось открыть детали алерта. Возможные причины: компьютер не в сети, проблемы с сетью, истек срок хранения алерта*. Вы можете открыть детали алерта с помощью Kaspersky Industrial CyberSecurity for Networks.
- Приложение поддерживает работу с Siemens SIMATIC PCS 7 версии 9.0 SP1 и выше.
- Для работы Sigma-правила "Детект записи файла на съемный диск" из предустановленной коллекции Аудит обмена файлами по сети и через съемные носители требуется перезагрузить компьютер.

Включение обнаружения аномалий с помощью Sigma-правил

Включение обнаружения аномалий с помощью Sigma-правил в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.
4. В блоке **Обнаружение аномалий с помощью Sigma-правил** нажмите на кнопку **Настройка**.
5. В открывшемся окне установите флажок **Обнаружение аномалий с помощью Sigma-правил**.

6. Добавьте одну или несколько коллекций Sigma-правил:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Добавление коллекции правил**.

   b. С помощью раскрывающегося списка **Выберите коллекцию правил** выполните одно из следующих действий:

      - Выберите одну из предустановленных коллекций Sigma-правил.

        Если предустановленные коллекции Sigma-правил не отображаются, убедитесь, что приложение активировано лицензионным ключом с объектами EDR Optimum и ICS Telemetry. Также вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* для обновления предустановленных коллекций.

        > При добавлении предустановленных коллекций Sigma-правил вам необходимо убедиться, что выбранная коллекция поддерживается всеми версиями Kaspersky Industrial CyberSecurity for Nodes, установленными на управляемых устройствах.

      - Выберите вариант **Коллекция пользовательских правил**, чтобы добавить пользовательскую коллекцию Sigma-правил.

        Если вы добавляете пользовательскую коллекцию Sigma-правил, в одноименном поле введите уникальное имя коллекции. Созданная пользовательская коллекция не содержит ни одного правила.

   c. Нажмите на кнопку **OK**.

      Добавленная коллекция отобразится в списке. По умолчанию после добавления коллекция Sigma-правил включена. Если необходимо, измените состояние коллекции Sigma-правил с помощью флажка слева от имени коллекции.

7. При необходимости снимите флажок **Автоматически вносить изменения в локальную политику аудита безопасности**. Если функция включена, приложение автоматически изменяет параметры локальной политики, если это требуется для корректной работы добавленных коллекций Sigma-правил. Если функция выключена, необходимо самостоятельно настроить параметры локальной политики для корректной работы Sigma-правил. По умолчанию функция включена.

   > Приложение не вносит изменения в параметры локальной политики для пользовательских коллекций Sigma-правил. Вам необходимо самостоятельно настроить параметры локальной политики для корректной работы пользовательских Sigma-правил.

8. Закройте замок для применения политики на компьютерах.

9. Нажмите на кнопку **OK** для сохранения внесенных изменений.

   Kaspersky Industrial CyberSecurity for Nodes будет искать аномалии с помощью включенных коллекций Sigma-правил.

Включение обнаружения аномалий с помощью Sigma-правил в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. В разделе **Обнаружение аномалий с помощью Sigma-правил** установите флажок **Включить обнаружение аномалий с помощью Sigma-правил**.

5. При необходимости снимите флажок **Автоматически вносить изменения в локальную политику аудита безопасности**. Если функция включена, приложение автоматически изменяет параметры локальной политики, если это требуется для корректной работы добавленных коллекций Sigma-правил. Если функция выключена, необходимо самостоятельно настроить параметры локальной политики для корректной работы Sigma-правил. По умолчанию функция включена.

   Приложение не вносит изменения в параметры локальной политики для пользовательских коллекций Sigma-правил. Вам необходимо самостоятельно настроить параметры локальной политики для корректной работы пользовательских Sigma-правил.

6. Добавьте одну или несколько коллекций Sigma-правил:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Добавление коллекции правил**.

   b. С помощью раскрывающегося списка **Выберите коллекцию правил** выполните одно из следующих действий:

      - Выберите одну из предустановленных коллекций Sigma-правил.

        Если предустановленные коллекции Sigma-правил не отображаются, убедитесь, что приложение активировано лицензионным ключом с объектами EDR Optimum и ICS Telemetry. Также вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* для обновления предустановленных коллекций.

        При добавлении предустановленных коллекций Sigma-правил вам необходимо убедиться, что выбранная коллекция поддерживается всеми версиями Kaspersky Industrial CyberSecurity for Nodes, установленными на управляемых устройствах.

      - Выберите вариант **Коллекция пользовательских правил**, чтобы добавить пользовательскую коллекцию Sigma-правил.

        Если вы добавляете пользовательскую коллекцию Sigma-правил, в одноименном поле введите уникальное имя коллекции. Созданная пользовательская коллекция не содержит ни одного правила.

   c. Нажмите на кнопку **OK**.

      Добавленная коллекция отобразится в списке. По умолчанию после добавления коллекция Sigma-правил включена. Если необходимо, измените состояние коллекции Sigma-правил с помощью переключателя слева от имени коллекции.

   d. Нажмите на кнопку **Сохранить**.

      Kaspersky Industrial CyberSecurity for Nodes будет искать аномалии с помощью включенных коллекций Sigma-правил.

Включение обнаружения аномалий с помощью Sigma-правил в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Detection and Response → Обнаружение аномалий с помощью Sigma-правил**.

   В панели результатов перейдите по ссылке **Свойства**.

2. Установите флажок **Обнаружение аномалий с помощью Sigma-правил**.

3. Добавьте одну или несколько коллекций Sigma-правил:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Добавление коллекции правил**.

   b. С помощью раскрывающегося списка **Выберите коллекцию правил** выполните одно из следующих действий:

      - Выберите одну из предустановленных коллекций Sigma-правил.

        Если предустановленные коллекции Sigma-правил не отображаются, убедитесь, что приложение активировано лицензионным ключом с объектами EDR Optimum и ICS Telemetry. Также вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования* для обновления предустановленных коллекций.

      - Выберите вариант **Коллекция пользовательских правил**, чтобы добавить пользовательскую коллекцию Sigma-правил.

        Если вы добавляете пользовательскую коллекцию Sigma-правил, в одноименном поле введите уникальное имя коллекции. Созданная пользовательская коллекция не содержит ни одного правила.

        > Пользовательские коллекции Sigma-правил, созданные с использованием Консоли приложения, недоступны в Консоли администрирования Kaspersky Security Center и Web Console.

   c. Нажмите на кнопку **OK**.

      Добавленная коллекция отобразится в списке. По умолчанию после добавления коллекция Sigma-правил включена. Если необходимо, измените состояние коллекции Sigma-правил с помощью флажка слева от имени коллекции.

4. При необходимости снимите флажок **Автоматически вносить изменения в локальную политику аудита безопасности**. Если функция включена, приложение автоматически изменяет параметры локальной политики, если это требуется для корректной работы добавленных коллекций Sigma-правил. Если функция выключена, необходимо самостоятельно настроить параметры локальной политики для корректной работы Sigma-правил. По умолчанию функция включена.

   > Приложение не вносит изменения в параметры локальной политики для пользовательских коллекций Sigma-правил. Вам необходимо самостоятельно настроить параметры локальной политики для корректной работы пользовательских Sigma-правил.

5. Нажмите на кнопку **OK** для сохранения внесенных изменений.

   Kaspersky Industrial CyberSecurity for Nodes будет искать аномалии с помощью включенных коллекций Sigma-правил.

Также вы можете включить обнаружение аномалий с помощью Sigma-правил из командной строки.

Добавление Sigma-правил в пользовательскую коллекцию

Добавление Sigma-правил в пользовательскую коллекцию в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.
4. В блоке **Обнаружение аномалий с помощью Sigma-правил** нажмите на кнопку **Настройка**.
5. В открывшемся окне выберите пользовательскую коллекцию Sigma-правил, в которую вы хотите добавить одно или несколько Sigma-правил.
6. Нажмите на кнопку **Изменить**.
7. В открывшемся окне добавьте в коллекцию Sigma-правила любым из следующих способов:
   - Вручную:
     a. Нажмите на кнопку **Добавить**.
     b. В открывшейся форме для редактирования опишите правило **в формате Sigma**.

     В таблице дана базовая информация об атрибутах и секциях Sigma-правила, которые интерпретирует Kaspersky Industrial CyberSecurity for Nodes. Более детальную информацию вы можете получить по ссылке.

     > Значения атрибутов чувствительны к регистру. Например, названия исполняемых файлов AnyDesk.exe и anyDesk.exe Kaspersky Industrial CyberSecurity for Nodes обрабатывает как разные.

<table>
<tr><th>Атрибут / Секция</th><th>Обязательный</th><th>Описание</th></tr>
<tr><td><code>logsource</code></td><td>Да</td><td>
В секции можно определить источник событий, в которых программа ищет аномалии. Основные атрибуты секции: <code>category</code>, <code>product</code>, <code>service</code>.

Источники событий, которые поддерживает Kaspersky Industrial CyberSecurity for Nodes

Поддерживаемые Kaspersky Industrial CyberSecurity for Nodes источники событий
<table>
<tr><th>Источник (logsource)</th><th>Событие</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события о запуске процесса, которое по содержанию соответствует событию EventID 1 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события о загрузке драйвера, которое по содержанию соответствует событию EventID 6 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 7 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутренних событий, которые по содержанию соответствуют событиям EventID 12, EventID 13 и EventID 14 в журнале Microsoft-Windows-Sysmon/Operational и дополнены полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 22 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию в журнале провайдера службы трассировки Windows Microsoft-Windows-Kernel-File и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 11 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/Application.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/Security.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/System.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутренних событий, связанных с нормализованными данными из журналов событий системы Emerson DeltaV.
События источника не связаны с внешними журналами событий.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала Windows PowerShell.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала Microsoft-Windows-PowerShell/Operational.</td></tr>
</table>
В операционной системе Microsoft Windows 7 для источников <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> отсутствуют некоторые внутренние события либо в событиях могут отсутствовать некоторые поля или необходимые данные. В результате Sigma-правила могут не срабатывать.

Подробнее читайте по ссылке.
</td></tr>
<tr><td><code>title</code></td><td>Да</td><td>Название правила, указывающее на то, что оно обнаруживает. Максимальная длина 256 символов.

Например:

<code>title: Creation of a new RAT service</code></td></tr>
<tr><td><code>id</code></td><td>Нет</td><td>Глобальный уникальный идентификатор правила. Например:

<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code></td></tr>
<tr><td><code>status</code></td><td>Нет</td><td>Статус правила. Возможные значения: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.

Например:

<code>status: test</code></td></tr>
</table>

`description`	Нет	Описание правила и вредоносной активности, которую можно обнаружить с его помощью. Максимальная длина 65 535 символов. Например: `description: Detects the installation of a new Remote Utilities host application service.`
`license`	Нет	Идентификатор лицензии согласно спецификации SPDX ID. Правило публикуется на условиях указанного типа лицензии.
`author`	Нет	Любой признак, указывающий на автора правила. Например, имя-фамилия, прозвище, идентификатор в социальной сети.
`reference`	Нет	Ссылка на источник, из которого было получено правило. Например, статья в блоге, технический документ.
`date`	Нет	Дата создания правила в формате ГГГГ/ММ/ДД.
`modified`	Нет	Дата в формате ГГГГ/ММ/ДД, когда был изменен один из атрибутов правила: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	Нет	Тег для категоризации правила. Подробнее читайте по ссылке.

`category`	Нет	Определяет категорию продуктов, в журналах событий которых программа ищет аномалии. Например: брандмауэр, интернет, антивирус или обобщенная категория.
		`logsource:`
		`  category: firewall`

`product`	Нет	Определяет программный продукт или операционную систему, в журналах событий которых программа ищет аномалии. Например:
		`logsource:`
		`  product: Windows`

`service`	Нет	Определяет службу, в журналах событий которой программа ищет аномалии. Например:
		`logsource:`
		`  service: AppLocker`

`definition`	Нет	Описание особенностей источника журналов событий, в которых программа ищет аномалии.
`detection`	Да	Секция содержит один или несколько критериев для поиска аномалий в журналах событий и условие срабатывания правила. В качестве критериев поиска могут быть списки, словари и их комбинация. Kaspersky Industrial CyberSecurity for Nodes не поддерживает модификатор значения `windash`.

список	Нет	Список из значений какого-либо параметра из журнала событий, объединенных логическим ИЛИ. Например:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		Согласно условию, будут искаться совпадения `OriginalFileName='AnyDesk.exe'` ИЛИ `OriginalFileName='TeamViewer.exe'`.

словарь	Нет	Пары типа *параметр журнала событий - значение*. Соединены логическим И. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		Согласно условию, будут искаться совпадения EventLog='Security' И Event ID=517.

комбинация списка и словаря	Нет	Список, состоящий из значений параметров журнала событий и словарей. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		Согласно условию, будут искаться совпадения EventLog='Security' И (Event ID=517 ИЛИ Event ID=1102)

`condition`	Да	Условие срабатывания правила. Например:
		
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	Нет	Строки из журнала событий, которые могут быть интересны аналитику для дальнейшего анализа события.

`falsepositives`	Нет	Список известных сценариев, которые могут привести к ложному срабатыванию правила. Например:
		
		`falsepositives:`
		`- Use of a utility by system administrators`

`level`	Нет	Показатель критичности аномалий, которые могут быть найдены с помощью правила. Возможные значения: `informational`, `low`, `medium`, `high`, `critical`.

c. Нажмите на кнопку **OK**.

Описанное Sigma-правило отобразится в списке правил коллекции.

d. Повторите пункты a-c для каждого добавляемого вручную правила.

- Из файлов:

a. Нажмите на кнопку **Добавить файл**.

b. В открывшемся окне выберите один или несколько YAML-файлов, в которых описаны Sigma-правила.

Sigma-правила, описанные в YAML-файлах, отобразятся в списке правил коллекции.

> Если в синтаксисе Sigma-правила допущены ошибки, или отсутствуют обязательные атрибуты, то правило не будет добавлено в коллекцию.

8. Добавленные правила по умолчанию включены. Если необходимо, измените состояние Sigma-правила с помощью флажка слева от имени коллекции. Вы можете изменять состояние всех правил в коллекции с помощью кнопок **Включить все** и **Выключить все**.

9. Для удаления правила из списка выберите правило и нажмите на кнопку **Удалить**.

10. Сохраните внесенные изменения.

Добавление Sigma-правил в пользовательскую коллекцию в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.

5. В блоке **Обнаружение аномалий с помощью Sigma-правил** выберите пользовательскую коллекцию Sigma-правил, в которую вы хотите добавить одно или несколько Sigma-правил, с помощью флажка напротив имени коллекции.

6. Нажмите на кнопку **Изменить**.

7. В открывшемся окне добавьте в коллекцию Sigma-правила любым из следующих способов:

- Вручную:

  a. Нажмите на кнопку **Добавить**.

  b. В открывшейся форме для редактирования опишите правило **в формате Sigma**.

  В таблице дана базовая информация об атрибутах и секциях Sigma-правила, которые интерпретирует Kaspersky Industrial CyberSecurity for Nodes. Более детальную информацию вы можете получить по ссылке.

  > Значения атрибутов чувствительны к регистру. Например, названия исполняемых файлов AnyDesk.exe и anyDesk.exe Kaspersky Industrial CyberSecurity for Nodes обрабатывает как разные.

<table>
<tr><th>Атрибут / Секция</th><th>Обязательный</th><th>Описание</th></tr>
<tr><td><code>logsource</code></td><td>Да</td><td>
В секции можно определить источник событий, в которых программа ищет аномалии. Основные атрибуты секции: <code>category</code>, <code>product</code>, <code>service</code>.

Источники событий, которые поддерживает Kaspersky Industrial CyberSecurity for Nodes

Поддерживаемые Kaspersky Industrial CyberSecurity for Nodes источники событий
<table>
<tr><th>Источник (logsource)</th><th>Событие</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события о запуске процесса, которое по содержанию соответствует событию EventID 1 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события о загрузке драйвера, которое по содержанию соответствует событию EventID 6 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 7 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутренних событий, которые по содержанию соответствуют событиям EventID 12, EventID 13 и EventID 14 в журнале Microsoft-Windows-Sysmon/Operational и дополнены полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 22 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию в журнале провайдера службы трассировки Windows Microsoft-Windows-Kernel-File и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 11 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/Application.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/Security.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/System.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутренних событий, связанных с нормализованными данными из журналов событий системы Emerson DeltaV.
События источника не связаны с внешними журналами событий.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала Windows PowerShell.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала Microsoft-Windows-PowerShell/Operational.</td></tr>
</table>
В операционной системе Microsoft Windows 7 для источников <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> отсутствуют некоторые внутренние события либо в событиях могут отсутствовать некоторые поля или необходимые данные. В результате Sigma-правила могут не срабатывать.

Подробнее читайте по ссылке.
</td></tr>
<tr><td><code>title</code></td><td>Да</td><td>Название правила, указывающее на то, что оно обнаруживает. Максимальная длина 256 символов.

Например:

<code>title: Creation of a new RAT service</code></td></tr>
<tr><td><code>id</code></td><td>Нет</td><td>Глобальный уникальный идентификатор правила. Например:

<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code></td></tr>
<tr><td><code>status</code></td><td>Нет</td><td>Статус правила. Возможные значения: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.

Например:

<code>status: test</code></td></tr>
</table>

`description`	Нет	Описание правила и вредоносной активности, которую можно обнаружить с его помощью. Максимальная длина 65 535 символов. Например: `description: Detects the installation of a new Remote Utilities host application service.`
`license`	Нет	Идентификатор лицензии согласно спецификации SPDX ID. Правило публикуется на условиях указанного типа лицензии.
`author`	Нет	Любой признак, указывающий на автора правила. Например, имя-фамилия, прозвище, идентификатор в социальной сети.
`reference`	Нет	Ссылка на источник, из которого было получено правило. Например, статья в блоге, технический документ.
`date`	Нет	Дата создания правила в формате ГГГГ/ММ/ДД.
`modified`	Нет	Дата в формате ГГГГ/ММ/ДД, когда был изменен один из атрибутов правила: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	Нет	Тег для категоризации правила. Подробнее читайте по ссылке.

`category`	Нет	Определяет категорию продуктов, в журналах событий которых программа ищет аномалии. Например: брандмауэр, интернет, антивирус или обобщенная категория.
		`logsource:`
		`  category: firewall`

`product`	Нет	Определяет программный продукт или операционную систему, в журналах событий которых программа ищет аномалии. Например:
		`logsource:`
		`  product: Windows`

`service`	Нет	Определяет службу, в журналах событий которой программа ищет аномалии. Например:
		`logsource:`
		`  service: AppLocker`

`definition`	Нет	Описание особенностей источника журналов событий, в которых программа ищет аномалии.
`detection`	Да	Секция содержит один или несколько критериев для поиска аномалий в журналах событий и условие срабатывания правила. В качестве критериев поиска могут быть списки, словари и их комбинация. Kaspersky Industrial CyberSecurity for Nodes не поддерживает модификатор значения `windash`.

список	Нет	Список из значений какого-либо параметра из журнала событий, объединенных логическим ИЛИ. Например:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		Согласно условию, будут искаться совпадения `OriginalFileName='AnyDesk.exe'` ИЛИ `OriginalFileName='TeamViewer.exe'`.

словарь	Нет	Пары типа *параметр журнала событий - значение*. Соединены логическим И. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		Согласно условию, будут искаться совпадения EventLog='Security' И Event ID=517.

комбинация списка и словаря	Нет	Список, состоящий из значений параметров журнала событий и словарей. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		Согласно условию, будут искаться совпадения EventLog='Security' И (Event ID=517 ИЛИ Event ID=1102)

`condition`	Да	Условие срабатывания правила. Например:
		
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	Нет	Строки из журнала событий, которые могут быть интересны аналитику для дальнейшего анализа события.

`falsepositives`	Нет	Список известных сценариев, которые могут привести к ложному срабатыванию правила. Например:
		
		`falsepositives:`
		`- Use of a utility by system administrators`

`level`	Нет	Показатель критичности аномалий, которые могут быть найдены с помощью правила. Возможные значения: `informational`, `low`, `medium`, `high`, `critical`.

c. Нажмите на кнопку **OK**.

Описанное Sigma-правило отобразится в списке правил коллекции.

d. Повторите пункты a-c для каждого добавляемого вручную правила.

- Из файлов:

a. Нажмите на кнопку **Добавить файл**.

b. В открывшемся окне выберите один или несколько YAML-файлов, в которых описаны Sigma-правила.

Sigma-правила, описанные в YAML-файлах, отобразятся в списке правил коллекции.

> Если в синтаксисе Sigma-правила допущены ошибки, или отсутствуют обязательные атрибуты, то правило не будет добавлено в коллекцию.

8. Добавленные правила по умолчанию включены. Если необходимо, измените состояние Sigma-правила с помощью переключателя слева от имени коллекции. Вы можете изменять состояние всех правил в коллекции с помощью кнопок **Включить все** и **Выключить все**.

9. Для удаления правила из списка выберите правило и нажмите на кнопку **Удалить**.

10. Сохраните внесенные изменения.

Добавление Sigma-правил в пользовательскую коллекцию в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Detection and Response → Обнаружение аномалий с помощью Sigma-правил**.

2. В панели результатов перейдите по ссылке **Свойства**.

3. В открывшемся окне выберите пользовательскую коллекцию Sigma-правил, в которую вы хотите добавить одно или несколько Sigma-правил.

4. Нажмите на кнопку **Изменить**.

5. В открывшемся окне добавьте в коллекцию Sigma-правила любым из следующих способов:

- Вручную:

  a. Нажмите на кнопку **Добавить**.

  b. В открывшейся форме для редактирования опишите правило **в формате Sigma**.

  В таблице дана базовая информация об атрибутах и секциях Sigma-правила, которые интерпретирует Kaspersky Industrial CyberSecurity for Nodes. Более детальную информацию вы можете получить по ссылке.

  > Значения атрибутов чувствительны к регистру. Например, названия исполняемых файлов AnyDesk.exe и anyDesk.exe Kaspersky Industrial CyberSecurity for Nodes обрабатывает как разные.

<table>
<tr><th>Атрибут / Секция</th><th>Обязательный</th><th>Описание</th></tr>
<tr><td><code>logsource</code></td><td>Да</td><td>
В секции можно определить источник событий, в которых программа ищет аномалии. Основные атрибуты секции: <code>category</code>, <code>product</code>, <code>service</code>.

Источники событий, которые поддерживает Kaspersky Industrial CyberSecurity for Nodes

Поддерживаемые Kaspersky Industrial CyberSecurity for Nodes источники событий
<table>
<tr><th>Источник (logsource)</th><th>Событие</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события о запуске процесса, которое по содержанию соответствует событию EventID 1 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события о загрузке драйвера, которое по содержанию соответствует событию EventID 6 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 7 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутренних событий, которые по содержанию соответствуют событиям EventID 12, EventID 13 и EventID 14 в журнале Microsoft-Windows-Sysmon/Operational и дополнены полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 22 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию в журнале провайдера службы трассировки Windows Microsoft-Windows-Kernel-File и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутреннего события, которое по содержанию соответствует событию EventID 11 в журнале Microsoft-Windows-Sysmon/Operational и дополнено полями Kaspersky Industrial CyberSecurity for Nodes.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/Application.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/Security.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала WEL/System.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует экземпляры внутренних событий, связанных с нормализованными данными из журналов событий системы Emerson DeltaV.
События источника не связаны с внешними журналами событий.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала Windows PowerShell.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes анализирует события из журнала Microsoft-Windows-PowerShell/Operational.</td></tr>
</table>
В операционной системе Microsoft Windows 7 для источников <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> отсутствуют некоторые внутренние события либо в событиях могут отсутствовать некоторые поля или необходимые данные. В результате Sigma-правила могут не срабатывать.

Подробнее читайте по ссылке.
</td></tr>
<tr><td><code>title</code></td><td>Да</td><td>Название правила, указывающее на то, что оно обнаруживает. Максимальная длина 256 символов.

Например:

<code>title: Creation of a new RAT service</code></td></tr>
<tr><td><code>id</code></td><td>Нет</td><td>Глобальный уникальный идентификатор правила. Например:

<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code></td></tr>
<tr><td><code>status</code></td><td>Нет</td><td>Статус правила. Возможные значения: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.

Например:

<code>status: test</code></td></tr>
</table>

`description`	Нет	Описание правила и вредоносной активности, которую можно обнаружить с его помощью. Максимальная длина 65 535 символов. Например: `description: Detects the installation of a new Remote Utilities host application service.`
`license`	Нет	Идентификатор лицензии согласно спецификации SPDX ID. Правило публикуется на условиях указанного типа лицензии.
`author`	Нет	Любой признак, указывающий на автора правила. Например, имя-фамилия, прозвище, идентификатор в социальной сети.
`reference`	Нет	Ссылка на источник, из которого было получено правило. Например, статья в блоге, технический документ.
`date`	Нет	Дата создания правила в формате ГГГГ/ММ/ДД.
`modified`	Нет	Дата в формате ГГГГ/ММ/ДД, когда был изменен один из атрибутов правила: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	Нет	Тег для категоризации правила. Подробнее читайте по ссылке.

`category`	Нет	Определяет категорию продуктов, в журналах событий которых программа ищет аномалии. Например: брандмауэр, интернет, антивирус или обобщенная категория.
		`logsource:`
		`  category: firewall`

`product`	Нет	Определяет программный продукт или операционную систему, в журналах событий которых программа ищет аномалии. Например:
		`logsource:`
		`  product: Windows`

`service`	Нет	Определяет службу, в журналах событий которой программа ищет аномалии. Например:
		`logsource:`
		`  service: AppLocker`

`definition`	Нет	Описание особенностей источника журналов событий, в которых программа ищет аномалии.
`detection`	Да	Секция содержит один или несколько критериев для поиска аномалий в журналах событий и условие срабатывания правила. В качестве критериев поиска могут быть списки, словари и их комбинация. Kaspersky Industrial CyberSecurity for Nodes не поддерживает модификатор значения `windash`.

список	Нет	Список из значений какого-либо параметра из журнала событий, объединенных логическим ИЛИ. Например:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		Согласно условию, будут искаться совпадения `OriginalFileName='AnyDesk.exe'` ИЛИ `OriginalFileName='TeamViewer.exe'`.

словарь	Нет	Пары типа *параметр журнала событий - значение*. Соединены логическим И. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		Согласно условию, будут искаться совпадения EventLog='Security' И Event ID=517.

комбинация списка и словаря	Нет	Список, состоящий из значений параметров журнала событий и словарей. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		Согласно условию, будут искаться совпадения EventLog='Security' И (Event ID=517 ИЛИ Event ID=1102)

`condition`	Да	Условие срабатывания правила. Например:
		
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	Нет	Строки из журнала событий, которые могут быть интересны аналитику для дальнейшего анализа события.

`falsepositives`	Нет	Список известных сценариев, которые могут привести к ложному срабатыванию правила. Например:
		
		`falsepositives:`
		`- Use of a utility by system administrators`

`level`	Нет	Показатель критичности аномалий, которые могут быть найдены с помощью правила. Возможные значения: `informational`, `low`, `medium`, `high`, `critical`.

c. Нажмите на кнопку **OK**.

Описанное Sigma-правило отобразится в списке правил коллекции.

d. Повторите пункты a-c для каждого добавляемого вручную правила.

- Из файлов:

a. Нажмите на кнопку **Добавить файл**.

b. В открывшемся окне выберите один или несколько YAML-файлов, в которых описаны Sigma-правила.

Sigma-правила, описанные в YAML-файлах, отобразятся в списке правил коллекции.

> Если в синтаксисе Sigma-правила допущены ошибки, или отсутствуют обязательные атрибуты, то правило не будет добавлено в коллекцию.

6. Добавленные правила по умолчанию включены. Если необходимо, измените состояние Sigma-правила с помощью флажка слева от имени коллекции. Вы можете изменять состояние всех правил в коллекции с помощью кнопок **Включить все** и **Выключить все**.

7. Для удаления правила из списка выберите правило и нажмите на кнопку **Удалить**.

8. Сохраните внесенные изменения.

Фильтрация Sigma-правил внутри коллекции правил

Если в коллекции содержится большое количество Sigma-правил, и вам необходимо вывести список Sigma-правил с определенными параметрами, вы можете воспользоваться фильтром.

Фильтрация Sigma-правила в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.

4. В блоке **Обнаружение аномалий с помощью Sigma-правил** нажмите на кнопку **Настройка**.

5. В открывшемся окне выберите коллекцию, для которой вы хотите применить фильтрацию правил.
6. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить**.
7. Нажмите на кнопку **Фильтр**.

   Откроется окно с критериями для фильтрации.
8. Задайте значения необходимых вам критериев фильтрации:

   - Критерий **Правило содержит текст** отбирает правила в соответствии с указанным фрагментом содержимого без учета регистра. Вы можете ввести любой атрибут правила и/или его значение.
   - Критерий **Состояние правила** отбирает правила в зависимости от состояния.
   - Критерий **Наличие исключений** отбирает правила в зависимости от наличия исключений.

     Этот критерий доступен только для фильтрации правил внутри коллекции, поставляемой АО "Лаборатория Касперского".
9. Нажмите на кнопку **ОК**.

   В списке правил коллекции отобразятся правила, соответствующие критериям фильтрации.

Фильтрация Sigma-правила в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.
5. В блоке **Обнаружение аномалий с помощью Sigma-правил** выберите с помощью флажка коллекцию, для которой вы хотите применить фильтрацию правил.
6. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить**.
7. Нажмите на кнопку **Фильтр**.

   Откроется окно с критериями для фильтрации.
8. Задайте значения необходимых вам критериев фильтрации:

   - Критерий **Правило содержит текст** отбирает правила в соответствии с указанным фрагментом содержимого без учета регистра. Вы можете ввести любой атрибут правила и/или его значение.
   - Критерий **Состояние правила** отбирает правила в зависимости от состояния.

- Критерий **Наличие исключений** отбирает правила в зависимости от наличия исключений.

  Этот критерий доступен только для фильтрации правил внутри коллекции, поставляемой АО "Лаборатория Касперского".

9. Нажмите на кнопку **ОК**.
10. В списке правил коллекции отобразятся правила, соответствующие критериям фильтрации.

Фильтрация Sigma-правила в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Detection and Response → Обнаружение аномалий с помощью Sigma-правил**.

   В панели результатов перейдите по ссылке **Свойства**.

2. В открывшемся окне выберите коллекцию, для которой вы хотите применить фильтрацию правил.
3. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить**.

4. Нажмите на кнопку **Фильтр**.

   Откроется окно с критериями для фильтрации.

5. Задайте значения необходимых вам критериев фильтрации:

   - Критерий **Правило содержит текст** отбирает правила в соответствии с указанным фрагментом содержимого без учета регистра. Вы можете ввести любой атрибут правила и/или его значение.
   - Критерий **Состояние правила** отбирает правила в зависимости от состояния.
   - Критерий **Наличие исключений** отбирает правила в зависимости от наличия исключений.

     Этот критерий доступен только для фильтрации правил внутри коллекции, поставляемой АО "Лаборатория Касперского".

6. Нажмите на кнопку **ОК**.

   В списке правил коллекции отобразятся правила, соответствующие критериям фильтрации.

Экспорт и импорт Sigma-правил пользовательской коллекции

Экспорт и импорт Sigma-правил в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.

4. В блоке **Обнаружение аномалий с помощью Sigma-правил** нажмите на кнопку **Настройка**.

5. В открывшемся окне выберите нужную пользовательскую коллекцию Sigma-правил.

6. Нажмите на кнопку **Изменить**.

7. Для экспорта Sigma-правила из пользовательской коллекции нажмите на кнопку **Экспорт**.

   Kaspersky Industrial CyberSecurity for Nodes сохранит в стандартной папке загрузок архив sigma.zip.

8. Для импорта Sigma-правил в пользовательскую коллекцию выполните следующие действия:

   a. Нажмите на кнопку **Импорт**.

   b. В открывшемся окне выберите ZIP-архив, в котором содержатся YAML-файлы с описанными Sigma-правилами.

   > Если в синтаксисе Sigma-правила допущены ошибки или отсутствуют обязательные атрибуты, то правило не будет добавлено в коллекцию.

   Sigma-правила, содержащиеся в архиве, отобразятся в списке правил коллекции.

   > Если в импортируемом ZIP-архиве есть дубликаты Sigma-правил, уже имеющихся в коллекции, то такие правила не будут перезаписаны.

9. Сохраните внесенные изменения.

Экспорт и импорт Sigma-правил в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.

5. В блоке **Обнаружение аномалий с помощью Sigma-правил** выберите нужную пользовательскую коллекцию Sigma-правил с помощью флажка напротив имени коллекции.

6. Нажмите на кнопку **Изменить**.

7. Для экспорта Sigma-правила из пользовательской коллекции нажмите на кнопку **Экспорт**.

   Kaspersky Industrial CyberSecurity for Nodes сохранит в стандартной папке загрузок архив sigma.zip.

8. Для импорта Sigma-правил в пользовательскую коллекцию выполните следующие действия:

   a. Нажмите на кнопку **Импорт**.

   b. В открывшемся окне выберите ZIP-архив, в котором содержатся YAML-файлы с описанными Sigma-правилами.

Если в синтаксисе Sigma-правила допущены ошибки или отсутствуют обязательные атрибуты, то правило не будет добавлено в коллекцию.

Sigma-правила, содержащиеся в архиве, отобразятся в списке правил коллекции.

Если в импортируемом ZIP-архиве есть дубликаты Sigma-правил, уже имеющихся в коллекции, то такие правила не будут перезаписаны.

9. Сохраните внесенные изменения.

Экспорт и импорт Sigma-правил в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Detection and Response → Обнаружение аномалий с помощью Sigma-правил**.
2. В панели результатов перейдите по ссылке **Свойства**.
3. В открывшемся окне выберите нужную пользовательскую коллекцию Sigma-правил.
4. Нажмите на кнопку **Изменить**.
5. Для экспорта Sigma-правила из пользовательской коллекции нажмите на кнопку **Экспорт**.

   Kaspersky Industrial CyberSecurity for Nodes сохранит в стандартной папке загрузок архив sigma.zip.
6. Для импорта Sigma-правил в пользовательскую коллекцию выполните следующие действия:
   a. Нажмите на кнопку **Импорт**.
   b. В открывшемся окне выберите ZIP-архив, в котором содержатся YAML-файлы с описанными Sigma-правилами.

   Если в синтаксисе Sigma-правила допущены ошибки или отсутствуют обязательные атрибуты, то правило не будет добавлено в коллекцию.

   Sigma-правила, содержащиеся в архиве, отобразятся в списке правил коллекции.

   Если в импортируемом ZIP-архиве есть дубликаты Sigma-правил, уже имеющихся в коллекции, то такие правила не будут перезаписаны.
7. Сохраните внесенные изменения.

Изменение Sigma-правила

Вы можете вносить любые изменения в пользовательские Sigma-правила. Для Sigma-правил, поставляемых АО "Лаборатория Касперского" в составе предустановленных коллекций, доступно только добавление и удаление исключений, а также изменение состояния.

Изменение Sigma-правила в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.
4. В блоке **Обнаружение аномалий с помощью Sigma-правил** нажмите на кнопку **Настройка**.
5. В открывшемся окне выберите пользовательскую коллекцию Sigma-правил, в которой вы хотите изменить одно или несколько Sigma-правил.
6. Нажмите на кнопку **Изменить**.
7. В открывшемся окне выберите правило, которое вы хотите изменить.
8. Если необходимо, измените состояние правила с помощью флажка слева от имени правила.
9. Нажмите на кнопку **Изменить**.
10. В открывшемся окне внесите необходимые изменения в Sigma-правило.

    Если вы изменяете Sigma-правило, которое поставляется АО "Лаборатория Касперского" в составе коллекции, вам доступно только редактирование исключений для правила.

11. Сохраните внесенные изменения.

Изменение Sigma-правила в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Обнаружение аномалий с помощью Sigma-правил**.
5. В блоке **Обнаружение аномалий с помощью Sigma-правил** выберите пользовательскую коллекцию Sigma-правил, в которой вы хотите изменить одно или несколько Sigma-правил, с помощью флажка напротив имени коллекции.
6. Нажмите на кнопку **Изменить**.
7. В открывшемся окне с помощью флажка выберите правило, которое вы хотите изменить.
8. Если необходимо, измените состояние правила с помощью переключателя **Включено**/**Выключено** над именем правила.
9. Нажмите на кнопку **Изменить**.

10. В открывшемся окне внесите необходимые изменения в Sigma-правило.

    Если вы изменяете Sigma-правило, которое поставляется АО "Лаборатория Касперского" в составе коллекции, вам доступно только редактирование исключений для правила.

11. Сохраните внесенные изменения.

Изменение Sigma-правила в Консоли приложения

1. В дереве Консоли приложения выберите раздел **Detection and Response → Обнаружение аномалий с помощью Sigma-правил**.
2. В панели результатов перейдите по ссылке **Свойства**.
3. В открывшемся окне выберите пользовательскую коллекцию Sigma-правил, в которой вы хотите изменить одно или несколько Sigma-правил.
4. Нажмите на кнопку **Изменить**.
5. В открывшемся окне выберите правило, которое вы хотите изменить.
6. Если необходимо, измените состояние правила с помощью флажка слева от имени правила.
7. Нажмите на кнопку **Изменить**.
8. В открывшемся окне внесите необходимые изменения в Sigma-правило.

    Если вы изменяете Sigma-правило, которое поставляется АО "Лаборатория Касперского" в составе коллекции, вам доступно только редактирование исключений для правила.

9. Сохраните внесенные изменения.

Исключения в Sigma-правиле

Содержимое Sigma-правил, поставляемых с базами программы, закрыто от пользователя. Это связано с тем, что условия срабатывания правил являются интеллектуальной собственностью АО "Лаборатория Касперского" и не подлежат разглашению.

В редакторе изменения Sigma-правила, поставляемого с базами программы, вы можете только добавить исключения из правила внутри секции `detection`.

Шаблон исключения задан следующим образом:

```
detection:
   exclude1:
        - ...
   condition: not 1 of exclude*
```

Данный шаблон предполагает указание исключений с помощью атрибутов `exclude*`, а условие срабатывания правила предполагает выполнение условий, которые скрыты от пользователя, и несовпадение со всеми заданными исключениями.

Например:

```
detection:
   exclude1:
     Image|endswith:
       - '\chrome.exe'
       - '\tor.exe'
   exclude2:
     QueryName|endswith: 'api.parsec.app'
   condition: not 1 of exclude*
```

Изолирование и резервное копирование объектов

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также информацию об изолировании возможно зараженных объектов.

Изолирование возможно зараженных объектов. Карантин

При реагировании на угрозы Kaspersky Industrial CyberSecurity for Nodes может создавать задачи *Помещение файла на карантин*. Это нужно, чтобы минимизировать последствия угрозы. Карантин – это специальное локальное хранилище на компьютере. Администратор может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Industrial CyberSecurity for Nodes использует карантин только при работе с решениями Kaspersky Industrial CyberSecurity Endpoint Detection and Response, Endpoint Detection and Response Expert (on-premises) и Kaspersky Industrial CyberSecurity for Networks. В остальных случаях Kaspersky Industrial CyberSecurity for Nodes помещает файл в резервное хранилище.

Вы можете создавать задачи *Помещение файла на карантин* следующими способами:

- В деталях алерта (только для Kaspersky Industrial CyberSecurity Endpoint Detection and Response).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Industrial CyberSecurity Endpoint Detection and Response.

- С помощью мастера создания задач.

  Вам нужно ввести путь к файлу или контрольную сумму и путь к папке.

Задача Помещение файла на карантин имеет следующие ограничения:

- Размер файла не должен превышать 100 МБ.
- Критически важные системные объекты (англ. System Critical Object, SCO) поместить на карантин невозможно. К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Industrial CyberSecurity for Nodes.
- Вы можете настроить параметры задачи для Kaspersky Industrial CyberSecurity Endpoint Detection and Response в Web Console.

Как создать задачу Помещение файла на карантин в Web Console

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky Industrial CyberSecurity for Nodes**.

   b. В раскрывающемся списке **Тип задачи** выберите **Помещение файла на карантин**.

   c. В поле **Название задачи** введите короткое описание задачи и нажмите **Далее**.

4. В разделе **Область действия задачи** выберите управляемые устройства и нажмите **Далее**.

5. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите на кнопку **Далее**.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes запускает задачу под системной учетной записью (SYSTEM).

6. Завершите работу мастера по кнопке **Готово**. В списке задач отобразится новая задача.

7. Нажмите на новую задачу. Откроется окно свойств задачи.

8. Выберите закладку **Параметры приложения**.

9. В списке файлов нажмите на кнопку **Добавить**. Запустится мастер добавления файла.

10. Для добавления файла вам нужно ввести полный путь к файлу или контрольную сумму и путь к папке.

    Если файл расположен на сетевом диске, введите путь к файлу начиная с символов \\, а не с буквы диска. Например, `\\server\shared_folder\file.exe`. Если путь к файлу содержит букву сетевого диска, вы можете получить ошибку Файл не найден.

11. В окне свойств задачи выберите закладку **Расписание**. Настройте расписание запуска задачи.

    Для этой задачи функция Wake-on-LAN недоступна. Убедитесь, что компьютер включен для выполнения задачи.

12. Нажмите на кнопку **Сохранить**.

13. Установите флажок напротив задачи и нажмите на кнопку **Запустить**.

В результате Kaspersky Industrial CyberSecurity for Nodes переместит файл в карантин.

Если файл заблокирован другим процессом, то задача будет отображаться со статусом **Выполнено**, но сам файл будет помещен на карантин только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Задача *Помещение файла на карантин* может быть завершена с ошибкой *Недостаточно места в хранилище карантина*, если вы пытаетесь поместить на карантин большой файл. Очистите карантин или увеличьте размер карантина. Затем повторите попытку.

Вы можете восстановить файл из карантина или очистить карантин в Web Console.

Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в Консоли администрирования и Web Console.

Просмотр объектов на карантине в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Хранилища**.
3. Перейдите в папку **Карантин.**
4. Информация об объектах, помещенных на карантин, отобразится в правой панели консоли.

Просмотр объектов на карантине в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Карантин**.
4. Информация об объектах, помещенных на карантин, отобразится в правой панели консоли.

Чтобы найти нужный объект в списке объектов на карантине,

отсортируйте объекты или отфильтруйте их.

Сортировка объектов на карантине

По умолчанию объекты на карантине отсортированы в таблице по дате помещения на карантин в обратном хронологическом порядке. Чтобы найти нужный объект, можно отсортировать объекты по столбцам с информацией об объектах. Чтобы отсортировать объекты, выполните следующие действия:

Отсортировать файлы на карантине в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Карантин**.
3. В таблице файлов выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы на карантине будут отсортированы по выбранному критерию.

Отсортировать файлы на карантине в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Карантин**.
3. В таблице файлов выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы на карантине будут отсортированы по выбранному критерию.

Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, можно отфильтровать объекты в таблице – отобразить только те объекты, которые удовлетворяют заданным критериям фильтрации (фильтрам).

Отфильтровать файлы на карантине в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Хранилища**.
3. Перейдите в папку **Карантин**.
4. В правой панели консоли нажмите на ссылку **Фильтр не задан,**.
5. Нажмите на ссылку **Настроить фильтр** и выберите графы для фильтрации в окне **Настройка фильтрации**.
6. Укажите операторы и значения для выбранных граф.
7. Созданные фильтры будут сохранены.
8. Чтобы вернуть отображение всех объектов на карантине, в окне **Настройка фильтрации** нажмите **Очистить все**.

Отсортировать файлы на карантине в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Карантин**.
4. Нажмите на значок фильтра и нажмите на кнопку **Добавить** на закладке **Фильтры**.
5. Выберите свойство, по которому нужно осуществить фильтрацию.
6. Укажите условие и значение для выбранного свойства.
7. Нажмите на кнопку **Применить**.

   Настройки фильтра будут сохранены.
8. Чтобы вернуть отображение всех объектов на карантине, на закладке **Фильтры** нажмите **Очистить все**.

Восстановление содержимого карантина

Kaspersky Industrial CyberSecurity for Nodes помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Вы можете восстановить любой объект с карантина, если вы считаете объект безопасным для защищаемого устройства и хотите его использовать. Чтобы программа Kaspersky Industrial CyberSecurity for Nodes не изолировала этот объект при последующих проверках, вы можете исключить объект из обработки компонентом Постоянная защита файлов и задачами проверки по требованию, либо добавьте объект в Доверенную зону.

Восстановление объектов из карантина может привести к заражению защищаемого устройства.

Вы можете восстановить один или несколько объектов.

Восстановление объектов из карантина в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Дополнительно** → **Хранилища**.
2. Перейдите в папку **Карантин**.
3. Выполните одно из следующих действий:
   - Чтобы восстановить один объект, в контекстном меню этого объекта выберите **Восстановить**.
   - Чтобы восстановить несколько объектов, выберите нужные объекты в списке, используя клавиши CTRL и SHIFT, затем откройте контекстное меню любого из выбранных объектов и выберите **Восстановить**.
4. Объект будет восстановлен в исходную папку.

Восстановление объектов из карантина в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Карантин**.
4. Выберите объекты из списка и нажмите на кнопку **Восстановить**.
5. Объект будет восстановлен в исходную папку.

Удаление объектов с карантина

Можно удалять объекты с карантина в Консоли администрирования и Web Console.

Удаление объектов с карантина в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Хранилища**.
3. Перейдите в папку **Карантин.**
4. Выполните одно из следующих действий:
   - Чтобы удалить один объект, в контекстном меню этого объекта выберите **Удалить**.
   - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши CTRL и SHIFT, затем откройте контекстное меню любого из выбранных объектов и выберите **Удалить**.
5. Объекты будут удалены с карантина.

Удаление объектов с карантина в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Карантин**.
4. Выберите объекты из списка и нажмите на кнопку **Удалить**.
5. Подтвердите операцию удаления.
6. Объекты будут удалены из резервного хранилища.

Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"

Если поведение какого-нибудь объекта дает вам основание подозревать в нем наличие угрозы, а Kaspersky Industrial CyberSecurity for Nodes признает этот объект незараженным, то, возможно, вы встретились с новой, неизвестной угрозой, описание которой еще не добавлено в базы. Вы можете отправить этот объект на исследование в "Лабораторию Касперского". Вирусные аналитики "Лаборатории Касперского" проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Industrial CyberSecurity for Nodes признает его зараженным и сможет его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Отправить объект на исследование в "Лабораторию Касперского" в консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Хранилища**.
3. Перейдите в папку **Карантин** или **Резервное хранилище**.

4. Выполните одно из следующих действий:

   - Чтобы отправить один объект, в контекстном меню этого объекта выберите **Отправить в "Лабораторию Касперского"**.

   - Чтобы отправить несколько объектов, выберите нужные объекты в списке, используя клавиши CTRL и SHIFT, затем откройте контекстное меню любого из выбранных объектов и выберите **Отправить в "Лабораторию Касперского"**.

5. Выберите папку для сохранения объекта на вашем компьютере.

6. После этого вам будет предложено перейти на веб-сайт Kaspersky Threat Intelligence Portal и загрузить сохраненный объект, чтобы получить о нем подробную информацию.

Отправить объект на исследование в "Лабораторию Касперского" в Web Console

1. Откройте Web Console.

2. В дереве консоли выберите папку **Операции** → **Хранилища**.

3. Перейдите в папку **Карантин** или **Файлы резервных копий**.

4. Выберите объекты из списка и нажмите на кнопку **Отправить в "Лабораторию Касперского"**.

5. Выберите папку для сохранения объекта на вашем компьютере.

6. После этого вам будет предложено перейти на веб-сайт Kaspersky Threat Intelligence Portal и загрузить сохраненный объект, чтобы получить о нем подробную информацию.

Невозможно в Консоли администрирования и Web Console отправить для анализа в "Лабораторию Касперского" объекты карантина и резервного хранилища, если они мигрировали после обновления приложения версии 4.0 и ниже до версии 4.5 и выше или были помещены в хранилища по сценариям Kaspersky Anti Targeted Attack Platform или Kaspersky Industrial CyberSecurity for Networks.

Настройка параметров карантина

Вы можете настраивать параметры карантина. Новые параметры карантина применяются сразу после сохранения.

Настройка параметров карантина в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне политики выберите **Дополнительные возможности** → **Хранилища** и нажмите на кнопку **Настройка**.

4. Перейдите на закладку **Карантин**.

5. Укажите настройки карантина (см. таблицу ниже).

6. Сохраните внесенные изменения.

Настройка параметров карантина в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите **Дополнительные возможности → Хранилища** и нажмите на кнопку **Настроить**.
5. Перейдите на вкладку **Карантин**.
6. Укажите настройки карантина (см. таблицу ниже).
7. Сохраните внесенные изменения.

Параметры карантина

Параметр	Описание
Ограничить размер карантина до	Если функция включена, Kaspersky Industrial CyberSecurity for Nodes отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 1024 МБ) Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен максимальный размер карантина* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа. При этом приложение прекращает помещать новые объекты на карантин. Вам нужно вручную очистить карантин. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes не отслеживает суммарный размер объектов в карантине. По умолчанию функция выключена.
Порог доступного пространства	Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes отслеживает минимальный объем свободного места в папке карантина (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен порог свободного места в карантине* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа. Флажок **Порог доступного пространства** активен, если установлен флажок **Ограничить размер карантина до**. По умолчанию функция включена.

Резервное копирование объектов. Резервное хранилище

Kaspersky Industrial CyberSecurity for Nodes сохраняет в папке Резервное хранилище зашифрованные копии объектов, которые были вылечены или удалены.

Если объект является частью составного объекта (например, входит в архив), Kaspersky Industrial CyberSecurity for Nodes сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Industrial CyberSecurity for Nodes признает зараженным один из объектов в составе почтовой базы, он сохраняет копию всей почтовой базы.

Если объект, который Kaspersky Industrial CyberSecurity for Nodes помещает в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске.

Можно восстановить файлы из резервного хранилища как в исходную папку, так и в другую папку на защищаемом устройстве. Вы можете восстановить файл из резервного хранилища, если зараженный файл содержал важную информацию, но при лечении этого файла программа Kaspersky Industrial CyberSecurity for Nodes не смогла сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению защищаемого устройства.

Просмотр объектов в резервном хранилище

Этот раздел содержит информацию о том как просмотреть список файлов, находящихся в резервном хранилище.

Просмотр объектов в резервном хранилище в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище**.
4. Информация об объектах, помещенных в резервное хранилище, отобразится в правой панели консоли.

Просмотр объектов в резервном хранилище в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище.**
4. Информация об объектах, помещенных в резервное хранилище, отобразится в правой панели консоли.

Просмотр объектов в резервном хранилище в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Хранилища** → **Резервное хранилище**.
2. Информация об объектах, помещенных в резервное хранилище, отобразится в правой панели консоли.

Чтобы найти нужный объект в списке объектов в резервном хранилище,

отсортируйте объекты или отфильтруйте их.

Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их попадания в резервное хранилище в обратном хронологическом порядке. Чтобы найти нужный файл, отсортируйте файлы по содержимому любого столбца в панели результатов.

Отсортировать файлы в резервном хранилище в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище**.
4. В таблице файлов выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

Отсортировать файлы в резервном хранилище в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище**.
4. В таблице файлов выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

Отсортировать файлы в резервном хранилище в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Хранилища** → **Резервное хранилище**.
2. В таблице файлов выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

Фильтрация файлов в резервном хранилище

Чтобы найти нужный файл в резервном хранилище, вы можете отфильтровать файлы, чтобы в списке отображались только те файлы, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

Фильтрация файлов в резервном хранилище в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительные возможности** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище**.
4. В правой панели консоли нажмите на ссылку **Фильтр не задан,**.
5. Нажмите на ссылку **Настроить фильтр** и выберите графы для фильтрации в окне **Настройка фильтрации**.

6. Укажите операторы и значения для выбранных граф.
7. Созданные фильтры будут сохранены.
8. Чтобы вернуть отображение всех объектов в резервном хранилище, в окне **Настройка фильтрации** нажмите **Очистить все**.

Фильтрация файлов в резервном хранилище в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище**.
4. Нажмите на значок фильтра и нажмите на кнопку **Добавить** на закладке **Фильтры**.
5. Выберите свойство, по которому нужно осуществить фильтрацию.
6. Укажите условие и значение для выбранного свойства.
7. Нажмите на кнопку **Применить**.

   Настройки фильтра будут сохранены.
8. Чтобы вернуть отображение всех объектов в резервном хранилище, на закладке **Фильтры** нажмите **Очистить все**.

Фильтрация файлов в резервном хранилище в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Хранилища** → **Резервное хранилище**.
2. В таблице файлов выберите заголовок графы и нажмите на значок фильтра в левом верхнем углу.
3. Настройте параметры фильтра и нажмите **OK**.

   Настройки фильтра будут сохранены.

Восстановление файлов из резервного хранилища

Kaspersky Industrial CyberSecurity for Nodes хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный зараженный файл содержал важную информацию и при лечении файла приложение Kaspersky Industrial CyberSecurity for Nodes не смогло сохранить его целостность, в результате чего информация в файле стала недоступной;
- если вы считаете файл безопасным для защищаемого устройства и хотите его использовать. Чтобы приложение Kaspersky Industrial CyberSecurity for Nodes не признавало файл зараженным при последующих проверках, вы можете исключить его из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию.

Восстановление файлов из резервного хранилища может привести к заражению защищаемого устройства.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходное местоположение (по умолчанию), в специальную папку для восстановленных объектов на защищаемом устройстве, в указанную папку на защищаемом устройстве, на котором установлена Консоль приложения.

По умолчанию, когда Kaspersky Industrial CyberSecurity for Nodes восстанавливает файл, его копия сохраняется в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

Восстановление файлов из резервного хранилища в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Дополнительно** → **Хранилища**.
2. Перейдите в папку **Резервное хранилище**.
3. Выполните одно из следующих действий:
   - Чтобы восстановить один объект, в контекстном меню этого объекта выберите **Восстановить**.
   - Чтобы восстановить несколько объектов, выберите нужные объекты в списке, используя клавиши **Ctrl** и **Shift**, затем откройте контекстное меню любого из выбранных объектов и выберите **Восстановить**.
4. Объект будет восстановлен в исходную папку.

Восстановление файлов из резервного хранилища в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище**.
4. Выберите объекты из списка нажмите на кнопку **Восстановить**.
5. Объект будет восстановлен в исходную папку.

Восстановление файлов из резервного хранилища в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Хранилища** → **Резервное хранилище**.

2. В панели результатов узла **Резервное хранилище** выполните одно из следующих действий:

   - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.

   - Чтобы восстановить несколько объектов, выберите нужные объекты, используя клавиши **Ctrl** или **Shift**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

3. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.

   Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.

4. Выполните одно из следующих действий:

   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.

   - Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления при установке приложения, выберите **Восстановить в папку, используемую по умолчанию**.

   - Чтобы сохранить объект в другую папку на защищаемом устройстве, на котором установлена Консоль приложения, выберите **Восстановить в папку на локальном компьютере**, а затем выберите нужную папку или укажите путь к ней.

5. Если вы не хотите сохранить копию файла в папке резервного хранилища после его восстановления, установите флажок **Удалить объекты из хранилища после восстановления** (по умолчанию флажок снят).

6. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

7. Нажмите на кнопку **OK**.

8. Kaspersky Industrial CyberSecurity for Nodes начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Industrial CyberSecurity for Nodes:

      - **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.

      - **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.

      - **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Заменить** или **Переименовать**, к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.

c. Нажмите на кнопку **OK**.

Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект.

Удаление файлов из резервного хранилища

Удаление файлов из резервного хранилища в Консоли администрирования Kaspersky Security Center

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите папку **Дополнительно** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище**. В правой панели отобразится список объектов, находящихся в резервном хранилище.
4. Выполните одно из следующих действий:
   - Чтобы удалить один объект, в контекстном меню этого объекта выберите **Удалить**.
   - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **Ctrl** и **Shift**, затем откройте контекстное меню любого из выбранных объектов и выберите **Удалить**.
5. Объекты будут удалены из резервного хранилища.

Удаление файлов из резервного хранилища в Web Console

1. Откройте Web Console.
2. В дереве консоли выберите папку **Операции** → **Хранилища**.
3. Перейдите в папку **Резервное хранилище.**
4. Выберите объекты из списка нажмите на кнопку **Удалить**.
5. Объекты будут удалены из резервного хранилища.

Удаление файлов из резервного хранилища в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Хранилища** → **Резервное хранилище**.
2. В правой панели отобразится список объектов, находящихся в резервном хранилище.

3. Выполните одно из следующих действий:

   - Чтобы удалить один объект, в контекстном меню этого объекта выберите **Удалить**.
   - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **Ctrl** и **Shift**, затем откройте контекстное меню любого из выбранных объектов и выберите **Удалить**.

4. Объекты будут удалены из резервного хранилища.

Настройка параметров резервного хранилища

Настройка параметров резервного хранилища в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Дополнительные возможности** → **Хранилища** и нажмите на кнопку **Настройка**.
4. Перейдите на вкладку **Резервное хранилище**.
5. Укажите настройки резервного хранилища (см. таблицу ниже).
6. Сохраните внесенные изменения.

Настройка параметров резервного хранилища в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите **Дополнительные возможности** → **Хранилища** и нажмите на кнопку **Настроить**.
5. Перейдите на вкладку **Резервное хранилище**.
6. Укажите настройки резервного хранилища (см. таблицу ниже).
7. Сохраните внесенные изменения.

Настройка параметров резервного хранилища в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Хранилища** → **Резервное хранилище**.
2. В панели результатов узла **Резервное хранилище** нажмите **Свойства**.
3. В окне **Свойства: Резервное хранилище** укажите настройки резервного хранилища (см. таблицу ниже).
4. Сохраните внесенные изменения.

Параметры резервного хранилища

Параметр	Описание
Хранить объекты не более	Если функция включена, то максимальный срок хранения файлов ограничен заданным интервалом времени. По умолчанию максимальный срок хранения файлов составляет 30 дней. По истечении максимального срока хранения Kaspersky Industrial CyberSecurity for Nodes удаляет наиболее старые файлы из резервного хранилища.
Ограничить размер хранилища до	Если функция включена, Kaspersky Industrial CyberSecurity for Nodes отслеживает суммарный размер объектов, размещенных в папке резервного хранилища. В случае превышения заданного значения (по умолчанию 400 МБ) Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен максимальный размер резервного хранилища* и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа. Если функция выключена, Kaspersky Industrial CyberSecurity for Nodes не отслеживает суммарный размер объектов в резервном хранилище. По умолчанию функция выключена.
Ограничить порог доступного пространства до	Если функция включена, Kaspersky Industrial CyberSecurity for Nodes отслеживает минимальный объем свободного места в резервном хранилище (по умолчанию 100 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes регистрирует событие *Превышен порог доступного пространства в резервном хранилище* и выполняет уведомление в соответствии с параметрами уведомлений о событиях такого типа. Флажок **Ограничить порог доступного пространства до** активен, если установлен флажок **Ограничить размер хранилища до**. По умолчанию функция включена.

Если объем объектов в резервном хранилище превышает значение максимального размера резервного хранилища или превышает порог доступного пространства, Kaspersky Industrial CyberSecurity for Nodes уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

Статистика резервного хранилища

Можно просматривать информацию о текущем состоянии резервного хранилища – статистику резервного хранилища.

Чтобы просмотреть статистику резервного хранилища, выполните следующие действия:

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Хранилища** → **Резервное хранилище**.

2. В панели результатов узла **Резервное хранилище** нажмите **Статистика**.

   Откроется окно **Резервное хранилище. Статистика**. В окне **Резервное хранилище. Статистика** отображается информация о текущем состоянии резервного хранилища (см. таблицу ниже).

Информация о текущем состоянии резервного хранилища

Поле	Описание
Текущий размер резервного хранилища	Объем данных в папке резервного хранилища; учитывается размер файлов в зашифрованном виде.
Всего объектов	Количество объектов в резервном хранилище в текущий момент.

Устранение необработанных угроз

Kaspersky Industrial CyberSecurity for Nodes фиксирует информацию о файлах, которые по каким-либо причинам не были обработаны. Эта информация записывается в виде событий в список активных угроз.

Зараженный файл считается *обработанным*, если Kaspersky Industrial CyberSecurity for Nodes в процессе проверки компьютера на вирусы и другие приложения, представляющие угрозу, вылечил или удалил угрозу. Если Kaspersky Industrial CyberSecurity for Nodes не совершил действие с этим файлом согласно заданным настройкам приложения, файл будет помещен в список активных угроз.

При наличии необработанных угроз Kaspersky Industrial CyberSecurity for Nodes в консоли Kaspersky Security Center статус устройства будет изменен на *Критический* – ⓘ.

Вы можете обрабатывать активные угрозы в Консоли администрирования и Web Console.

Для обработки активных угроз в консоли Kaspersky Security Center необходимо включить передачу данных о необработанных файлах на Сервер администрирования. По умолчанию передача данных включена.

Как обработать угрозу в Консоли администрирования Kaspersky Security Center

1. В Консоли администрирования перейдите в папку **Сервер администрирования → Дополнительно → Хранилища → Активные угрозы**.

   Откроется список активных угроз.

2. Выберите объект, который вы хотите обработать.

3. Выберите способ обработки угрозы:

   - **Лечить**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

   - **Удалить**. Если выбран этот вариант действия, то приложение удаляет обнаруженный зараженный файл из хранилища активных угроз. При этом приложение оставляет обнаруженный файл в памяти компьютера. Для устранения угрозы на компьютере нужно выбрать **Лечить**.

Как обработать угрозу в Web Console

1. В главном окне Web Console выберите **Операции → Хранилища → Активные угрозы**.

   Откроется список активных угроз.

2. Выберите объект, который вы хотите обработать.

3. Выберите способ обработки угрозы:

   - **Лечить**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить обнаруженный зараженный файл. Если лечение невозможно, то приложение удаляет файл.

   - **Удалить**. Если выбран этот вариант действия, то приложение удаляет обнаруженный зараженный файл из хранилища активных угроз. При этом приложение оставляет обнаруженный файл в памяти компьютера. Для устранения угрозы на компьютере нужно выбрать **Лечить**.

Блокировка доступа к сетевым ресурсам. Заблокированные сетевые сеансы

В этом разделе описано, как заблокировать удаленные устройства и настроить параметры списка заблокированных сетевых сеансов.

Список заблокированных сетевых сеансов

По умолчанию Список заблокированных сетевых сеансов доступен, если установлен хотя бы один из следующих компонентов: Защита от сетевых угроз или Защита от шифрования. Эти компоненты обнаруживают удаленные попытки зашифровать, открыть или исполнить файлы в папках общего доступа защищаемого устройства или сетевого хранилища в соответствии со списком заблокированных сетевых сеансов. Информация о заблокированных сетевых сеансах со всех защищаемых устройств отправляется в Kaspersky Security Center. Kaspersky Industrial CyberSecurity for Nodes блокирует текущий сеанс и делает недоступными общие папки или папки сетевого хранилища в рамках текущего сеанса.

Список заблокированных сетевых сеансов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Для задачи *Защита от сетевых угроз*: обнаружена активность, характерная для сетевых атак.

  > Kaspersky Industrial CyberSecurity for Nodes очищает список заблокированных узлов при перезапуске приложения или при изменении настроек Защиты от сетевых угроз.

- Для задачи *Защита от шифрования*: обнаружено вредоносное шифрование со стороны устройства, обращающегося к сетевым файловым ресурсам.

При обнаружении вредоносной активности или попыток шифрования задача отправляет информацию об атакующем сетевом сеансе в Список заблокированных сетевых сеансов, а для текущего сеанса атакующего устройства создается событие *Предупреждение*. Все попытки данного сеанса получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

Если локальный уникальный идентификатор (LUID) узла, инициировавшего атакующий сетевой сеанс, добавлен в Список заблокированных сетевых сеансов, Kaspersky Industrial CyberSecurity for Nodes определяет IP-адрес этого узла и добавляет его в Список заблокированных сетевых сеансов вместо идентификатора LUID атакующего узла.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes удаляет заблокированные сетевые сеансы из списка через 30 минут после добавления. Доступ к сетевым файловым ресурсам восстанавливается автоматически после удаления сетевых сеансов из Списка заблокированных сетевых сеансов. Вы можете указать период, после которого заблокированные сетевые сеансы автоматически разблокируются.

> В случае запрета доступа к управлению хранилищами какому-либо пользователю, Список заблокированных сетевых сеансов останется доступным. Параметры заблокированных сетевых сеансов не могут быть изменены, если у пользователя отсутствует разрешение типа **Изменение прав** для управления Kaspersky Industrial CyberSecurity for Nodes.

Управление списком заблокированных сетевых сеансов

Чтобы добавить сетевые сеансы, проявляющие вредоносную активность или попытки шифрования, в список заблокированных сетевых сеансов и заблокировать для них доступ к сетевым файловым ресурсам, хотя бы один из следующих компонентов должен работать в активном режиме:

- Защита от сетевых угроз;
- Защита от шифрования.

Включение блокировки недоверенных узлов в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Контроль активности в сети** → **Настройки защиты от сетевых угроз** и нажмите на кнопку **Настройка**.
4. В открывшемся окне установите флажок **Защита от сетевых угроз**.
5. На закладке **Общие** установите режим **Блокировать**.
6. Установите флажок **Блокировать атакующие устройства на** и укажите время блокировки.
7. Сохраните внесенные изменения.

Чтобы настроить блокировку недоверенных сетевых сеансов для компонента Защита от шифрования в свойствах политики:

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне политики выберите **Постоянная защита компьютера** → **Защита от шифрования** и нажмите на кнопку **Настройка**.
4. В открывшемся окне установите флажок **Защита от шифрования**.
5. Перейдите на закладку **Защита общих папок** и установите флажок **Защищать папки общего доступа**.
6. Выберите вариант **Блокировать соединение на** и укажите время блокировки.
7. Если требуется, укажите область защиты и исключения по IP-адресам и маскам.
8. Сохраните внесенные изменения.

Включение блокировки недоверенных узлов в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Контроль активности в сети** → **Защита от сетевых угроз** и нажмите на кнопку **Настроить**.
5. В открывшемся окне установите флажок **Включить Защиту от сетевых угроз**.
6. Установите режим **Блокировать**.
7. Установите флажок **Блокировать атакующие устройства на** и укажите время блокировки.
8. Если требуется, укажите исключения по IP-адресам.
9. Сохраните внесенные изменения.

Чтобы настроить блокировку недоверенных сетевых сеансов для компонента Защита от шифрования, выполните следующие действия:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Постоянная защита компьютера** → **Защита от шифрования** и нажмите на кнопку **Настроить**.
5. В открывшемся окне установите флажок **Включить защиту от шифрования**.
6. Перейдите на закладку **Защита общих папок** и установите флажок **Включить защиту папок общего доступа от внешнего шифрования**.
7. Выберите вариант **Блокировать соединение** и укажите время блокировки в разделе **При обнаружении внешнего шифрования папок общего доступа.**
8. Если требуется, укажите область защиты и исключения по IP-адресам и маскам.
9. Сохраните внесенные изменения.

Включение блокировки недоверенных узлов в Консоли приложения

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера** → **Защита от сетевых угроз**.
2. В панели результатов узла **Защита от сетевых угроз** нажмите **Свойства**.

   Откроется окно **Свойства: Защита от сетевых угроз**.

3. В открывшемся окне установите флажок **Защита от сетевых угроз**.

4. На закладке **Общие** установите режим **Блокировать**.

5. Установите флажок **Блокировать атакующие устройства на** и укажите время блокировки.

6. Сохраните внесенные изменения.

Чтобы настроить блокировку недоверенных сетевых сеансов для компонента Защита от шифрования, выполните следующие действия:

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes выберите **Постоянная защита компьютера → Защита от шифрования**.

2. В панели результатов узла **Защита от шифрования** нажмите **Свойства**.

3. В открывшемся окне установите флажок **Защита от шифрования**.

4. Перейдите на закладку **Защита общих папок** и установите флажок **Защищать папки общего доступа**.

5. Выберите вариант **Блокировать соединение на** и укажите время блокировки.

6. Если требуется, укажите область защиты и исключения по IP-адресам и маскам.

7. Сохраните внесенные изменения.

Настройка параметров списка заблокированных сеансов в Консоли приложения

1. В дереве Консоли приложения разверните узел **Хранилища**.

2. Выберите вложенный узел **Заблокированные сетевые сессии**.

3. В панели результатов нажмите на кнопку **Свойства**.

4. В открывшемся окне установите флажок **Блокировать атакующие устройства на** и укажите время блокировки.

5. Чтобы восстановить доступ для всех заблокированных сетевых сеансов, нажмите **Разблокировать все** в верхней части окна.

   Все сетевые сеансы будут удалены из списка и разблокированы.

6. Чтобы удалить сетевые сеансы из списка заблокированных, в списке заблокированных сетевых сеансов в панели результатов выберите один или несколько сеансов и нажмите **Разблокировать выбранное** в верхней части окна.

   Выбранные сетевые сеансы будут разблокированы.

Запись событий. Журналы Kaspersky Industrial CyberSecurity for Nodes

В этом разделе приведена информация о работе с журналами Kaspersky Industrial CyberSecurity for Nodes.

Способы записи событий Kaspersky Industrial CyberSecurity for Nodes

События Kaspersky Industrial CyberSecurity for Nodes делятся на две группы:

- события, связанные с работой компонентов приложения, обработкой объектов в задачах Kaspersky Industrial CyberSecurity for Nodes;
- события, связанные с управлением Kaspersky Industrial CyberSecurity for Nodes, например: запуск приложения, создание или удаление задач, изменение параметров задач.

Kaspersky Industrial CyberSecurity for Nodes использует следующие способы записи событий:

- **Журналы работы компонентов приложения**. Журналы содержат информацию о событиях, возникших во время работы компонентов приложения.
- **Журнал системного аудита**. Журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Industrial CyberSecurity for Nodes. А также включает информацию о событиях, связанных с нарушениями безопасности или с попытками нарушения безопасности на защищаемом устройстве.
- **Журнал событий**. Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Industrial CyberSecurity for Nodes. Журнал событий доступен в "Просмотре событий" Microsoft Windows.

Файлы, доступные для загрузки по следующим ссылкам, содержат таблицы с полными списками событий Kaspersky Industrial CyberSecurity for Nodes следующих категорий:

- События, которые Kaspersky Industrial CyberSecurity for Nodes записывает в журнал событий.

  DOWNLOAD WEL-EVENTS.ZIP
- События, которые Kaspersky Industrial CyberSecurity for Nodes отправляет на Сервер администрирования.

  DOWNLOAD KSC-EVENTS.ZIP

Настройка параметров журнала

Вы можете настраивать следующие параметры журналов Kaspersky Industrial CyberSecurity for Nodes:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита;
- местоположение папки, в которой Kaspersky Industrial CyberSecurity for Nodes сохраняет файлы журналов выполнения задач и журнала системного аудита;
- пороги формирования событий *Базы устарели*, *Базы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*;
- события, которые Kaspersky Industrial CyberSecurity for Nodes сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий";
- событий, которые Kaspersky Industrial CyberSecurity for Nodes отправляет на SIEM-сервер.

Настроить параметры журналов с помощью Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Журналы и уведомления**.
4. В разделе **Журналы выполнения задач** нажмите **Настройка**.

   Откроется окно **Уведомления**.
5. В открывшемся окне выберите журнал, параметры которого вы хотите настроить, и укажите параметры для конкретных событий:
   - Место сохранения событий: локальный отчет и/или журнал событий Windows;
   - Уведомления о событиях: уведомлять по почте, уведомлять средствами службы терминалов и/или уведомлять путем запуска исполняемого файла;
   - Отправлять ли событие на SIEM сервер и/или в Kaspersky Security Center.
6. Настройте пороги формирования событий, нажав на кнопку **Настройка порогов формирования событий**.
7. В открывшемся окне укажите количество дней, по истечении которого будут регистрироваться события *Базы устарели*, *Базы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*.
8. Укажите настройки почтовых уведомлений, нажав на кнопку **Настройка почтовых уведомлений**.
9. Сохраните внесенные изменения.

Настроить параметры журналов с помощью Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Журналы и уведомления** → **Журналы выполнения задач** и нажмите на кнопку **Настроить**.
5. В открывшемся окне на вкладке **Уведомления** выберите журнал, параметры которого вы хотите настроить, и укажите параметры для конкретных событий:
   - Место сохранения событий: локальный отчет и/или журнал событий Windows;
   - Уведомления о событиях: уведомлять по почте, уведомлять средствами службы терминалов и/или уведомлять путем запуска исполняемого файла;
   - Отправлять ли событие на SIEM сервер и/или в Kaspersky Security Center.
6. Укажите настройки почтовых уведомлений на вкладке **Настройки уведомлений по электронной почте**.
7. Сохраните внесенные изменения.

Настроить параметры журналов с помощью Консоли приложения

1. В дереве Консоли приложения откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

   Откроется окно **Уведомления**.
3. В открывшемся окне выберите журнал, параметры которого вы хотите настроить, и укажите параметры для конкретных событий:
   - Место сохранения событий: локальный отчет и/или журнал событий Windows;
   - Уведомления о событиях: уведомлять по почте, уведомлять средствами службы терминалов и/или уведомлять путем запуска исполняемого файла;
   - Отправлять ли событие на SIEM сервер и/или в Kaspersky Security Center.
4. Настройте пороги формирования событий, нажав на кнопку **Настройка порогов формирования событий**.
5. В открывшемся окне укажите количество дней, по истечении которого будут регистрироваться события *Базы устарели (дни)*, *Базы сильно устарели (дни)* и *Проверка важных областей защищаемого устройства давно не выполнялась (дни)*.
6. Укажите настройки почтовых уведомлений, нажав на кнопку **Настройка почтовых уведомлений**.
7. Сохраните внесенные изменения.

Сортировка событий в журнале

По умолчанию события отображаются в журнале в обратном хронологическом порядке.

Чтобы отсортировать события в журнале, выполните следующие действия:

1. В дереве Консоли приложения откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите нужный журнал.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в списке событий.

Результат сортировки сохранится до следующего просмотра журнала.

Фильтрация событий в журнале

Вы можете отобразить в журнале записи только о тех событиях, которые удовлетворяют заданным условиям фильтрации (фильтрам).

Чтобы отфильтровать события в журнале, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Журналы и уведомления**.
2. Выберите журнал, для которого вы хотите настроить фильтр и в панели результатов нажмите **Фильтр**.

   Откроется окно **Настройки фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите графу, по которой вы хотите отфильтровать события.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.

   c. В списке **Значение поля** выберите значение фильтра.

   d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Настройки фильтра**.

4. Если требуется, выполните одно из следующих действий:

   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.

5. Нажмите на кнопку **ОК**, чтобы сохранить условия фильтрации событий журнала.

   В списке событий журнала отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журнала.

Чтобы выключить действие фильтра, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Журналы и уведомления**.
2. Выберите журнал, для которого вы хотите удалить фильтр, и нажмите на кнопку **Снять фильтр**.

   В списке событий журнала отобразятся все события.

Удаление событий из журнала

По умолчанию Kaspersky Industrial CyberSecurity for Nodes хранит записи в журналах в течение 30 дней. Вы можете изменять длительность хранения записей в журналах.

Чтобы удалить события из журнала, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Журналы и уведомления**.
2. Выберите журнал, для которого вы хотите удалить события и в панели результатов нажмите **Очистить**.
3. Подтвердите операцию очистки.

   Журнал будет очищен.

Экспорт информации из журнала

Вы можете экспортировать информацию из журналов в файл в CSV или TXT-формате.

Чтобы экспортировать события из журналов, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Журналы и уведомления**.
2. Выберите любой журнал и в панели результатов нажмите на кнопку **Экспортировать журнал**.

   Откроется окно **Сохранить как**.

3. Укажите имя, местоположение файла и тип файла, в который вы хотите экспортировать информацию из журналов.

4. Нажмите на кнопку **Сохранить**.

Информация из журналов будет сохранена в указанный файл.

Журнал системного аудита

Kaspersky Industrial CyberSecurity for Nodes ведет системный аудит событий, связанных с управлением Kaspersky Industrial CyberSecurity for Nodes. Приложение сохраняет информацию, например, о запуске приложения, запуске и остановке задач Kaspersky Industrial CyberSecurity for Nodes, изменении параметров задач, создании и удалении задач проверки по требованию. Также приложение сохраняет информацию о событиях, связанных с нарушениями безопасности или с попытками нарушения безопасности на защищаемом устройстве. Записи об этих событиях отображаются в панели результатов при выборе узла **Системный аудит** в Консоли приложения.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes хранит записи в журнале системного аудита в течение 30. Вы можете изменять длительность хранения записей в журнале.

Вы можете указать папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

Журналы работы компонентов и задач

Информация о работе компонентов и задач Kaspersky Industrial CyberSecurity for Nodes отображается в Консоли приложения в панели результатов при выборе узла с названием компонента или задачи в разделе **Журналы и уведомления**.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes хранит записи в журналах работы компонентов и задач в течение 30 дней. Для задач – с момента их завершения. Вы можете изменять длительность хранения записей в журналах работы компонентов и задач.

Вы можете указать папку, в которой Kaspersky Industrial CyberSecurity for Nodes сохраняет файлы журналов работы компонентов и задач, отличную от папки, установленной по умолчанию. Можно также выбрать события, записи о которых Kaspersky Industrial CyberSecurity for Nodes сохраняет в журналах работы компонентов и задач.

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска, а также статистику выполнения задач и параметры задач.

Чтобы просмотреть статистику и информацию о задаче Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Журналы и уведомления**.

2. Выберите нужную задачу и в панели результатов перейдите на вкладку **Статистика**.

Просмотр статистики и информации о задачах Kaspersky Industrial CyberSecurity for Nodes в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска, а также статистику выполнения задач и параметры задач.

Чтобы просмотреть статистику и информацию о задаче Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. В дереве Консоли приложения разверните узел **Журналы и уведомления**.
2. Выберите нужную задачу и в панели результатов перейдите на вкладку **Статистика**.

Просмотр журнала событий Kaspersky Industrial CyberSecurity for Nodes в оснастке "Просмотр событий"

С помощью оснастки "Просмотр событий" в Microsoft Management Console можно просматривать журнал событий Kaspersky Industrial CyberSecurity for Nodes. В журнале содержатся события, зарегистрированные Kaspersky Industrial CyberSecurity for Nodes и необходимые для диагностики сбоев в работе программы.

Вы можете выбирать события для записи в журнал событий на основе следующих критериев:

- **по типам событий**;
- **по уровню детализации**. Уровень детализации соответствует уровню важности событий, которые регистрируются в журнале (информационные, важные или критические события). Наиболее подробным является уровень Информационные события, при котором регистрируются все события. Наименее подробным является уровень Критические события, при котором регистрируются только критические события.

Чтобы просмотреть журнал событий Kaspersky Industrial CyberSecurity for Nodes, выполните следующие действия:

1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

   Откроется Microsoft Management Console.

2. Выберите **Файл** > **Добавить или удалить оснастку**.

   Откроется окно **Добавление и удаление оснасток**.

3. В списке доступных оснасток выберите оснастку **Просмотр событий** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор компьютера**.

4. В окне **Выбор компьютера** укажите защищаемое устройство, на котором установлена программа Kaspersky Industrial CyberSecurity for Nodes, и нажмите на кнопку **OK**.

5. В окне **Добавление и удаление оснасток** нажмите на кнопку **OK**.

   В дереве Microsoft Management Console появится узел **Просмотр событий**.

6. В дереве Консоли раскройте узел **Просмотр событий** и выберите вложенный узел **Журналы приложений и служб** > **Kaspersky Industrial CyberSecurity for Nodes**.

Откроется журнал событий Kaspersky Industrial CyberSecurity for Nodes.

Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к устройству, о событиях, связанных с работой Kaspersky Industrial CyberSecurity for Nodes, и о состоянии антивирусной защиты устройства.

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к устройству, и пользователи терминального устройства могут получать информацию о событиях типа *Обнаружен объект*, возникших в задаче Постоянная защита файлов.

Можно активировать уведомления администратора или пользователей несколькими способами:

- Средства службы терминалов.

  Вы можете применять этот способ для оповещения пользователей терминального защищаемого устройства, если защищаемое устройство является терминальным.

- Запуск исполняемого файла.

  При возникновении события запускается исполняемый файл, который хранится на локальном диске защищаемого устройства.

- Отправка по электронной почте.

  Этот способ использует для передачи сообщений электронную почту.

Вы можете составить текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется стандартный текст сообщений.

Настройка уведомлений администратора и пользователей

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений, а также составление текста сообщения.

Как настроить уведомления о событиях в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В окне свойств политики выберите **Журналы и уведомления**.

4. В разделе **Журналы выполнения задач** нажмите **Настройка**.

   Откроется окно **Уведомления**.

5. Выберите событие, для которого вы хотите выбрать способ уведомления, и нажмите на кнопку **Настройка уведомлений**.

   Откроется окно **Настройка уведомлений**.

6. Для уведомления по электронной почте, на вкладке **Эл. почта** можно добавить текст сообщения, который будет отображаться в сообщении о событии.

   Чтобы добавить поля с информацией о событии, нажмите на кнопку **Переменная** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

7. Для уведомления путем запуска исполняемого файла, на вкладке **Исполняемый файл** выберите файл на локальном диске защищаемого устройства или введите полный путь к нему. Этот файл будет выполняться на защищаемом устройстве при возникновении события. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

   Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

8. Для уведомления через службу терминалов, на вкладке **Служба терминалов** можно добавить текст сообщения, который будет отображаться в сообщении о событии.

   Чтобы добавить поля с информацией о событии, нажмите на кнопку **Переменная** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

9. Сохраните внесенные изменения.

Как настроить уведомления о событиях в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.

2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.

4. Перейдите в раздел **Журналы и уведомления → Журналы выполнения задач** и нажмите на кнопку **Настроить**.

5. В открывшемся окне выберите событие, для которого вы хотите выбрать способ уведомления, и нажмите на него.

   Откроется окно **Настройки уведомлений**.

6. Для уведомления по электронной почте, в разделе **Уведомление пользователей** установите флажок **По электронной почте** и добавьте текст сообщения, которое будет отображаться в сообщении о событии.

   Чтобы добавить поля с информацией о событии, нажмите на кнопку **Добавить переменную** и выберите нужные пункты из списка. Поля с информацией о событиях описаны в таблице в этом разделе.

Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **Сбросить**.

7. Для уведомления путем запуска исполняемого файла, в разделе **Уведомление администраторов** установите флажок **Путем запуска исполняемого файла** и введите полный путь к файлу на локальном диске защищаемого устройства. Этот файл будет выполняться на защищаемом устройстве при возникновении события. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

   Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

8. Для уведомления через службу терминалов, в разделе **Уведомление администраторов** установите флажок **Средствами службы терминалов** и добавьте текст сообщения, которое будет отображаться в сообщении о событии.

   Чтобы добавить поля с информацией о событии, нажмите на кнопку **Добавить переменную** и выберите нужные пункты из списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **Сбросить**.

9. Сохраните внесенные изменения.

Как настроить уведомления о событиях в Консоли приложения

1. В дереве Консоли приложения откройте контекстное меню узла **Журналы и уведомления**.

2. Выберите пункт **Свойства**.

   Откроется окно **Уведомления**.

3. Выберите событие, для которого вы хотите выбрать способ уведомления, и нажмите на кнопку **Настройка уведомлений**.

   Откроется окно **Настройка уведомлений**.

4. Для уведомления по электронной почте, на вкладке **Эл. почта** можно добавить текст сообщения, который будет отображаться в сообщении о событии.

   Чтобы добавить поля с информацией о событии, нажмите на кнопку **Переменная** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

5. Для уведомления путем запуска исполняемого файла, на вкладке **Исполняемый файл** выберите файл на локальном диске защищаемого устройства или введите полный путь к нему. Этот файл будет выполняться на защищаемом устройстве при возникновении события. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

   Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

6. Для уведомления через службу терминалов, на вкладке **Служба терминалов** можно добавить текст сообщения, который будет отображаться в сообщении о событии.

   Чтобы добавить поля с информацией о событии, нажмите на кнопку **Переменная** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

7. Сохраните внесенные изменения.

Поля с информацией о событии

Переменная	Описание
%EVENT_TYPE%	Тип события.
%EVENT_TIME%	Время возникновения события.
%EVENT_SEVERITY%	Уровень важности события.
%OBJECT%	Имя объекта (в задачах постоянной защиты компьютера и проверки по требованию). В задаче Обновление модулей программы включает название обновления и адрес страницы в интернете с информацией об обновлении.
%VIRUS_NAME%	Имя объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Industrial CyberSecurity for Nodes возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
%VIRUS_TYPE%	Тип обнаруженного объекта по классификации "Лаборатории Касперского", например, "вирус" или "троянская программа". Входит в полное название обнаруженного объекта, которое Kaspersky Industrial CyberSecurity for Nodes возвращает, признав объект зараженным или возможно зараженным. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
%USER_COMPUTER%	В задаче *Постоянная защита файлов* – имя защищаемого устройства пользователя, который обратился к объекту на устройстве.
%USER_NAME%	В задаче *Постоянная защита файлов* – имя пользователя, который обратился к объекту на устройстве.
%FROM_COMPUTER%	Имя защищаемого устройства, с которого поступило уведомление.
%EVENT_REASON%	Причина возникновения события (некоторые события не имеют этого поля).
%ERROR_CODE%	Код ошибки (только для события "внутренняя ошибка задачи").
%TASK_NAME%	Название задачи (имеется только у событий, связанных с выполнением задач).
%PROTOCOL%	Используемый протокол.
%MESSAGE%	Текст сообщения.
%DEVICE_INSTANCEPATH%	Путь к экземпляру устройства.
%DEVICE_VID%	Производитель устройства.
%DEVICE_PID%	Тип контроллера.
%DEVICE_SERIALNUMBER%	Серийный номер устройства.

Настройка почтовых уведомлений

Как настроить почтовые уведомления в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Журналы и уведомления**.
4. В разделе **Журналы выполнения задач** нажмите **Настройка**.

   Откроется окно **Уведомления**.
5. Нажмите на кнопку **Настройка почтовых уведомлений**.

6. В открывшемся окне установите флажок **Отправлять сообщения о событиях**.
7. Укажите данные отправителя в блоке **Отправка уведомлений от имени**: адрес отправителя, SMTP-сервер, порт SMTP-сервера, имя пользователя и пароль.
8. Укажите почтовый адрес получателя в блоке **Получатель уведомлений**.
9. Для проверки корректности заданных настроек нажмите на кнопку **Отправить пробное сообщение**.

   Функционал отправки пробных сообщений доступен только в Консоли администрирования Kaspersky Security Center и Консоли приложения.

10. Укажите режим рассылки **При возникновении события** или **По расписанию (расписание не задано)**. Чтобы задать настройки расписания, нажмите на кнопку **Изменить**.
11. Сохраните внесенные изменения.

Как настроить почтовые уведомления в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.

3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Журналы и уведомления** → **Журналы выполнения задач** и нажмите на кнопку **Настроить**.
5. В открывшемся окне выберите вкладку **Настройки уведомлений по электронной почте**.
6. Установите флажок **Отправлять сообщения о событиях**.
7. Укажите данные отправителя: адрес отправителя, SMTP-сервер, порт SMTP-сервера, имя пользователя и пароль.
8. Укажите почтовый адрес получателя.
9. Укажите режим рассылки **При возникновении событий** или **По расписанию**. Если применимо, то укажите настройки расписания.
10. Сохраните внесенные изменения.

Как настроить почтовые уведомления в Консоли приложения

1. В дереве Консоли приложения откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

   Откроется окно **Уведомления**.

3. Нажмите на кнопку **Настройка почтовых уведомлений**.
4. В открывшемся окне установите флажок **Отправлять сообщения о событиях**.

5. Укажите данные отправителя в блоке **Отправка уведомлений от имени**: адрес отправителя, SMTP-сервер, порт SMTP-сервера, имя пользователя и пароль.

6. Укажите почтовый адрес получателя в блоке **Получатель уведомлений**.

7. Для проверки корректности заданных настроек нажмите на кнопку **Отправить пробное сообщение**.

   Функционал отправки пробных сообщений доступен только в Консоли администрирования Kaspersky Security Center и Консоли приложения.

8. Укажите режим рассылки **При возникновении события** или **По расписанию (расписание не задано)**. Чтобы задать настройки расписания, нажмите на кнопку **Изменить**.

9. Сохраните внесенные изменения.

Настройка обмена информацией с Сервером администрирования

Необходимо выбрать типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes будет передавать на Сервер администрирования Kaspersky Security Center.

Как настроить взаимодействие с Сервером администрирования в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В разделе **Журналы и уведомления** в подразделе **Взаимодействие с Сервером администрирования** нажмите на кнопку **Настройка**.

4. В открывшемся окне выберите типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes будет передавать на Сервер администрирования Kaspersky Security Center:

   - **О файлах карантина**
   - **О файлах резервного хранилища**
   - **О необработанных файлах**
   - **Об установленных устройствах**
   - **О цепочке развития угрозы**
   - **О проектах ПЛК**

5. Сохраните внесенные изменения.

   Kaspersky Industrial CyberSecurity for Nodes будет передавать информацию о выбранных типах объектов на Сервер администрирования.

Как настроить взаимодействие с Сервером администрирования в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. В разделе **Журналы и уведомления** в подразделе **Взаимодействие с Сервером администрирования** нажмите на кнопку **Настроить**.
5. В открывшемся окне выберите типы объектов, информацию о которых Kaspersky Industrial CyberSecurity for Nodes будет передавать на Сервер администрирования Kaspersky Security Center:
   - **Файлы карантина**
   - **Файлы резервного хранилища**
   - **О необработанных файлах**
   - **Заблокированные сетевые сессии**
   - **Установленные устройства**
   - **Цепочка развития угрозы**
   - **Версии проектов ПЛК**
6. Сохраните внесенные изменения.

Настройка формирования инцидентов

В базе данных Сервера администрирования хранится информация о событиях приложения, произошедших на управляемых защищаемых устройствах.

Как настроить формирование инцидентов в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В окне свойств политики выберите **Журналы и уведомления**.
4. В разделе **Инциденты** нажмите **Настройка**.
5. В открывшемся окне, если необходимо, измените выборку событий, на основании которых Kaspersky Industrial CyberSecurity for Nodes будет формировать инциденты (см. таблицу ниже).
6. Сохраните внесенные изменения.

   Параметры формирования инцидентов будут сохранены.

Как настроить формирование инцидентов в Web Console

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Перейдите в раздел **Журналы и уведомления** → **Инциденты** и нажмите на кнопку **Настроить**.
5. В открывшемся окне, если необходимо, измените выборку событий, на основании которых Kaspersky Industrial CyberSecurity for Nodes будет формировать инциденты (см. таблицу ниже).
6. Сохраните внесенные изменения.

   Параметры формирования инцидентов будут сохранены.

Список событий для формирования инцидентов

Событие	Значение по умолчанию
Проект ПЛК не соответствует эталонному	Выбрано
Не удалось сравнить проект ПЛК с эталонным	Выбрано
Не удалось получить данные о проекте ПЛК	Выбрано
Срок действия лицензии истек	Не выбрано
Нарушено Лицензионное соглашение	Выбрано
Не обновлено	Не выбрано
Базы повреждены	Не выбрано
Базы сильно устарели	Не выбрано
Базы устарели	Не выбрано
Сетевая сессия добавлена в список недоверенных	Выбрано
Запуск приложения запрещен	Не выбрано
Только статистика: запуск приложения запрещен	Выбрано
Запуск приложения не обработан	Не выбрано
Обнаружено и запрещено недоверенное устройство	Выбрано
Только статистика: обнаружено недоверенное устройство	Выбрано
Подключение устройства не обработано	Выбрано
Обнаружен зараженный объект или объект другого типа	Выбрано
Объект обнаружен (Обнаружен объект, недоверенный в KSN)	Выбрано
Объект не вылечен	Не выбрано
Объект не помещен в резервное хранилище	Не выбрано
Обнаружена сетевая атака	Не выбрано

Portable Auditor

Portable Auditor – приложение, которое позволяет выполнять на устройствах поиск вредоносного ПО, поиск уязвимостей и аудит настроек безопасности, а также запись входящего и исходящего трафика. Portable Auditor запускается с подключаемого к устройству съемного диска и не требует установки на проверяемое устройство. Таким образом, вы можете использовать Portable Auditor для проверки устройств, на которых по каким-либо причинам не может быть установлено приложение Kaspersky Industrial CyberSecurity for Nodes:

- Изолированные устройства.
- Устройства, где установка Kaspersky Industrial CyberSecurity for Nodes невозможна из-за:
  - политик безопасности, действующих в вашей организации;
  - требований производителей устройств;
  - технических ограничений устройств и других факторов.
- Гостевые устройства.

Portable Auditor не оставляет на проверяемом устройстве следов своей работы: по умолчанию все файлы, создаваемые приложением во время работы, хранятся на съемном диске. При необходимости вы можете записать Portable Auditor на защищенный съемный диск. В таком случае файлы приложения располагаются на разделе, доступном только для чтения, что позволяет защитить их в случае подключения съемного диска с Portable Auditor к зараженному устройству. Результаты проверок сохраняются на защищенном разделе съемного диска, что позволяет обезопасить их от несанкционированного доступа.

Portable Auditor выполняет проверку устройств с помощью следующих задач:

- *Поиск вредоносного ПО*. По умолчанию Portable Auditor проверяет локальные жесткие диски, оперативную память устройства, а также объекты автозапуска на наличие вирусов и других программ, представляющих угрозу. При необходимости вы можете сформировать область проверки самостоятельно. При обнаружении зараженного объекта приложение выполняет действие, заданное в настройках задачи.
- *Аудит безопасности*. Portable Auditor выполняет поиск уязвимостей на устройствах, выполняет оценку соответствия устройств требованиям безопасности операционных систем и собирает **данные об их конфигурации.**

  Portable Auditor собирает следующие данные об устройстве:

  - запущенные службы;
  - установленные драйверы;
  - задачи с расписанием запуска;
  - установленные приложения и патчи;
  - имена сетевых ресурсов с общим доступом;
  - объекты автозапуска;
  - информация об устройстве (IP-адрес, DNS-имя);

- локальные пользователи и группы;
- аппаратное обеспечение.

- *Запись сетевого трафика*. Portable Auditor выполняет запись входящего и исходящего трафика проверяемого устройства в течение указанного времени в файл формата PcapNG.

С помощью одного экземпляра Portable Auditor вы можете выполнять проверку нескольких устройств подряд. В дальнейшем вы можете работать в Консоли Portable Auditor с результатами проверок каждого устройства по отдельности.

По результатам выполнения каждой задачи приложение формирует отдельный отчет, доступный для экспорта. Также вы можете просмотреть отчет о найденных угрозах в Консоли Portable Auditor.

Для управления Portable Auditor вы можете использовать Консоль Portable Auditor или командную строку.

Аппаратные и программные требования

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Создание Portable Auditor

Для создания Portable Auditor вам потребуется:

- Устройство с установленным приложением Kaspersky Industrial CyberSecurity for Nodes с действующей лицензией.
- Лицензия на Kaspersky Industrial CyberSecurity for Nodes Portable Auditor.
- Подключаемый по USB съемный диск размером 2 ГБ и более или поддерживаемый безопасный съемный диск:
  - Рутокен ЭЦП 2.0 Flash;
  - Рутокен ЭЦП 3.0 Flash.

Аппаратные требования к проверяемым устройствам

Вы можете проверять устройства, удовлетворяющие следующим минимальным требованиям:

- Процессор: 1 ГГц одноядерный, не ниже Celeron III или VIA C3.
- Оперативная память: 256 МБ.
- Объем свободного места на жестком диске: 2 ГБ.

Программные требования к проверяемым устройствам

Вы можете проверять устройства под управлением одной из следующих 32- или 64-разрядных операционных систем Microsoft Windows:

- Windows 2000 Professional SP4 32-разрядная.
- Windows XP Professional SP2 32-разрядная/64-разрядная.
- Windows XP Professional SP3 32-разрядная.
- Windows Vista SP2 32-разрядная/64-разрядная.
- Windows 7 SP1 Home/Pro/Enterprise/Ultimate 32-разрядная/64-разрядная.
- Windows 8 Pro/Enterprise 32-разрядная/64-разрядная.
- Windows 8.1 Pro/Enterprise 32-разрядная/64-разрядная.
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32-разрядная/64-разрядная.
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.

- Windows 11 25H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.
- Windows 11 26H2 Home / Pro / Pro for Workstations / Education / Enterprise 64-разрядная.

Серверные операционные системы:

- Windows Server 2003 SP1 Standard/Enterprise 32-разрядная/64-разрядная.
- Windows Server 2008 R2 SP1 Foundation/Standard/Enterprise 64-разрядная.
- Windows Server 2008 R2 SP2 Foundation/Standard/Enterprise 64-разрядная.
- Windows Server 2008 SP2 Standard/Enterprise 64-разрядная.
- Windows Small Business Server 2011 Essentials/Standard 64-разрядная.
- Windows MultiPoint Server 2011 64-разрядная.
- Windows Server 2012 Foundation/Essentials/Standard 64-разрядная.
- Windows Server 2012 R2 Foundation/Essentials/Standard 64-разрядная.
- Windows Server 2016 Essentials/Standard 64-разрядная.
- Windows Server 2019 RS5 Essentials/Standard 64-разрядная.
- Windows Server 2022 21H2 64-разрядная.
- Windows Server 2022 версия 20348.350 64-разрядная.
- Windows Server 2025 версия 26100.1742 64-разрядная.

Встраиваемые системы:

- Windows XP Embedded Service Pack 3 32-разрядная.
- Windows Embedded POSReady 7 32-разрядная/64-разрядная.
- Windows Embedded Standard 7 Service Pack 1 32-разрядная/64-разрядная.
- Windows Embedded 8 Standard 32-разрядная/64-разрядная.
- Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1507 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1607 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1803 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1809 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 1903 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 2004 32-разрядная/64-разрядная.

- Windows 10 IoT Enterprise Version 20H2 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 21H1 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 21H2 32-разрядная/64-разрядная.
- Windows 10 IoT Enterprise Version 22H2 32-разрядная/64-разрядная.
- Windows 11 IoT Enterprise Version 21H2 64-разрядная.
- Windows 11 IoT Enterprise Version 22H2 64-разрядная.
- Windows 11 IoT Enterprise Version 23H2 64-разрядная.
- Windows 11 IoT Enterprise Version 24H2 64-разрядная.
- Windows 11 IoT Enterprise Version 25H2 64-разрядная.

Ограничения функциональности Portable Auditor

Portable Auditor имеет следующие ограничения:

- На устройствах под управлением Windows 2000 Professional доступно только выполнение задачи *Поиск вредоносного ПО*. Задачи *Аудит безопасности* и *Запись сетевого трафика* не могут быть выполнены в связи с ограничениями операционной системы.
- На устройствах под управлением Windows XP Professional, Windows Vista, Windows Server 2003 и Windows XP Embedded в связи с ограничениями операционных систем не может быть выполнена задача *Запись сетевого трафика*.
- Создание Portable Auditor на защищенном съемном диске и запуск Portable Auditor с защищенного съемного диска недоступны на устройствах под управлением операционных систем Windows 2000 Professional, Windows XP Professional, Windows Vista, Windows Server 2003, Windows XP Embedded.

Создание Portable Auditor

Чтобы создать Portable Auditor, выполните следующие действия:

1. Подключите поддерживаемый съемный диск к устройству с установленным Kaspersky Industrial CyberSecurity for Nodes с действующей лицензией.

   Чтобы на компьютере под управлением операционной системы Windows Server 2022 съемный диск Рутокен отображался в списке подключенных съемных дисков, необходимо драйвер UMDF2 для подключаемых по USB картридеров заменить на драйвер WUDF.

2. В области уведомлений в контекстном меню значка приложения выберите **Диагностическое окно**.
3. В открывшемся Диагностическом окне нажмите на ссылку **Создать Portable Auditor**.

   Запустится мастер создания Portable Auditor. Следуйте его указаниям.

Для перехода к следующему шагу мастера нажимайте на кнопку **Далее >**.

Шаг 1. Импорт настроек

Если необходимо, импортируйте настройки Portable Auditor из ранее созданного XML-файла:

1. Нажмите на кнопку **Импорт настроек**.
2. В открывшемся окне выберите XML-файл с параметрами Portable Auditor.
3. Нажмите на кнопку **Открыть**.

   Параметры, загруженные из XML-файла, отобразятся на следующих шагах мастера. При необходимости вы можете их изменить.

Шаг 2. Добавление файла ключа

Для создания Portable Auditor необходима действительная лицензия на Kaspersky Industrial CyberSecurity for Nodes Portable Auditor.

Добавьте файл ключа:

1. Нажмите на кнопку **Выбрать лицензионный файл**.
2. В открывшемся окне выберите файл ключа для Portable Auditor.
3. Нажмите на кнопку **Открыть**.

   Информация о лицензии отобразится в текущем окне мастера.

Шаг 3. Выбор задач Portable Auditor

Выберите задачи, которые будет выполнять Portable Auditor после запуска на устройстве:

- **Проверять выбранные области антивирусными базами**. Если функция включена, Portable Auditor выполняет проверку выбранной области на наличие вирусов и других программ, представляющих угрозу. Portable Auditor применяет установленный по умолчанию уровень безопасности – **Информировать**. По умолчанию функция включена.

- **Записать трафик со всех сетевых интерфейсов**. Если функция включена, Portable Auditor записывает входящий и исходящий трафик проверяемого устройства в течение указанного времени. По умолчанию функция включена.

- **Выполнять аудит безопасности**. Если функция включена, Portable Auditor в зависимости от заданных параметров может выполнять поиск уязвимостей на устройстве, оценку безопасности устройства и соответствия стандартам операционной системы или собирать данные о конфигурации устройства с помощью правил, написанных на языках OVAL и XCCDF. По умолчанию функция включена.

При необходимости вы сможете настроить выбор задач, которые будут выполняться Portable Auditor, при запуске проверки.

Шаг 4. Настройка параметров задачи проверки

Этот шаг доступен, если на шаге 3 выбрано действие **Проверять выбранные области антивирусными базами**.

1. По умолчанию в область проверки добавлены следующие объекты: **Локальные жесткие диски**, **Системная память и процессы** и **Объекты автозапуска**.

   Вы можете исключить объект из области проверки, не удаляя его. Для этого снимите флажок слева от названия объекта. В дальнейшем вы сможете включить нужные объекты в область проверки в настройках задачи.

   Исключенные из области проверки объекты не добавляются в список исключений из проверки и могут попасть в область действия задачи *Поиск вредоносного ПО*. Например, если вы исключили папку на локальном жестком диске, но объект **Локальные жесткие диски** включен в область проверки, данная папка будет проверена задачей.

2. При необходимости вы можете добавить объекты в область проверки:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Область проверки** выберите тип объектов, который вы хотите добавить:

   - **Предопределенная область**, если вы хотите включить в область проверки одну из предопределенных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.
   - **Диск, папка или сетевой объект**, если вы хотите включить в область проверки отдельный диск или папку. Затем в открывшемся окне по кнопке **Обзор** выберите нужную область.

     При добавлении в область проверки локального жесткого диска Portable Auditor не проверяет подключенные к нему папки общего доступа. Если вы хотите включить в область проверки папки общего доступа, вам необходимо добавить их отдельно.

   - **Файл**, если вы хотите включить в область проверки отдельный файл. Затем в открывшемся окне по кнопке **Обзор** выберите нужный файл.

   c. Нажмите на кнопку **OK**.

   d. Повторите шаги a – c для каждого добавляемого объекта.

   Добавленные объекты по умолчанию включены в область проверки. Если необходимо, исключите объект из области проверки с помощью флажка слева от его названия.

   e. Если необходимо, удалите объект из списка с помощью кнопки **Удалить**.

3. Настройте параметры выполнения задачи:

   a. Нажмите на кнопку **Настройки проверки**.

   b. На вкладке **Общие** в блоке **Проверка объектов** выберите объекты, которые требуется включить в область проверки:

   - **Все объекты**. Portable Auditor проверяет все объекты.
   - **Объекты, проверяемые по формату**. Portable Auditor проверяет только потенциально заражаемые файлы на основании формата файла. Список форматов составляется специалистами "Лаборатории Касперского" и входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
   - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**. Portable Auditor проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений составляется специалистами "Лаборатории Касперского" и входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
   - **Объекты, проверяемые по указанному списку расширений**. Portable Auditor проверяет только потенциально заражаемые файлы на основании расширения файла. Вы можете самостоятельно сформировать список расширений, нажав на кнопку **Изменить**.

- **Проверять загрузочные секторы дисков**. Если флажок установлен, Portable Auditor проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства. По умолчанию флажок установлен.

- **Проверять альтернативные потоки NTFS**. Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS. Если флажок установлен, Portable Auditor выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом. Если флажок снят, приложение проверяет только обнаруженный объект, который считается возможно зараженным. По умолчанию флажок установлен.

c. В блоке **Проверка составных объектов** укажите типы составных объектов, которые вы хотите включить в область проверки:

- **Архивы**. Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

- **SFX-архивы**. Проверка самораспаковывающихся архивов.

- **Упакованные объекты**. Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX, ASPack и др.

- **Файлы почтовых форматов**. Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.

- **Почтовые базы**. Проверка файлов почтовых баз Microsoft Outlook и Microsoft Outlook Express. Этот вариант доступен, если установлен флажок **Файлы почтовых форматов**.

- **Вложенные OLE-объекты**. Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

d. Перейдите на вкладку **Дополнительно**.

e. В блоке **Общие настройки**.

- **Восстанавливать атрибуты файлов после проверки**. Если при проверке выполняется открытие файла, обновляется время последнего доступа к файлу. В результате архиваторы и облачные хранилища пересчитывают данные файлов, чтобы передать их в облако или в резервную копию. Чтобы избежать пересчета, можно восстановить время последнего доступа к файлу после завершения проверки. По умолчанию этот параметр выключен.

- **Ограничить потребление ресурсов процессора для задач проверки**. Этот параметр используется, чтобы избежать зависания компьютера во время проверки. Этот параметр может оказаться критичным для промышленных систем, основное программное обеспечение которых не должно зависать. По умолчанию этот параметр выключен.

- **Папка для временных файлов, создаваемых при проверке**. По умолчанию временные файлы сохраняются в папке kavscan\Results\<Имя проверяемого устройства>\<дата_время>\Temp, расположенной на съемном диске с Portable Auditor. При необходимости вы можете изменить папку для сохранения временных файлов. Например, если в процессе выполнения проверки на съемном диске заканчивается место, или проверка выполняется слишком долго из-за низкой скорости чтения/записи, вы можете настроить сохранение временных файлов в папку на проверяемом устройстве.

f. В блоке **Действия над обнаруженными объектами** выберите действие, которое Portable Auditor будет выполнять над зараженными и другими обнаруживаемыми объектами:

- **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет.

- **Информировать** (значение по умолчанию). Если выбран этот вариант действия, Portable Auditor не выполняет над зараженным или другим обнаруженным объектами никаких действий. Приложение только фиксирует соответствующее событие в отчете. Используйте этот вариант для быстрой проверки или, например, для систем, в которых нельзя допустить удаления промышленных программных модулей.

g. Если выбран вариант **Лечить. Удалять, если лечение невозможно**, настройте функцию **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением**. Если функция включена, Portable Auditor принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если приложение не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем). Если функция выключена, Portable Auditor не выполняет удаление родительского объекта. По умолчанию функция включена.

h. Перейдите на вкладку **Производительность**.

i. В блоке **Исключения** при необходимости добавьте исключения из области проверки:

- **Исключать файлы**. Используйте эту функцию, чтобы исключить файлы из области проверки и избежать их удаления в случае обнаружения. Вы можете указать полный путь или использовать маску. По умолчанию функция выключена.

- **Не проверять объекты по типу**. Используйте эту функцию, чтобы избежать обнаружения и дальнейшего удаления объектов определенного типа. Вы можете указать имя объекта или использовать маску. По умолчанию функция выключена.

j. Вы можете сократить время проверки и увеличить скорость работы Portable Auditor с помощью параметров в блоке **Дополнительные настройки**:

- **Останавливать проверку, если она длится более (сек.)**. Если функция включена и проверка объекта выполняется дольше указанного времени, Portable Auditor прерывает проверку объекта и продолжает проверку области. Используйте эту функцию, например, если при проверке больших файлов или сетевого окружения время работы Portable Auditor сильно увеличивается. По умолчанию функция включена. Значение по умолчанию – 60 сек.

- **Не проверять составные объекты размером более (МБ)**. Если функция включена, Portable Auditor исключает из области проверки объекты, размер которых больше заданного. По умолчанию функция включена. Значение по умолчанию – 100 МБ.

- **Использовать технологию iChecker**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Portable Auditor, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

4. Для создания исключений из проверки нажмите на кнопку **Настройки исключений**.

   Откроется окно **Исключения из проверки**.

Portable Auditor не проверяет папки и объекты из списка исключений, даже если они входят в область проверки. Например, если в список исключений добавлен жесткий диск, то Portable Auditor не будет проверять включенные в область проверки папки, расположенные на этом диске.

5. Создайте исключения из проверки:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Добавление исключения из проверки** выберите тип объектов, который вы хотите добавить:

   - **Предопределенная область**, если вы хотите включить в список исключений одну из предопределенных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.
   - **Диск, папка или сетевой объект**, если вы хотите включить в список исключений отдельный диск или папку. Затем в открывшемся окне по кнопке **Обзор** выберите нужную область.

     При добавлении в список исключений локального жесткого диска Portable Auditor не исключает из области проверки подключенные к нему папки общего доступа. Если вы хотите включить в список исключений папки общего доступа, вам необходимо добавить их отдельно.

   - **Файл**, если вы хотите включить в область проверки отдельный файл. Затем в открывшемся окне по кнопке **Обзор** выберите нужный файл.

   c. Нажмите на кнопку **OK**.

   d. Повторите шаги a–c для всех добавляемых исключений.

   e. Вы можете удалить добавленное исключение с помощью кнопки **Удалить**.

Шаг 5. Настройка параметров записи сетевого трафика

Этот шаг доступен, если на шаге 3 выбрано действие **Записать трафик со всех сетевых интерфейсов**.

Если необходимо, в поле **Записывать входящий и исходящий трафик проверяемого устройства в течение указанного времени (сек.)** измените период времени, в течение которого Portable Auditor будет записывать входящий и исходящий трафик проверяемого устройства. Значение по умолчанию – 30 сек.

Шаг 6. Настройка параметров аудита безопасности

Этот шаг доступен, если на шаге 3 выбрано действие **Выполнять аудит безопасности**.

Выберите источники OVAL- и XCCDF-правил, с помощью которых Portable Auditor будет выполнять аудит безопасности устройства:

- **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП**. Portable Auditor проверяет устройство на все уязвимости, описанные в OVAL-правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП. По умолчанию этот параметр выбран.

- **Правила для сбора данных конфигурации хоста**. Portable Auditor собирает данные о конфигурации устройства. По умолчанию этот параметр выбран.

- **Конфигурации безопасности и соответствий стандартам для операционных систем**. Portable Auditor проверяет параметры операционной системы устройства на соответствие стандартам безопасности. По умолчанию этот параметр выбран.

  Так как не во всех случаях заранее известно, какие операционные системы установлены на проверяемых устройства, по умолчанию выбраны конфигурации для всех поддерживаемых операционных систем. При необходимости вы можете исключить неиспользуемые конфигурации по кнопке **Выбрать конфигурации**.

  > База данных уязвимостей Kaspersky ICS CERT для АСУ ТП, Правила для сбора данных конфигурации хоста и Конфигурации безопасности и соответствий стандартам для операционных систем поставляются вместе с базами Portable Auditor. Поэтому, прежде чем запускать Portable Auditor с хотя бы одним из перечисленных источников правил, убедитесь, что базы Portable Auditor актуальны.

- **Пользовательская база правил**. Portable Auditor проверяет устройство на уязвимости, описанные в пользовательских OVAL- и XCCDF-правилах. Если вы выбрали данный параметр, необходимо загрузить ZIP-архив с базой правил.

Шаг 7. Выбор съемного диска

Выберите съемный диск, на котором будет создан Portable Auditor:

- **Съемный диск**. Подключенный по USB съемный диск. В раскрывающемся списке выберите съемный диск.

- **Безопасный съемный диск**. Подключенный по USB съемный диск, защищенный от чтения, копирования и записи паролем администратора. Если вы выбрали этот вариант, выберите защищенный съемный диск на следующем шаге мастера.

  > Вы не можете использовать один и тот же защищенный съемный диск одновременно для создания Portable Auditor и для безопасного копирования баз приложения.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes проверяет данные созданного Portable Auditor. Если вы планируете записать Portable Auditor с одинаковыми параметрами на несколько съемных дисков, проверка данных для первого Portable Auditor и обнаружение расхождений на ранней стадии позволят сэкономить время. Если необходимо, отключите данную функцию с помощью флажка **Проверить данные Portable Auditor после его создания**.

Шаг 8. Настройка параметров безопасного съемного диска

> Этот шаг доступен, если на шаге 7 выбран вариант **Безопасный съемный диск**.

Настройте параметры защищенного съемного диска:

1. Выберите подключенный защищенный съемный диск, на котором будет сформирован Portable Auditor.
2. В блоке **Настройки безопасности** в поле **Введите текущий PIN-код администратора** введите PIN-код, который был установлен на защищенном съемном диске для защиты его содержимого.

   Данный PIN-код будет запрашиваться в дальнейшем при выполнении всех операций с Portable Auditor.

3. Если необходимо, измените текущий PIN-код администратора:

   a. Установите флажок **Сменить текущий PIN-код (допускаются только цифры и латинские символы)**.

   b. Введите новый PIN-код в одноименном поле.

   c. Повторите новый PIN-код.

Шаг 9. Запись Portable Auditor на съемный диск

На данном шаге вы можете просмотреть все настроенные параметры Portable Auditor перед началом его создания. Если необходимо, вы можете экспортировать данные параметры в XML-файл по кнопке **Экспортировать**.

Нажмите на кнопку **Завершить**, чтобы создать Portable Auditor с указанными параметрами.

Не рекомендуется подключать к одному устройству два съемных дисках Рутокен и одновременно запускать безопасное копирование баз приложения и создание Portable Auditor. В таком случае выполнение этих задач может завершаться с ошибкой.

Portable Auditor будет записан на выбранном съемном диске. На съемном диске появится папка kavscan, содержащая в себе файлы и папки, необходимые для работы Portable Auditor.

Если на съемном диске уже есть Portable Auditor, мастер перезаписывает все файлы существующего Portable Auditor в папке kavscan. Если вы решите прервать запись, мастер прекратит запись без отката изменений.

После завершения записи мастер предложит создать следующий Portable Auditor.

Чтобы избежать повреждения данных на съемном диске, используйте функцию безопасного извлечения устройств при работе с Portable Auditor.

Также вы можете создать Portable Auditor через интерфейс командной строки.

Обновление Portable Auditor

Для обновления версии Portable Auditor вам необходимо подключить съемный диск к устройству, на котором установлена актуальная версия Kaspersky Industrial CyberSecurity for Nodes, и заново создать Portable Auditor.

При обновлении версии Portable Auditor результаты проверок, хранящиеся на съемном диске, не сохраняются.

Работа с Консолью Portable Auditor

Запуск Консоли Portable Auditor недоступен, если на съемном диске с Portable Auditor осталось менее 200 КБ свободного места.

Чтобы запустить Консоль Portable Auditor на проверяемом устройстве, выполните следующие действия:

1. Подключите съемным диск с Portable Auditor к проверяемому устройству.
2. Перейдите в папку kavscan на съемном диске с Portable Auditor.
3. Запустите исполняемый файл kavscan_ui.exe.

   Для запуска задач Portable Auditor пользователь, от имени которого выполняется запуск приложения, должен обладать правами администратора на проверяемом устройстве.

4. Если Portable Auditor записан на защищенный съемный диск, введите PIN-код.

   Откроется окно Консоли Portable Auditor.

Вы можете запустить только один экземпляр Консоли Portable Auditor на проверяемом устройстве.

После запуска Консоли Portable Auditor открывается раздел **Панель управления**. В данном разделе доступна следующая информация о приложении:

- В блоке **Задачи** вы можете просмотреть текущий статус выполнения задач Portable Auditor.
- В блоке **Статистика** отображается статистика использования данного экземпляра Portable Auditor за все время с момента его создания:
  - **Последний запуск** – дата завершения последней запущенной задачи.
  - **Проверено устройств** – количество уникальных устройств, на которых запускалась хотя бы одна задача.

- **Устройства с обнаруженными угрозами** – количество проверенных устройств, на которых обнаружены угрозы.
- **Задачи поиска вредоносного ПО** – общее количество запущенных задач *Поиск вредоносного ПО*.
- **Задачи аудита безопасности** – общее количество запущенных задач *Аудит безопасности*.
- **Задачи записи сетевого трафика** – общее количество запущенных задач *Запись сетевого трафика*.

- В блоке **Место на диске** отображается информация о доступном и использованном пространстве на съемном диске.

Чтобы удалить со съемного диска файлы, созданные в процессе работы Portable Auditor, выполните следующие действия:

a. В блоке **Место на диске** нажмите на ссылку **Освободить место на диске**.

   В открывшемся окне вы можете просмотреть детальную информацию о том, какой объем памяти на съемном диске (в МБ) занимают отчеты о выполнении задач Portable Auditor, файлы дампов и файлы трассировки.

b. Нажмите кнопку **Удалить** в соответствующем блоке и подтвердите действие.

c. Для удаления всех файлов нажмите на кнопку **Удалить все** и подтвердите действие.

Portable Auditor удалит выбранные файлы со съемного диска.

Также вы можете удалить файлы с отчетами о выполнении задач для отдельных устройств в разделе **Отчеты**.

Чтобы завершить работу Консоли Portable Auditor,

в контекстном меню значка Portable Auditor в области уведомлений выберите **Выход**.

При закрытии окна Консоли Portable Auditor приложение продолжит работу в фоновом режиме.

Чтобы избежать повреждения данных на съемном диске, используйте функцию безопасного извлечения устройств при работе с Portable Auditor.

Проверка устройств

Запуск задач недоступен, если на съемном диске с Portable Auditor осталось менее 100 МБ свободного места.

Чтобы запустить проверку устройства с помощью Portable Auditor, выполните следующие действия:

1. Запустите Консоль Portable Auditor на проверяемом устройстве.

   Для запуска задач Portable Auditor пользователь, от имени которого выполняется запуск приложения, должен обладать правами администратора на проверяемом устройстве.

2. Перейдите в раздел **Задачи**.

   В открывшемся окне вы можете просмотреть текущий статус каждой задачи, дату и время ее последнего запуска, а также выбранный способ задания настроек – **По умолчанию** или **Пользовательские**.

   Настройками задач по умолчанию являются настройки, заданные при создания Portable Auditor.

3. Для запуска задач с текущими настройками выберите с помощью флажков те задачи, которые вы хотите запустить, и нажмите на кнопку **Запуск выбранных задач**. По умолчанию выбраны задачи, запуск которых был настроен при создании Portable Auditor.

   Также вы можете запустить одну задачу с помощью кнопки **Запустить** в соответствующем блоке.

4. Чтобы задать пользовательские настройки задачи нажмите на кнопку **Настройки** в соответствующем блоке. Для восстановления настроек по умолчанию нажмите на ссылку **Восстановить настройки по умолчанию**.

   При необходимости вы можете экспортировать и импортировать настройки задач.

5. После запуска задач приложение отобразит на экране текущий прогресс их выполнения. При запуске нескольких задач одновременно Portable Auditor будет выполнять задачи последовательно друг за другом. Вы можете остановить выполнение задач с помощью кнопки **Отмена**.

После завершения выполнения задач Portable Auditor сохранит файлы с отчетами на съемном диске и отобразит информацию о результате в поле **Статус**. Вы можете перейти к просмотру результатов проверки или завершить работу с Portable Auditor на текущем устройстве.

Чтобы избежать повреждения данных на съемном диске, используйте функцию безопасного извлечения устройств при работе с Portable Auditor.

Также вы можете запускать проверку устройств из командной строки.

Настройка задачи Поиск вредоносного ПО

Чтобы настроить параметры задачи Поиск вредоносного ПО, выполните следующие действия:

1. В блоке **Поиск вредоносного ПО** нажмите на кнопку **Настройки**.

   Откроется окно **Настройки проверки**.

2. В поле **Настройки** выберите вариант **Пользовательские**.

3. На вкладке **Область проверки** сформируйте область проверки. По умолчанию область проверки содержит объекты, включенные при создании Portable Auditor.

Вы можете исключить объект из области проверки, не удаляя его. Для этого снимите флажок слева от названия объекта.

Исключенные из области проверки объекты не добавляются в список исключений из проверки и могут попасть в область действия задачи *Поиск вредоносного ПО*. Например, если вы исключили папку на локальном жестком диске, но объект **Локальные жесткие диски** включен в область проверки, данная папка будет проверена задачей.

4. При необходимости вы можете добавить объекты в область проверки:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне **Добавление области проверки** выберите область проверки, отдельный диск, папку или сетевой объект.

      При добавлении в область проверки локального жесткого диска Portable Auditor не проверяет подключенные к нему папки общего доступа. Если вы хотите включить в область проверки папки общего доступа, вам необходимо добавить их отдельно.

   c. Нажмите на кнопку **OK**.

      Добавленный объект отобразится в списке.

   d. Повторите шаги a–d для всех добавляемых объектов.

      Добавленные объекты по умолчанию включены в область проверки. Если необходимо, исключите объект из области проверки с помощью флажка слева от его названия.

   e. Если необходимо, удалите объект из области проверки с помощью кнопки **Удалить**.

   f. При необходимости вы можете изменить существующий объект области проверки, нажав на кнопку **Изменить**.

5. Для каждого объекта области проверки вы можете отдельно настроить параметры выполнения задачи *Поиск вредоносного ПО*:

   a. Выделите объект области проверки, для которого вы хотите настроить параметры задачи, и нажмите на кнопку **Настройки области**.

   b. Откроется окно **Настройки области** на вкладке **Общие**.

   c. В блоке **Действия над обнаруженными объектами** выберите действие, которое Portable Auditor будет выполнять над зараженными и другими обнаруживаемыми объектами:

      - **Лечить. Удалять, если лечение невозможно**. Если выбран этот вариант действия, то приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то приложение их удаляет.

      - **Информировать** (значение по умолчанию). Если выбран этот вариант действия, Portable Auditor не выполняет над зараженным или другим обнаруженным объектами никаких действий. Приложение только фиксирует соответствующее событие в отчете. Используйте этот вариант для быстрой проверки или, например, для систем, в которых нельзя допустить удаления промышленных программных модулей.

d. В блоке **Проверка объектов** выберите объекты, которые требуется включить в область проверки:

- **Все объекты**. Portable Auditor проверяет все объекты.
- **Объекты, проверяемые по формату**. Portable Auditor проверяет только потенциально заражаемые файлы на основании формата файла. Список форматов составляется специалистами "Лаборатории Касперского" и входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
- **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**. Portable Auditor проверяет только потенциально заражаемые файлы на основании расширения файла. Список расширений составляется специалистами "Лаборатории Касперского" и входит в состав баз Kaspersky Industrial CyberSecurity for Nodes.
- **Объекты, проверяемые по указанному списку расширений**. Portable Auditor проверяет только потенциально заражаемые файлы на основании расширения файла. Вы можете самостоятельно сформировать список расширений, нажав на кнопку **Обзор**.

e. В блоке **Проверка составных объектов** укажите типы составных объектов, которые вы хотите включить в область проверки:

- **Архивы**. Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.
- **SFX-архивы**. Проверка самораспаковывающихся архивов.
- **Упакованные объекты**. Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX, ASPack и др.
- **Файлы почтовых форматов**. Проверка файлов почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express.
- **Почтовые базы**. Проверка файлов почтовых баз Microsoft Outlook и Microsoft Outlook Express. Этот вариант доступен, если установлен флажок **Файлы почтовых форматов**.
- **Вложенные OLE-объекты**. Проверка встроенных в файлы объектов (таких как макросы Microsoft Word или вложения в сообщения электронной почты).

f. Если выбран вариант **Лечить. Удалять, если лечение невозможно**, настройте функцию **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен приложением**. Если функция включена, Portable Auditor принудительно удаляет весь родительский составной объект при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление родительского объекта со всем его содержимым выполняется, если приложение не может удалить только вложенный обнаруженный объект (например, если родительский объект неизменяем). Если функция выключена, Portable Auditor не выполняет удаление родительского объекта. По умолчанию функция включена.

g. Перейдите на вкладку **Дополнительно**.

h. Вы можете сократить время проверки и увеличить скорость работы Portable Auditor с помощью параметров в блоке **Оптимизация проверки**:

- **Останавливать проверку, если она длится более (сек.)**. Если функция включена и проверка объекта выполняется дольше указанного времени, Portable Auditor прерывает проверку объекта и продолжает проверку области. Используйте эту функцию, например, если при проверке больших файлов или сетевого окружения время работы Portable Auditor сильно увеличивается. По умолчанию функция включена. Допустимые значения: от 1 до 6000 сек. Значение по умолчанию – 60 сек.

- **Не проверять составные объекты размером более (МБ)**. Если функция включена, Portable Auditor исключает из области проверки объекты, размер которых больше заданного. По умолчанию функция включена. Допустимые значения: от 1 до 10 000 МБ. Значение по умолчанию – 100 МБ.

- **Использовать технологию iChecker**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Portable Auditor, дату предыдущей проверки файла, а также изменение настроек проверки. Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной приложению структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

i. В блоке **Исключения из проверки** при необходимости добавьте исключения из области проверки:

- **Исключать файлы**. Используйте эту функцию, чтобы исключить файлы из области проверки и избежать их удаления в случае обнаружения. Вы можете указать полный путь к файлу или использовать маску. По умолчанию функция выключена.

- **Не проверять объекты по типу**. Используйте эту функцию, чтобы избежать обнаружения и дальнейшего удаления объектов определенного типа. Вы можете указать имя объекта или использовать маску. По умолчанию функция выключена.

6. При необходимости вы можете переносить пользовательские настройки задачи с одного объекта области проверки на другой:

a. Выберите область проверки, настройки которой вы хотите перенести.

b. Нажмите на кнопку **Дублировать настройки**.

c. В открывшемся окне выберите области проверки, на которые будут распространены настройки.

d. Нажмите на кнопку **ОК**.

Настройки задачи будут перенесены на выбранные области.

7. Для создания исключений из проверки перейдите на вкладку **Исключения**.

Portable Auditor не проверяет папки и объекты из списка исключений, даже если они входят в область проверки. Например, если в список исключений добавлен жесткий диск, то Portable Auditor не будет проверять включенные в область проверки папки, расположенные на этом диске.

8. Создайте исключения из проверки:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне выберите способ задания исключения:

   - **Исключить категорию**. Используйте этот вариант, чтобы избежать обнаружения и дальнейшего удаления объектов определенного типа:

   - **Указать путь к объекту**. Используйте этот вариант, чтобы исключить файлы из области проверки и избежать их удаления в случае обнаружения. Вы можете указать полный путь к файлу или использовать маску.

   c. Нажмите на кнопку **OK**.

   d. Повторите шаги a–c для всех добавляемых исключений.

9. Перейдите на вкладку **Общие настройки**.

10. В блоке **Проверка объектов** задайте типы объектов, которые требуется включить в область проверки:

    - **Проверять загрузочные секторы дисков**. Если функция включена, Portable Auditor проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства. По умолчанию функция включена.

    - **Проверять альтернативные потоки NTFS**. Проверка дополнительных потоков файлов и папок на дисках с файловой системой NTFS. Если функция включена, Portable Auditor выполняет проверку возможно зараженного объекта и всех потоков NTFS, связанных с этим объектом. Если функция включена, приложение проверяет только обнаруженный объект, который считается возможно зараженным. По умолчанию функция включена.

11. В блоке **Потребление ресурсов компьютера** при необходимости включите функцию **Ограничить потребление ресурсов процессора для задач проверки**. Если функция включена, Portable Auditor ограничивает использование процессора проверяемого устройства в задачах проверки. По умолчанию функция выключена.

    Если функция включена, настройте параметр **Максимальное значение**. Диапазон доступных значений: 10–100%. Значение по умолчанию – 50%.

Настройка задачи Аудит безопасности

Чтобы настроить параметры задачи Аудит безопасности, выполните следующие действия:

1. В блоке **Аудит безопасности** нажмите на кнопку **Настройки**.

   Откроется окно **Настройки аудита безопасности**.

2. В поле **Настройки** выберите вариант **Пользовательские**.

3. Выберите источники OVAL- и XCCDF-правил, с помощью которых Portable Auditor будет выполнять аудит безопасности устройства:

   - **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП**. Portable Auditor проверяет устройство на все уязвимости, описанные в OVAL-правилах базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП. По умолчанию этот параметр выбран.

   - **Правила для сбора данных конфигурации хоста**. Portable Auditor собирает данные о конфигурации устройства. По умолчанию этот параметр выбран.

   - **Конфигурации безопасности и соответствий стандартам для операционных систем**. Portable Auditor проверяет параметры операционной системы устройства на соответствие стандартам безопасности. По умолчанию этот параметр выбран.

     Так как не во всех случаях заранее известно, какие операционные системы установлены на проверяемых устройства, по умолчанию выбраны конфигурации для всех поддерживаемых операционных систем. При необходимости вы можете исключить неиспользуемые конфигурации по кнопке **Выбрать конфигурации**.

     > База данных уязвимостей Kaspersky ICS CERT для АСУ ТП, Правила для сбора данных конфигурации хоста и Конфигурации безопасности и соответствий стандартам для операционных систем поставляются вместе с базами Portable Auditor. Поэтому, прежде чем запускать Portable Auditor с хотя бы одним из перечисленных источников правил, убедитесь, что базы Portable Auditor актуальны.

   - **Пользовательская база правил**. Portable Auditor проверяет устройство на уязвимости, описанные в пользовательских OVAL- и XCCDF-правилах.

4. Если выбран вариант **Пользовательская база правил**, загрузите базы с правилами:

   a. Нажмите на кнопку **Настроить**.

   b. В открывшемся окне укажите ZIP-архив с базой правил.

   c. Вы можете загрузить только один архив, содержащий XML-файлы с OVAL- и XCCDF-правилами.

   d. Нажмите на кнопку **Открыть**.

5. Нажмите на кнопку **ОК** для сохранения внесенных изменений.

Настройка задачи Запись сетевого трафика

Чтобы настроить параметры задачи Запись сетевого трафика, выполните следующие действия:

1. В блоке **Запись сетевого трафика** нажмите на кнопку **Настройки**.

   Откроется окно **Настройки записи сетевого трафика**.

2. В поле **Настройки** выберите вариант **Пользовательские**.

3. В поле **Записывать входящий и исходящий трафик проверяемого устройства в течение указанного времени (сек.)** измените период времени, в течение которого Portable Auditor будет записывать входящий и исходящий трафик проверяемого устройства. Диапазон доступных значений: от 1 до 1800 сек. Значение по умолчанию – 30 сек.

4. Нажмите на кнопку **OK** для сохранения внесенных изменений.

Экспорт и импорт настроек задач

Вы можете использовать функцию экспорта/импорта настроек для переноса настроек задач с одного экземпляра Portable Auditor на другой.

Чтобы экспортировать настройки задачи в конфигурационный файл, выполните следующие действия:

1. В разделе **Задачи** нажмите на ссылку **Экспортировать настройки**.

2. В открывшемся окне нажмите на кнопку **Обзор**.

3. Введите имя XML-файла, в который приложение экспортирует настройки задач, а также выберите папку, в которой будет создан этот файл.

4. Нажмите на кнопку **Экспортировать**.

   Portable Auditor экспортирует в XML-файл пользовательские настройки задач, настройки задач по умолчанию, а также пользовательские OVAL- или XCCDF-правила (в случае их использования).

Чтобы импортировать настройки задачи из конфигурационного файла, выполните следующие действия:

1. Перейдите в раздел **Задачи**.

2. Нажмите на ссылку **Импортировать настройки**.

3. В открывшемся окне нажмите на кнопку **Обзор** и выберите XML-файл с настройками Portable Auditor.

4. Нажмите на кнопку **Импортировать**.

   Настройки задач из файла заменят пользовательские настройки задач Portable Auditor.

Просмотр информации о лицензии

Чтобы просмотреть информацию о действующей лицензии,

в Консоли Portable Auditor перейдите в раздел **Лицензирование**.

В панели результатов отобразится общая информация о действующей лицензии (см. таблицу ниже).

Поле	Описание
Статус ключа	Статус ключа и тип лицензии
Лицензионный ключ	Номер ключа, с помощью которого вы активировали Portable Auditor.
Осталось дней	Количество дней, оставшихся до даты окончания срока действия лицензии.
Дата окончания срока действия	Дата и время окончания срока действия лицензии.
Дата активации	Дата активации приложения.

Дополнительно для уведомления об окончании срока действия в разделе **Лицензирование** используется цветовая индикация:

- *Красный* – менее 10 дней до окончания срока действия лицензии.
- *Желтый* – от 11 до 30 дней до окончания срока действия лицензии.
- *Зеленый* – более 30 дней до окончания срока действия лицензии.

После окончания срока действия лицензии вам необходимо заново создать Portable Auditor с новым файлом ключа.

Просмотр результатов проверки

Чтобы просмотреть результаты выполнения задач Portable Auditor, выполните следующие действия:

1. Перейдите в раздел **Отчеты**.

   В панели результатов отобразится таблица со списком устройств, для которых Portable Auditor хранит результаты выполнения задач.

2. Вы можете экспортировать результаты проверки:

   a. Выберите одно или несколько устройств, для которых вы хотите экспортировать результаты проверки. Если вы хотите выбрать несколько устройств, выделите их, удерживая нажатой клавишу **CTRL** или **SHIFT**. Для выбора всех устройств нажмите на клавишу **Выбрать все**.

   b. Нажмите на кнопку **Экспорт** и выберите папку для экспорта.

      Portable Auditor экспортирует содержимое папки kavscan\Results\<Имя проверяемого устройства> в выбранную папку.

3. После экспорта вы можете удалить файлы с результатами проверки со съемного диска с помощью кнопки **Очистить**.

4. Для просмотра отчетов о выполнении задач выберите нужное устройство и нажмите на кнопку **Просмотр**.

5. В открывшемся окне нажмите на название задачи, для которой вы хотите просмотреть отчет.

Если выполнение задачи было завершено успешно, в правой части окна отобразится отчет:

- Для задачи *Поиск вредоносного ПО* отображается таблица с информацией об обнаруженных угрозах:
  - **Имя объекта** – имя зараженного файла.
  - **Название угрозы** – название угрозы по классификации Вирусной энциклопедии "Лаборатории Касперского".
  - **Путь к объекту** – полный путь к обнаруженному объекту на проверяемом устройстве.
  - **Время проверки** – время обнаружения объекта.
  - **Причина** – причина, по которой обнаруженный объект не был обнаружен приложением.

  Вы можете экспортировать отчет задачи с помощью кнопки **Экспорт отчета задачи поиска вредоносного ПО**. Portable Auditor экспортирует ZIP-архив, содержащий отчет об обнаруженных угрозах, в указанную папку.
- Для задач *Аудит безопасности* и *Запись сетевого трафика* просмотр отчетов в Консоли Portable Auditor недоступен. Для просмотра результатов выполнения этих задач вам необходимо выполнить экспорт отчетов с помощью кнопки **Экспорт**.

О составе и хранении файлов, содержащих результаты работы Portable Auditor

Результаты работы Portable Auditor, записанного на защищенный съемный диск, скрыты. Для получения доступа к результатам работы такого Portable Auditor необходимо их экспортировать на любой другой доступный носитель в Консоли Portable Auditor или через командную строку.

После завершения проверки в папке kavscan создается папка Results. Она имеет следующую структуру:

- <Имя проверяемого устройства> – папка, названная именем проверяемого устройства и содержащая следующие вложенные папки:
  - <дата_время> – папка, название которой содержит дату и время проверки устройства в формате ГГГГ-ММ-ДД_ЧЧ-ММ-СС. В зависимости от параметров выполненной проверки может содержать следующие вложенные папки:
    - Backup – папка, содержащая резервные копии исходных файлов, которые приложение пыталось вылечить, если задача проверки была запущена в режиме **Лечить. Удалять, если лечение невозможно**. В имени каждого файла содержится путь, по которому файл находился на проверяемом устройстве. Каждый файл упакован в защищенный паролем ZIP-архив. Пароль для доступа к этим файлам: `infected`.
    - Detects – папка, содержащая служебную информацию об обнаружениях. Содержимое папки необходимо для вывода деталей алерта в Kaspersky Industrial CyberSecurity for Networks.
    - Oval – папка, содержащая для каждого источника правил аудита безопасности ZIP-архив с отчетом в формате XML и HTML. Папка создана, если выполнялась Аудит безопасности.

- Network – папка, содержащая дампы входящего и исходящего сетевого трафика устройства. Папка создана, если выполнялась задача *Запись сетевого трафика*.
- Report – папка, содержащая файл report.txt с отчетом о работе Portable Auditor.
- Results – папка, содержащая архив results_<имя проверяемого устройства>_<дата_время проверки>.zip с артефактами, содержащими результаты выполненного сканирования. Архив необходим для импорта результатов сканирования в Kaspersky Industrial CyberSecurity for Networks.
- Temp – папка, содержащая временные данные, создаваемые во время сканирования.

Просмотр общего отчета о работе Portable Auditor

После завершения выполнения задач в папке kavscan\Results\<Имя проверяемого устройства>\<дата_время>\Reports создается файл отчета report.txt.

Отчет состоит из следующих разделов:

- **Заголовок**
  - Версия Portable Auditor.
  - Дата и время запуска проверки.
  - Команда, с помощью которой была запущена проверка.
  - Имя устройства, с которого была запущена проверка.
  - Операционная система проверяемого устройства.
  - Сетевой интерфейс: имя, MAC-адрес, IP-адрес.
  - Учетная запись пользователя, от имени которого была запущена проверка.
  - Дата и время создания баз программы.
  - Дата и время начала выполнения задачи *Аудит безопасности*.
  - Источники правил, с помощью которых Portable Auditor будет выполнять аудит безопасности устройства.
  - Дата и время окончания выполнения задачи *Аудит безопасности*.
  - Дата и время начала выполнения задачи *Поиск вредоносного ПО*.
  - Область проверки.
- **Список событий**

  Список событий содержит подробную информацию о проверке для режимов `/type=full` и `/type=critical`. Он содержит имя проверяемого устройства и действие, выполняемое с обнаруженными объектами.
  Для режима `/type=short` список событий не формируется.

- **Статистика**

  Раздел отчета содержит данные о дате и времени завершения проверки и количестве объектов в следующих категориях:

  - Обнаружено.
  - Зараженных и других обнаруживаемых объектов.
  - Не вылечено объектов.
  - Не проверено объектов.
  - Ошибок обработки.
  - Вылечено объектов.
  - Удалено объектов.
  - Защищенных паролем объектов.
  - Обработано объектов.
  - Дата и время завершения проверки.

Чтобы настроить детализацию общего отчета о проверке, выполните следующие действия, выполните следующие действия:

1. В Консоли Portable Auditor перейдите в разделе **Диагностика сбоев**.
2. В блоке **Тип отчета** выберите нужный уровень детализации:
   - **Полный** – полный отчет о проверке со всеми типами событий (значение по умолчанию).
   - **Критический** – отчет о проверке содержит только критические события.
   - **Краткий** – отчет о проверке содержит общую статистику и не содержит данных о событиях.

Обновление баз Portable Auditor

Вы можете просмотреть дату и время выпуска баз приложения в разделе **Обновление** Консоли Portable Auditor.

Чтобы обновить базы Portable Auditor, выполните следующие действия:

1. Загрузите обновленные базы приложения одним из следующих способов:
   - С помощью хранилищ точек распространения.

     На устройстве с установленным приложением Kaspersky Industrial CyberSecurity for Nodes создайте или настройте существующую задачу *Загрузка обновлений в хранилища точек распространения* для устройства или группы устройств. Подробную информацию о настройке задачи см. в справке Kaspersky Security Center. Далее запустите задачу.

Версия установленной на устройстве Kaspersky Industrial CyberSecurity for Nodes должна быть не ниже версии Kaspersky Industrial CyberSecurity for Nodes, с помощью которой был записан Portable Auditor. В противном случае обновленные базы приложения могут не содержать некоторые файлы, необходимых для полноценной работы Portable Auditor.

- С помощью Kaspersky Updater Utility.

  Загрузите актуальные базы приложения в папку на устройстве с помощью утилиты Kaspersky Updater Utility. Подробную информацию о работе с Kaspersky Update Utility см. в Базе знаний "Лаборатории Касперского".

2. Подключите съемный диск, на котором записан Portable Auditor, к устройству с обновленными базами приложения.
3. Запустите Консоль Portable Auditor.
4. Перейдите в раздел **Обновление**.
5. Нажмите на кнопку **Выбрать источник и обновить**.
6. В открывшемся окне укажите папку с загруженными на шаге 1 базами программы.

Portable Auditor обновит базы приложения в папке Bases и выполнит проверку баз. Вы можете просмотреть статус выполнения задачи обновления в поле **Статус**. Дополнительно для уведомления о статусе задачи обновления используется цветовая индикация:

- *Красный* – обновление завершено с ошибкой.
- *Зеленый* – обновление выполнено успешно или обновление не запускалось с момента создания Portable Auditor.

Настройка трассировки работы Portable Auditor и записи дампов памяти

Чтобы настроить трассировку работы Portable Auditor и запись дампов памяти, выполните следующие действия:

1. В Консоли Portable Auditor перейдите в раздел **Диагностика сбоев**.
2. В блоке **Настройки дампов** установите флажок **Создавать во время сбоя файл дампа**, чтобы включить запись дампов. По умолчанию запись дампов выключена.

   Portable Auditor сохраняет файлы дампов Консоли Portable Auditor в папку kavscan\Crash Dumps\Application Console Crash Dumps, а файлы дампов приложения – в папку kavscan\Crash Dumps\Application Crash Dumps.
3. В блоке **Настройки трассировок** установите флажок **Включить трассировку**, чтобы включить трассировку работы Portable Auditor. По умолчанию трассировка работы Portable Auditor выключена.

4. При необходимости измените уровень детализации отладочной информации:

   - **Обычный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждениях, а также информация о работе Portable Auditor в нормальном режиме (значение по умолчанию).
   - **Важный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждения, а также дополнительная информация.
   - **Детальный** – в файле трассировки сохраняется вся информация о работе Portable Auditor.

   Portable Auditor сохраняет файлы трассировки Консоли Portable Auditor в папку kavscan\Traces\Application Console Traces, а файлы трассировки приложения – в папку kavscan\Traces\Application Traces.

5. Для экспорта файлов дампов и файлов трассировки нажмите на кнопку **Экспортировать файлы дампов и трассировки** и в открывшемся окне выберите папку для экспорта.

Работа с Portable Auditor через командную строку

Чтобы запустить Portable Auditor, выполните следующие действия:

1. Подключите съемный диск, на который записан Portable Auditor, к устройству, которое вы хотите проверить.
2. На устройстве запустите интерпретатор командной строки с правами локального администратора.
3. С помощью команды `cd /d` (например, `cd /d "E:\kavscan"`, где `E` – наименование съемного диска) перейдите в папку, в которой находится файл kavscan.exe.
4. Выполните одно из следующих действий:

   - Если вы хотите запустить Portable Auditor с параметрами, указанными перед записью Portable Auditor, выполните команду:

     ```
     KAVSCAN SCAN
     ```

   - Если вы хотите запустить Portable Auditor с параметрами, отличными от указанных перед записью Portable Auditor, выполните команду:

     ```
     KAVSCAN SCAN [/AV] [/TRAFFIC=<duration in seconds>] [/OVAL=<full path to ZIP archive with security audit rules>] [/MYCOMPUTER] [/FIXED] [/REMOVABLE] [/REMOTE] [/SHARED] [/MEMORY] [/STARTUP] [/DRIVE=<disk>] [/FOLDER=<full path to folder to scan>] [/FILE=<full path to file including name>] [/CURE=<yes|no>] [/TRACE=<important|normal|detailed>] [/DUMP] [/REPORT=<full|critical|short>] [/SETTINGS=<full path to file with custom settings>]
     ```

     Если в командной строке вместо диалога отображаются символы `?`, то это указывает на несовпадение кодировок операционной системы и Kaspersky Industrial CyberSecurity for Nodes. Для корректного отображения диалога вам нужно в параметрах операционной системы выбрать язык приложений, не поддерживающих Юникод. Необходимо выбрать язык, соответствующий Kaspersky Industrial CyberSecurity for Nodes.

Для просмотра справки по командам, выполните команду `KAVSCAN HELP`.

Все ключи команды `KAVSCAN SCAN`, за исключением `/CURE`, `/TRACE`, `/DUMP`, `/REPORT` переопределяют параметры Portable Auditor, которые были заданы перед его созданием. Например, если ключи команды `KAVSCAN SCAN /AV`, `/TRAFFIC` и `/OVAL` указаны в любой комбинации или по отдельности, то Portable Auditor выполнит только те действия, которые определяют указанные ключи, даже если в параметрах Portable Auditor, указанных перед его созданием, включены все действия.

5. Если вы запускаете Portable Auditor с безопасного съемного диска, введите пароль администратора, который вы указывали в параметрах Portable Auditor перед его созданием.

Параметры команд для запуска Portable Auditor

Параметр	Описание
`/AV`	Запускает проверку на вирусы и другие программы, представляющие угрозу.
`/TRAFFIC=<duration in seconds>`	Запись входящего и исходящего трафика проверяемого устройства в течение указанного времени. Допустимые значения: от 1 до 1800 секунд. Если продолжительность записи сетевого трафика не указана в команде, применяется значение, указанное в параметрах Portable Auditor при его создании. Если в параметрах Portable Auditor значение не указано, применяется значение по умолчанию – 30 секунд.
`/OVAL=<full path to the ZIP archive containing security audit rules>`	Запускает выполнение задачи аудита безопасности на основе правил в указанном ZIP-архиве. ZIP-архив должен содержать XML-файл с правилами, написанными на языке OVAL, или набор XML-файлов с правилами, написанными на языке XCCDF. Полный путь к ZIP-архиву указывается вместе с именем архива. Если полный путь к ZIP-архиву с правилами не указан, Portable Auditor выполняет аудит безопасности в соответствии с параметрами, заданными перед его созданием.
`/MYCOMPUTER`	Проверка всего компьютера.
`/FIXED`	Проверка всех локальных жестких дисков.
`/REMOVABLE`	Проверка всех съемных дисков.
`/REMOTE`	Проверка всех удаленных дисков.
`/SHARED`	Проверка общих папок.
`/MEMORY`	Проверка всех процессов памяти.
`/STARTUP`	Проверка объектов автозапуска.
`/DRIVE=<drive>`	Проверка всех загрузочных секторов и файлов на указанном диске.
`/FOLDER=<full path to the folder to be scanned>`	Проверка указанной папки. В качестве значения этого параметра нельзя использовать шаблон метки папки.
`/FILE=<full path to the file including its name>`	Проверка указанного файла. Полный путь к файлу указывается вместе с именем файла.
`/CURE=<yes|no>`	Определяет режим проверки. Доступны следующие значения: • `yes` – проверка с последующим лечением. Если параметр не задан, применяется режим, заданный в настройках. • `no` – проверка в режиме обнаружения. Если параметр не задан, применяется режим, заданный в настройках.

`/TRACE=<important|normal|detailed>`	Включает трассировку работы Portable Auditor. • `important` – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждения, а также дополнительная информация. • `normal` – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждениях, а также информация о работе Portable Auditor в нормальном режиме. • `detailed` – в файле трассировки сохраняется вся информация о работе Portable Auditor (значение по умолчанию).
`/DUMP`	Включает запись дампа.
`/REPORT=<full|critical|short>`	Определяет тип отчета, который создается в файле Kavscan\Report\report.txt после окончания проверки. Доступны следующие значения: • `full` – полный отчет о проверке со всеми типами событий. • `critical` – отчет о проверке содержит только критические события. • `short` – отчет о проверке содержит общую статистику и не содержит данных о событиях. По умолчанию применяется тип `short`.
`/SETTINGS=<full path to the file containing custom settings>`	Применяет пользовательские настройки из файла, к которому указан полный путь вместе с именем. Если значение не задано, Portable Auditor применяет параметры, заданные перед его созданием. Эти параметры расположены в файле Kavscan\settings.dat.

Коды возврата команды `KAVSCAN SCAN`:

- `0` – команда успешно выполнена.
- `1` – общая ошибка.

Экспорт результатов работы Portable Auditor с защищенного съемного диска

Если Portable Auditor записан на защищенный съемный диск, результаты работы Portable Auditor, отображенные в папке kavscan\Results, записываются в скрытый раздел диска. Поэтому напрямую просматривать, копировать и переносить результаты работы Portable Auditor на другой носитель невозможно.

Чтобы экспортировать результаты работы Portable Auditor с защищенного съемного диска, выполните следующие действия:

1. Подключите защищенный съемный диск к устройству, на которое вы хотите экспортировать результаты работы Portable Auditor.

   Kaspersky Industrial CyberSecurity for Nodes блокирует доступ к защищенным съемным дискам для сторонних процессов. Чтобы выполнить экспорт результатов работы Portable Auditor, вам нужно использовать устройство, на котором не установлено приложение Kaspersky Industrial CyberSecurity for Nodes, или выключить блокировку.

2. На устройстве запустите интерпретатор командной строки с правами локального администратора.
3. С помощью команды `cd /d` (например, `cd /d "E:\kavscan"`, где `E` – наименование съемного диска) перейдите в папку, в которой находится файл kavscan.exe.

4. Выполните команду:

```
KAVSCAN EXPORT /FOLDER=<full path to folder> [/CLEAN]
```

Где:

`/FOLDER=<full path to folder>` – параметр задает полный путь к папке, в которую вы хотите скопировать результаты работы Portable Auditor. Это может быть папка на устройстве, съемном диске, подключенном к устройству, или сетевая папка.

`/CLEAN` – параметр указывает на удаление результатов работы Portable Auditor с защищенного съемного диска. Если доступ к папке для экспорта отсутствует и копирование в папку не выполнено, то приложение не удаляет результаты работы Portable Auditor.

5. Введите запрошенный PIN-код администратора, который вы указывали перед созданием Portable Auditor.

Результаты работы Portable Auditor, отображенные в папке kavscan\Results, будут скопированы в папку по указанному пути, структура папок будет сохранена. Если указан параметр `/CLEAN`, результаты работы Portable Auditor будут удалены с защищенного съемного диска.

Чтобы обновить базы Portable Auditor, выполните следующие действия:

1. На устройстве запустите интерпретатор командной строки с правами локального администратора.

2. С помощью команды `cd /d` (например, `cd /d "E:\kavscan"`, где `E` – наименование съемного диска) перейдите в папку, в которой находится файл kavscan.exe.

3. Подключите съемный диск, на который записан Portable Auditor, к устройству, на котором расположена папка с обновлениями баз.

4. Выполните команду:

```
KAVSCAN UPDATE /SOURCE=<full path to folder>
```

где `<full path to folder>` – это хранилище точек распространения или локальная папка с загруженными базами приложения.

Portable Auditor обновит базы приложения в папке Bases и выполнит проверку баз, о результатах которой выведет в командной строке сообщение.

Блокировка доступа к защищенным съемным дискам

Kaspersky Industrial CyberSecurity for Nodes может блокировать доступ к защищенным съемным дискам, подключаемым к устройству с установленным приложением. Если блокировка включена, пользователю на данном устройстве доступны только создание Portable Auditor и выполнение задач *Безопасное копирование баз приложения* и *Безопасное обновление баз приложения*, доступ к защищенному съемному диску стандартными средствами операционной системы заблокирован.

Вы можете настроить блокировку доступа к защищенным съемным дискам из командной строки.

Управление Kaspersky Industrial CyberSecurity for Nodes из командной строки

Вы можете выполнять операции по управлению и администрированию Kaspersky Industrial CyberSecurity for Nodes из командной строки.

Чтобы управлять Kaspersky Industrial CyberSecurity for Nodes из командной строки, выполните следующие действия:

1. На устройстве запустите интерпретатор командной строки (например, cmd.exe) с правами учетной записи локального администратора.

2. С помощью команды `cd` перейдите в папку, где находится файл kavshell.exe.

   Пример

   ```
   cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0
   ```

   Также вы можете добавить путь к исполняемому файлу в системную переменную %PATH% на этапе установки приложения и выполнять команду без перехода в папку приложения.

3. Используйте следующий шаблон для выполнения команды:

   ```
   KAVSHELL <command> [options]
   ```

   Вы можете просмотреть список команд для управления приложением с помощью команды `KAVSHELL HELP`. Чтобы получить справку по синтаксису конкретной команды, введите `KAVSHELL HELP <command>`.

В результате Kaspersky Industrial CyberSecurity for Nodes выполнит указанное действие.

APPCONTROL. Импорт правил контроля запуска программ

Команда `KAVSHELL APPCONTROL` позволяет импортировать правила компонента Контроль запуска программ из XML-файла, а также удалять все правила из списка правил компонента. Вы можете сформировать XML-файл с правилами с помощью локальной или групповой задачи *Формирование правил контроля запуска программ*.

Синтаксис команды

```
KAVSHELL APPCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/APPEND | /REPLACE | /MERGE | /CLEAR`	Обязательный параметр. Импорт правил контроля запуска программ из указанного XML-файла: • `/APPEND` – добавление всех правил из файла в список правил компонента. Если правило уже есть в списке, оно дублируется. • `/REPLACE` – полная замена существующего списка правил компонента правилами из файла. • `/MERGE` – объединение правил из файла с существующим списком правил. Если правило уже есть в списке, оно не дублируется. Для удаления всех правил компонента Контроль запуска программ используйте параметр `/CLEAR`.
`<path to XML file>`	Обязательный параметр, если переданы параметры `/APPEND`, `/REPLACE`, `/MERGE`. Полный путь к XML-файлу с правилами.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL APPCONTROL /APPEND c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

APPCONTROL /CONFIG. Настройка компонента Контроль запуска программ

Команда `KAVSHELL APPCONTROL /CONFIG` позволяет настраивать параметры компонента Контроль запуска программ.

Синтаксис команды

```
KAVSHELLKAVSHELL APPCONTROL /CONFIG [/MODE:<applyrules|statistics>] [/DLL:<no|yes>] [/SAVETOFILE:<path to XML file>] [/SDC] [/CLEARSDC] /PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/MODE: <applyrules|statistics>`	Необязательный параметр. Режим работы компонента Контроль запуска программ: • `applyrules` – Kaspersky Industrial CyberSecurity for Nodes контролирует запуск приложений с помощью правил контроля запуска программ. • `statistics` (значение по умолчанию) – Kaspersky Industrial CyberSecurity for Nodes разрешает запуск всех приложений. В этом режиме приложение только записывает информацию обо всех запусках приложений, правилах, под действие которых подпадают запущенные приложения, и действиях, которые были бы выполнены, если бы компонент работал в режиме `applyrules`.
`/DLL:<no|yes>`	Необязательный параметр. Контроль загрузки DLL-модулей: • `no` (значение по умолчанию) – Kaspersky Industrial CyberSecurity for Nodes не контролирует загрузку DLL-модулей с помощью правил контроля запуска программ. Загрузка DLL-модулей разрешена. • `yes` – Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает загрузку DLL-модулей с помощью правил контроля запуска программ.
`/SAVETOFILE:<path to XML file>`	Необязательный параметр. Сохранение списка правил контроля запуска программ в указанный XML-файл.

`/SDC`	Необязательный параметр. Экспорт кеша распространения программ в конфигурационный файл формата XML, заданный с помощью параметра `/SAVETOFILE`.
`/CLEARSDC`	Необязательный параметр. Удаление кеша распространения программ.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml /PWD:p@ssw0rd
```

APPCONTROL /GENERATE. Формирование правил контроля запуска программ.

Команда `KAVSHELL APPCONTROL /GENERATE` позволяет управлять задачей *Формирование правил контроля запуска программ*.

Синтаксис команды

```
KAVSHELL APPCONTROL /GENERATE <path to folder> | /SOURCE:<path to file with folders list> [/MASKS:<edms>]
[/RUNAPP] [/RULES:<ch|cp|h>] [/STRONG] [/USER:<user or group of users>] [/EXPORT:<path to XML file>] [/IMPORT:
<a|r|m>] [/PREFIX:<prefix for rules names>] [/UNIQUE] [/ADDPATH] /PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`<path to folder>`	Обязательный параметр, если не передан параметр `/SOURCE`. Путь к папке с исполняемыми файлами, пакетами MSI и скриптами. Задача будет формировать разрешающие правила в случае запуска файлов выбранных типов, расположенных в указанных папках.
`/SOURCE:<path to file with folders list>`	Обязательный параметр, если не передан параметр `<path to folder>`. Путь к TXT-файлу со списком папок, содержащих исполняемые файлы, для которых будут автоматически формироваться разрешающие правила.
`/MASKS:<edms>`	Необязательный параметр. Расширения исполняемых файлов, для которых будут автоматически формироваться разрешающие правила. В область действия задачи можно включить файлы со следующими расширениями: • `e` – файлы с расширением .EXE; • `d` – файлы с расширением .DLL; • `m` – файлы с расширением .MSI; • `s` – скрипты.
`/RUNAPP`	Необязательный параметр. Создавать разрешающие правила на основе запущенных приложений.

`/RULES:<ch|cp|h>`	Необязательный параметр. Критерий, который будет устанавливать задача при формировании разрешающих правил контроля запуска программ: • `ch` – использовать цифровой сертификат. Если сертификат отсутствует, использовать хеш SHA256. • `cp` – использовать цифровой сертификат. Если сертификат отсутствует, использовать путь к исполняемому файлу. • `h` – использовать хеш SHA256.
`/STRONG`	Необязательный параметр. Использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Используется вместе с параметром `/RULES:<ch|cp>`.
`/USER:<user or group of users>`	Необязательный параметр. Имя пользователя или группы пользователей, для которых должны применяться правила.
`/EXPORT:<path to XML file>`	Необязательный параметр. Путь и имя XML-файла, в который будут сохранены указанные правила.
`/IMPORT:<a|r|m>`	Необязательный параметр. Импорт сформированных правил в список правил компонента Контроль запуска программ: • `a` – добавление всех правил из файла в список правил компонента. Если правило уже есть в списке, оно дублируется. • `r` – полная замена существующего списка правил компонента правилами из файла. • `m` – объединение правил из файла с существующим списком правил. Если правило уже есть в списке, оно не дублируется.
`/PREFIX:<prefix for rules names>`	Указание префикса для названий разрешающих правил контроля запуска программ.
`/UNIQUE`	Добавление в правила информации о защищаемом устройстве, на основе приложений которого формируются разрешающие правила контроля запуска программ.
`/ADDPATH`	Добавление пути к исполняемому файлу в правила, сформированные на основе хешей.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml /PWD:p@ssw0rd
```

CONFIG. Поддержка технологии AM-PPL

Команда `KAVSHELL CONFIG` позволяет управлять защитой процессов приложения с помощью технологии AM-PPL.

Для успешного выполнения команды необходимо выключить механизм самозащиты приложения.

Синтаксис команды

```
KAVSHELL CONFIG /PPL:<ON|OFF> /PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/PPL:<ON|OFF>`	Обязательный параметр. Позволяет включить или выключить поддержку технологии AM-PPL: • `ON` – включение поддержки технологии AM-PPL; • `OFF` – выключение поддержки технологии AM-PPL.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL CONFIG /PPL:ON
KAVSHELL CONFIG /PPL:OFF
```

CREATEPORTABLE. Создание Portable Auditor

Команда `KAVSHELL CREATEPORTABLE` позволяет создавать Portable Auditor на съемном диске.

Синтаксис команды

```
KAVSHELL CREATEPORTABLE /DRIVE=<name of the removable drive or serial number of the Rutoken removable drive>
/LICENSE=<path to the license key file> [/TOKENPIN=<password> [/NEWTOKENPIN=<password>]] [/VERIFY] [/AV <settings
of the scan for viruses and other threatening programs>] [/TRAFFIC=<duration in seconds>] [/OVAL <settings of the
security audit task>]
```

Параметры команды

Параметр	Описание
`/DRIVE=<name of the removable drive or serial number of the Rutoken removable drive>`	Обязательный параметр. Позволяет выбрать съемный диск, на котором будет создан Portable Auditor. Если Portable Auditor будет записан на съемный диск Рутокен, необходимо ввести десятизначный серийный номер диска Рутокен. Вы можете узнать серийные номера дисков Рутокен, подключенных к текущему устройству, с помощью команды `KAVSHELL TOKEN /ENUMERATE`.
`/LICENSE=<path to the license key file>`	Обязательный параметр. Позволяет указать путь к файлу ключа, необходимого для создания Portable Auditor.
`/TOKENPIN=<password>`	Обязательный параметр, если используется съемный диск Рутокен. Позволяет указать пароль администратора для доступа к диску Рутокен.
`/NEWTOKENPIN=<password>`	Необязательный параметр. Позволяет задать новый пароль администратора для доступа к диску Рутокен.
`/VERIFY`	Необязательный параметр. Позволяет включить проверку Portable Auditor после записи на съемный диск.
`/AV <settings of the scan for viruses and other threatening programs>`	Необязательный параметр. Должен быть указан хотя бы один из параметров `/av`, `/oval` или `/traffic`. Позволяет включить режим проверки на вирусы и другие программы, представляющие угрозу.

`/TRAFFIC=<duration in seconds>`	Необязательный параметр. Позволяет включить запись входящего и исходящего трафика проверяемого устройства в течение указанного времени. Допустимые значения: от 1 до 1800 секунд. Значение по умолчанию – 30 секунд.
`/OVAL <settings of the security audit task>`	Необязательный параметр. Позволяет включить задачу аудита безопасности.
Параметры проверки на вирусы и другие программы, представляющие угрозу	
`<list of files>`	Список файлов, папок, сетевых путей или предопределенных областей для сканирования через пробел.
`/L=<path to file with a list of scan scopes>`	Путь к файлу со списком областей сканирования. Файл должен быть создан вручную и сохранен в формате TXT. Файл должен быть сохранен в кодировке UTF-8 без BOM.
`/MEMORY`	Проверка всех процессов памяти. Данная область проверки включена по умолчанию.
`/SHARED`	Проверка общих папок.
`/STARTUP`	Проверка объектов автозапуска. Данная область проверки включена по умолчанию.
`/REMDRIVES`	Проверка всех съемных дисков.
`/NETDRIVES`	Проверка сетевых дисков.
`/FIXDRIVES`	Проверка всех локальных жестких дисков. Данная область проверки включена по умолчанию.
`/MYCOMP`	Проверка всего компьютера.
`/F<A|C|E>`	Объекты, которые требуется включить в область проверки: • `/FA` – Проверять все объекты. Приложение проверяет все файлы без исключения (любых форматов и расширений). • `/FC` – Проверять объекты по формату. Приложение проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам. • `/FE` – Проверять объекты по расширению. Приложение проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.
`/AI=<action>`	Действие при обнаружении зараженного объекта. Допустимые значения параметра: • `DISINFDEL` – **Лечить. Удалять, если лечение невозможно**; • `REPORT` (значение по умолчанию) – **Информировать**.
`/E=ABMSPO`	Исключение указанных типов объектов. Допустимые значения параметра: • `A` – архивы ZIP, CAB, RAR, ARJ и других форматов; • `B` – файлы почтовых баз Microsoft Outlook и Microsoft Outlook Express; • `M` – файлы почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express; • `S` – самораспаковывающиеся архивы; • `P` – исполняемые файлы, упакованные программами-упаковщиками двоичного кода, такими как UPX, ASPack и др; • `O` – встроенные в файлы объекты (таких как макросы Microsoft Word или вложения в сообщения электронной почты). Вы можете указать несколько значений.
`/EM=<file mask>`	Исключение из проверки файлов по маске. Например: • Маска `*.exe` будет включать все пути к файлам с расширением exe. • Маска `example*` будет включать все пути к файлам с именем EXAMPLE.
`/ET=<scan duration in seconds>`	Исключение из проверки файлов, длительность проверки которых превышает установленное значение в секундах. Значение по умолчанию – 60 сек.
`/ES=<size in megabytes>`	Исключение из проверки файлов, размер которых превышает установленное значение в мегабайтах. Значение по умолчанию – 100 МБ.

`/NOICHECKER`	Отключение функции iChecker. По умолчанию функция включена.
`/EXCLUDE=<list of exlusions>`	Список файлов, папок или сетевых путей, которые будут исключены из области действия задачи проверки. Вы можете указать несколько значений через пробел.
`/W=<file path>`	Путь и имя файла лога сканирования.
Параметры выполнения задачи аудита безопасности	
`/SOURCE=<kl|kl-compl|file>`	Параметр определяет источник правил, которые необходимы для аудита безопасности. Доступные значения параметра: • `kl` (по умолчанию включено) – база данных уязвимостей Kaspersky ICS CERT для АСУ ТП, входящая в поставку. • `kl-compl` (по умолчанию включено) – конфигурации безопасности и соответствий стандартам для операционных систем, входящие в поставку. • `file` – пользовательская база правил из файла.
`/PATH=<full path to ZIP archive with security audit rules>`	Параметр передает путь к файлам с правилами для источника **Пользовательская база правил** (`/SOURCE=file`). Запускает выполнение задачи аудита безопасности на основе правил в указанном ZIP-архиве. ZIP-архив должен содержать XML-файл с правилами, написанными на языке OVAL. Полный путь к ZIP-архиву указывается вместе с именем архива. OVAL-правила должны быть сохранены в кодировке UTF-8 без BOM.
`/MODE=<all|exclude|include>`	Параметр определяет режим проверки на уязвимости. Доступные значения параметра: • `all` – выполняется проверка на все уязвимости, указанные в источнике. • `exclude` – выполняется проверка на уязвимости, указанные в источнике, кроме указанных с помощью параметра `/DEFINITIONS`. • `include` – выполняется проверка на уязвимости, которые указаны с помощью параметра `/DEFINITIONS`. Используется совместно с параметром `/SOURCE=kl`.
`/DEFINITIONS=<vuln_type_01;...;vuln_type_N>`	Параметр определяет список типов уязвимостей, разделенных точкой с запятой, которые необходимо проверить или исключить из проверки. Например: `oval:org.mitre.oval.test:def:998;oval:org.mitre.oval.test:def:999`. Используется совместно с параметром `/MODE=include` или `/MODE=exclude`.

Пример:

```
KAVSHELL CREATEPORTABLE /DRIVE=E: /LICENSE=C:\0000000A.key /VERIFY /AV /l="C:\Documents and Settings\file.txt"
/ai=DISINFDEL
```

DEVCONTROL. Импорт правил контроля устройств

Команда `KAVSHELL DEVCONTROL` позволяет импортировать правила компонента Контроль устройств из XML-файла, полученного в результате выполнения задачи *Формирование правил контроля устройств*, а также удалять все правила из списка правил компонента.

Синтаксис команды

```
KAVSHELL DEVCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/APPEND | /REPLACE | /MERGE | /CLEAR`	Обязательный параметр. Импорт правил контроля устройств из указанного XML-файла: • `/APPEND` – добавление всех правил из файла в список правил компонента. Если правило уже есть в списке, оно дублируется. • `/REPLACE` – полная замена существующего списка правил компонента правилами из файла. • `/MERGE` – объединение правил из файла с существующим списком правил. Если правило уже есть в списке, оно не дублируется. Для удаления всех правил компонента Контроль устройств используйте параметр `/CLEAR`.
`<path to XML file>`	Обязательный параметр, если переданы параметры `/APPEND`, `/REPLACE`, `/MERGE`. Полный путь к XML-файлу с правилами.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL DEVCONTROL /MERGE c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

DUMP. Запись дампов памяти

Команда `KAVSHELL DUMP` позволяет включать и выключать запись дампов памяти.

Синтаксис команды

```
KAVSHELL DUMP </ON /F:<dump_file_folder> | /SNAPSHOT /F:<dump_file_folder> /P:<process_ID> | /OFF > [/PWD:
<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/ON`	Включить создание файлов дампов.
`/F:<dump_file_folder>`	Обязательный параметр. Позволяет указать папку, в которую будут сохраняться файлы дампов.
`/SNAPSHOT`	Позволяет создать дамп памяти выполняющегося процесса с указанным идентификатором. Файл дампа будет сохранен в папку, заданную параметром `/F`.
`/P:<process_ID>`	Обязательный параметр, если передан параметр `/SNAPSHOT`. Позволяет указать идентификатор процесса (ID). Вы можете узнать ID процесса с помощью команды `tasklist`.
`/OFF`	Выключить создание файлов дампов.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.

`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL DUMP /ON /F:"C:\Dumps and others"
KAVSHELL DUMP /SNAPSHOT /F:"C:\Dumps and others" /P:1234 /PWD:p@ssw0rd
KAVSHELL DUMP /OFF
```

EDR_EXPERT_ON_PREM. Интеграция с EDR Expert (on-premises)

Команда `KAVSHELL EDR_EXPERT_ON_PREM` позволяет настраивать интеграцию с решением Kaspersky Endpoint Detection and Response Expert (on-premises).

Синтаксис команды

```
KAVSHELL EDR_EXPERT_ON_PREM /ENABLE /MODE:<EDRKATA|ERDExpertOnPrem> /SERVERS:<address>:<port> [/PINNED-
CERTIFICATE:<full path to the TLS certificate file>] [/CLIENT-CERTIFICATE:<full path to the certificate file>]
[/CLIENT-PASSWORD:<password for the client certificate>] [/TIMEOUT:<server connection timeout, in seconds>]
[/SYNC-PERIOD":<synchronization period with the server, in minutes> [/EVENTS-SEND-PERIOD:<period of send events to
server, in seconds>] [/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or
0>] [/EVENTS-PER-HOUR:<events count limit: max events per hour>] [/MAX-PACKET-LENGTH:<Maximum number of event
packets transmitted within a transaction>] [/TELEMETRY-SERVERS:<address>:<port>] [/TELEMETRY-PINNED-CERTIFICATE:
<full path to the telemetry server TLS certificate file>] [/TELEMETRY-CLIENT-CERTIFICATE:<full path to the
telemetry certificate file>] [/TELEMETRY-CLIENT-PASSWORD:<password for the client certificate>] [/TELEMETRY-
TIMEOUT:<Telemetry server connection timeout, in seconds>] [/TELEMETRY-ONLY-TAGGED-EVENTS:<0|1>] [/PWD:<password>]
[/LOGIN:<user name>]
| /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
| /SHOW
```

Параметры команды

Параметр	Описание
`/<ENABLE|DISABLE|SHOW>`	Обязательный параметр. Включение, выключение или просмотр статуса интеграции Kaspersky Industrial CyberSecurity for Nodes с решением Endpoint Detection and Response Expert (on-premises).
`/MODE:<EDRKATA|ERDExpertOnPrem>`	Обязательный параметр. Выбор решения, с которым будет выполняться интеграция: • `EDRKATA` – Kaspersky Anti Targeted Attack Platform • `ERDExpertOnPrem` – Kaspersky Endpoint Detection and Response Expert (on-premises).
`/SERVERS:<address>:<port>`	Обязательный параметр. Адрес сервера реагирования и порт подключения к серверу. Вы можете указать несколько значений через `;`.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	Необязательный параметр. TLS-сертификат для установки доверенного соединения Kaspersky Industrial CyberSecurity for Nodes с сервером реагирования.
`/CLIENT-CERTIFICATE:<full path to the certificate file>`	Необязательный параметр. Позволяет добавить *криптоконтейнер* – файл формата PFX, в котором в зашифрованном виде хранится клиентский сертификат для защиты соединения Kaspersky Industrial CyberSecurity for Nodes с сервером реагирования.
`/CLIENT-PASSWORD:<password for the client certificate>`	Обязательный параметр, если передан параметр `/CLIENT-CERTIFICATE`. Позволяет указать пароль для доступа к криптоконтейнеру.

`/TIMEOUT:<server connection timeout, in seconds>`	Необязательный параметр. Максимальное время ожидания ответа от сервера реагирования в секундах. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 10 сек.
`/SYNC-PERIOD:<synchronization period with the server, in minutes>`	Необязательный параметр. Интервал между запросами на сервер реагирования в минутах. Диапазон доступных значений: 1–60 мин. Значение по умолчанию 5 мин.
`/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>`	Необязательный параметр. Максимальная продолжительность задержки отправки событий на сервер реагирования. По истечении указанного времени приложение повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.
`/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or 0>`	Необязательный параметр. Позволяет включить ограничение количества передаваемых событий: • `1` – включено; • `0` – выключено (значение по умолчанию). Если количество событий превышает установленные ограничения, приложение прекращает отправлять события.
`/EVENTS-PER-HOUR:<events count limit: max events per hour>`	Необязательный параметр. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.
`/TELEMETRY-SERVERS:<address>:<port>`	Обязательный параметр. Адрес сервера сбора телеметрии и порт подключения к серверу. Вы можете указать несколько значений через `;`.
`/TELEMETRY-PINNED-CERTIFICATE:<full path to the telemetry server TLS certificate file>`	Необязательный параметр. TLS-сертификат для установки доверенного соединения Kaspersky Industrial CyberSecurity for Nodes с сервером сбора телеметрии.
`/TELEMETRY-CLIENT-CERTIFICATE:<full path to the telemetry certificate file>`	Необязательный параметр. Позволяет добавить *криптоконтейнер* – файл формата PFX, в котором в зашифрованном виде хранится клиентский сертификат для защиты соединения Kaspersky Industrial CyberSecurity for Nodes с сервером сбора телеметрии.
`/TELEMETRY-CLIENT-PASSWORD:<password for the client certificate>`	Обязательный параметр, если передан параметр `/CLIENT-CERTIFICATE`. Позволяет указать пароль для доступа к криптоконтейнеру.
`/TELEMETRY-TIMEOUT:<Telemetry server connection timeout, in seconds>`	Необязательный параметр. Максимальное время ожидания ответа от сервера сбора телеметрии в секундах. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 10 сек.
`/TELEMETRY-ONLY-TAGGED-EVENTS:<0|1>`	Необязательный параметр. Отправлять телеметрию только с IOA: • `1` – включено; • `0` – выключено (значение по умолчанию).
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL EDR_EXPERT_ON_PREM /MODE=EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-HOUR=3000
/PWD:p@ssw0rd
```

```
KAVSHELL EDR_EXPERT_ON_PREM /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx
/PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /MODE=EDRExpertOnPrem /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-
HOUR=3000 /telemetry-SERVERS:127.0.0.1:8080;telemetry.server.ru:8080 /telemetry-TIMEOUT=30 /PINNED-
CERTIFICATE:c:\user\certs\telemetry_cert.pfx /PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /DISABLE /PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /SHOW
```

EDRKATA. Интеграция с KATA

Команда `KAVSHELL EDRKATA` позволяет настраивать интеграцию с решением Kaspersky Anti Targeted Attack Platform.

Синтаксис команды

```
KAVSHELL EDRKATA /ENABLE /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS certificate file>]
[/CLIENT-CERTIFICATE:<full path to the certificate file>] [/CLIENT-PASSWORD:<password for the client certificate>]
[/TIMEOUT:<server connection timeout, in seconds>] [/SYNC-PERIOD:<synchronization period with the server, in
minutes> [/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>] [/EVENTS-LIMIT:<events count limit:
enable (1) or disable (0) events count limit, value 1 or 0>] [/EVENTS-PER-HOUR:<events count limit: max events per
hour>] [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/PWD:<current password>] [/LOGIN:<user name>] | /SHOW
```

Параметры команды

Параметр	Описание
`/<ENABLE|DISABLE|SHOW>`	Обязательный параметр. Включение, выключение или просмотр статуса интеграции Kaspersky Industrial CyberSecurity for Nodes с решением Kaspersky Anti Targeted Attack Platform.
`/SERVERS:<address>:<port>`	Обязательный параметр. Адрес сервера KATA Central Node (IPv4, IPv6) и порт подключения к серверу. Вы можете указать несколько значений через `;`.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	Необязательный параметр. TLS-сертификат для установки доверенного соединения Kaspersky Industrial CyberSecurity for Nodes с сервером Central Node.
`/CLIENT-CERTIFICATE:<full path to the certificate file>`	Необязательный параметр. Позволяет добавить *криптоконтейнер* – файл формата PFX, в котором в зашифрованном виде хранится клиентский сертификат для защиты соединения Kaspersky Industrial CyberSecurity for Nodes с сервером Central Node.
`/CLIENT-PASSWORD:<password for the client certificate>`	Обязательный параметр, если передан параметр `/CLIENT-CERTIFICATE`. Позволяет указать пароль для доступа к криптоконтейнеру.
`/TIMEOUT:<server connection timeout, in seconds>`	Необязательный параметр. Максимальное время ожидания ответа от сервера сбора телеметрии в секундах. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 10 сек.
`/SYNC-PERIOD:<synchronization period with the server, in minutes>`	Необязательный параметр. Интервал между запросами на сервер Central Node в минутах. Диапазон доступных значений: 1–60 мин. Значение по умолчанию 5 мин.
`/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>`	Необязательный параметр. Максимальная продолжительность задержки отправки событий на сервер Central Node. По истечении указанного времени приложение повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.

`/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or 0>`	Необязательный параметр. Позволяет включить ограничение количества передаваемых событий: • `1` – включено; • `0` – выключено (значение по умолчанию). Если количество событий превышает установленные ограничения, приложение прекращает отправлять события.
`/EVENTS-PER-HOUR:<events count limit: max events per hour>`	Необязательный параметр. По умолчанию установлено значение 3000 событий в час. Если приложение установлено на сервер, поток данных телеметрии выше. Для серверов рекомендуется увеличить значение до 60 тыс. событий в час.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-HOUR=3000 /PWD:p@ssw0rd
KAVSHELL EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx /PWD:p@ssw0rd
KAVSHELL EDRKATA /DISABLE /PWD:p@ssw0rd
KAVSHELL EDRKATA /SHOW
```

EXITPOLICY. Выключение политики на устройстве

Команда `KAVSHELL EXITPOLICY` позволяет выключить политику Kaspersky Security Center на устройстве. После выключения политики все параметры Kaspersky Industrial CyberSecurity for Nodes станут доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком (🔒).

Синтаксис команды

```
KAVSHELL EXITPOLICY [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL EXITPOLICY /PWD:p@ssw0rd
```

EXPORT. Экспорт настроек приложения

Команда `KAVSHELL EXPORT` позволяет экспортировать настройки Kaspersky Industrial CyberSecurity for Nodes в конфигурационный файл формата XML. Вы можете сохранить в конфигурационный файл как все настройки приложения, так и настройки его отдельных компонентов.

Синтаксис команды

```
KAVSHELL EXPORT <profile> <file name> [/LOGIN:<user name>] [/PWD:<password>]
```

Параметры команды

Параметр	Описание
`<profile>`	Обязательный параметр. Укажите название профиля настроек для экспорта. Профиль – компонент, задача или функция Kaspersky Industrial CyberSecurity for Nodes. Список доступных профилей вы можете узнать с помощью команды `KAVSHELL EXPORT /?`. Для экспорта всех настроек приложения укажите профиль `product`.
`<file name>`	Обязательный параметр. Укажите имя файла в формате XML для экспорта параметров профиля. Также вы можете указать путь к файлу. Пример: `C:\Test\settings.xml` • Если в команде указано только имя файла, приложение выполнит попытку разместить файл в папке установки приложения. Если механизмы самозащиты приложения включены, экспорт завершится с ошибкой, так как самозащита приложения заблокирует создание нового файла в папке приложения. Для экспорта параметров приложения укажите путь к файлу.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.

Пример

```
KAVSHELL EXPORT product C:\Test\settings.xml /LOGIN:Admin /PWD:p@ssw0rd
```

FBRESET. Очистка базы iSwift

Kaspersky Industrial CyberSecurity for Nodes может использовать технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен. Команда `KAVSHELL FBRESET` позволяет очистить базу, в которой хранится информация о проверенных незараженных файлах. После очистки базы Kaspersky Industrial CyberSecurity for Nodes проверяет все файлы, к которым обращается впервые.

Синтаксис команды

```
KAVSHELL FBRESET
```

FIM /BASELINE. Мониторинг целостности системы на основе эталона

Команда `KAVSHELL FIM /BASELINE` позволяет управлять задачей *Мониторинг целостности системы на основе эталона*.

```
KAVSHELL FIM /BASELINE [[/CREATE {<monitoring scope>|/L:<path to TXT file containing the list of monitoring areas>}] [/MD5 | /SHA256] [/SF] [/W:<file name>] [/ANSI]] [/SCAN {[/BL:<id baseline>] | [/ALIAS:<existing task id>]} [/W:<file name>] [/ANSI]] [/CLEAR [/BL:<id baseline>] | [/ALIAS:<existing task id>]] [/SHOW [[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/EXPORT:<path to folder>[[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/CREATE`	Запуск новой задачи *Мониторинг целостности системы на основе эталона*, во время которой будет создан снимок состояния системы.
`/SCAN`	Запустить задачи *Мониторинг целостности системы на основе эталона* с указанием идентификатора снимка состояния системы или альтернативного названия существующей задачи.
`/CLEAR`	Удаление снимка состояния системы. Укажите идентификатора снимка состояния системы или альтернативное название задачи, создавшей снимок. Если альтернативное название задачи или идентификатора снимка состояния системы не указаны, приложение удалит все снимки состояния системы.
`/EXPORT`	Экспорт данных всех снимков или указанного с помощью параметра `/BL` снимка в указанную папку в файл формата TXT.
`/SHOW`	Отобразить данные всех снимков состояния системы или указанного с помощью параметра `/BL` снимка.
`<monitoring scope>`	Обязательный параметр, если не задан параметр /L. Позволяет указать область мониторинга задачи. Вы можете использовать символы `*` и `?` для ввода маски пути.
`/L`	Обязательный параметр, если не задан параметр `<monitoring scope>`. Позволяет указать путь к TXT-файлу, содержащему список областей мониторинга.
`/MD5`	Необязательный параметр. Не используется совместно с параметром `/SHA256`. Позволяет задать алгоритм MD5 для вычисления контрольной суммы. По умолчанию используется алгоритм MD5.
`/SHA256`	Необязательный параметр. Не используется совместно с параметром `/MD5`. Позволяет задать алгоритм SHA256 для вычисления контрольной суммы. По умолчанию используется алгоритм MD5.
`/SF`	Необязательный параметр. Позволяет включить все вложенные папки в область мониторинга задачи. По умолчанию вложенные папки не входят в область мониторинга.
`/ALIAS:<existing task id>`	Обязательный параметр, если не задан параметр `/BL`. Альтернативное название задачи. Вы можете узнать альтернативное название задачи с помощью команды `KAVSHELL FIM /BASELINE /SHOW`.
`/BL:<id baseline>`	Обязательный параметр, если не задан параметр `/ALIAS`. Позволяет указать идентификатор снимка состояния системы. Вы можете узнать идентификатор снимка с помощью команды `KAVSHELL FIM /BASELINE /SHOW`.

`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL FIM /BASELINE /CREATE "c:\program files\*" /MD5 /SF
KAVSHELL FIM /BASELINE /CREATE /L:c:\programdata\mytask\list.txt /ALIAS:SystemIntegrityMonitorOnDemandTask$001
/MD5 /SF
KAVSHELL FIM /BASELINE /SCAN /ALIAS:SystemIntegrityMonitorOnDemandTask$001
KAVSHELL FIM /BASELINE /EXPORT:c:\programdata\mytask\baselines\
```

HELP. Вызов справки о командах

Чтобы вывести список всех доступных команд Kaspersky Industrial CyberSecurity for Nodes, выполните одну из следующих команд:

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

Чтобы вывести описание команды и ее синтаксис, выполните одну из следующих команд:

```
KAVSHELL HELP <command>
KAVSHELL <command> /?
```

Пример

```
KAVSHELL HELP SCAN
```

IMPORT. Импорт настроек приложения

Команда `KAVSHELL IMPORT` позволяет импортировать настройки Kaspersky Industrial CyberSecurity for Nodes из конфигурационного файла формата XML. Вы можете создать конфигурационный файл с помощью команды `KAVSHELL EXPORT`.

Синтаксис команды

```
KAVSHELL IMPORT <file_name> /PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`<file name>`	Обязательный параметр. Укажите полный путь к XML-файлу, включая его имя и расширение, из которого должны быть импортированы настройки.

`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL IMPORT C:\Test\settings.xml /PWD:p@ssw0rd
```

Коды возврата команды:

- 0 – операция выполнена успешно.
- -2 – служба не запущена.
- -3 – недостаточно прав для выполнения команды.
- -4 – объект не найден.
- -9 – неудачная попытка запустить управляемое устройство под другой учетной записью.
- -99 – неизвестная ошибка.
- -501 – операция выполнена успешно, однако во время выполнения возникла ошибка или предупреждение (например, приложение не импортировало параметры некоторых компонентов).
- -502 – файл импорта отсутствует или имеет неизвестный формат.
- -503 – несовместимые параметры (конфигурационный файл экспортирован из другого приложения или Kaspersky Industrial CyberSecurity for Nodes более поздней или несовместимой версии).

KICS. Интеграция с Kaspersky Industrial CyberSecurity for Networks

Команда `KAVSHELL KICS` позволяет настроить интеграцию с Kaspersky Industrial CyberSecurity for Networks:

1. Для настройки интеграции Kaspersky Industrial CyberSecurity for Nodes с Kaspersky Industrial CyberSecurity for Networks по протоколу TCP выполните следующую команду:

```
KAVSHELL KICS /ENABLE /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS certificate file>]
[/CLIENT-CERTIFICATE:<full path to the crypto-container>] [/CLIENT-PASSWORD:<password for the crypto-
container>] [/TIMEOUT:<maximum server response timeout>] [/SYNC-PERIOD:<synchronization request period>]
[/EVENTS-SENT-PERIOD:<maximum delay when sending events>] [/EVENTS-LIMIT:<1|0>] [/EVENTS-PER-HOUR:<maximum
number of events per hour>] [/VIRTUAL-SPAN-ENABLE] [/VIRTUAL-SPAN-DISABLE] [/VIRTUAL-SPAN-ADD-RULES:<subnet
IDs>] [/VIRTUAL-SPAN-REMOVE-RULES:<subnet IDs>] [/LOGIN:<user name>] [/PWD:<password>]
```

2. Для настройки интеграции Kaspersky Industrial CyberSecurity for Nodes с Kaspersky Industrial CyberSecurity for Networks в режиме MQTT-издателя выполните следующую команду:

```
KAVSHELL KICS /ENABLE /KICS-MODE:MQTT-PUBLISHER /MQTT-SERVER:<address>:<port> [/MQTT-USER:<login name for authorization at the MQTT broker>] [/MQTT-PASSWORD:<password for authorization at the MQTT broker>] [/LOGIN:<user name>] [/PWD:<password>]
```

3. Для настройки интеграции Kaspersky Industrial CyberSecurity for Nodes с Kaspersky Industrial CyberSecurity for Networks по протоколу UDP выполните следующую команду:

```
KAVSHELL KICS /ENABLE /KICS-MODE:UDP-DATA-DIODE /UDP-SERVER:<address>:<port> [/UDP-ENCRYPTION-DISABLE] [/UDP-ENCRYPTION-ENABLE] [/UDP-ENCRYPTION-KEY:<full path to the encryption key>] [/UDP-ENCRYPTION-PASSWORD:<password to the encryption key>]
```

4. Для настройки интеграции Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика выполните следующую команду:

```
KAVSHELL KICS /ENABLE /KICS-MODE:TELEMETRY /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS certificate file>] [/CLIENT-CERTIFICATE:<full path to the crypto-container>] [/CLIENT-PASSWORD:<password for the crypto-container>] [/TIMEOUT:<maximum server response timeout>] [/SYNC-PERIOD:<synchronization request period>] [/EVENTS-SENT-PERIOD:<maximum delay when sending events>] [/EVENTS-LIMIT:<1|0>] [/EVENTS-PER-HOUR:<maximum number of events per hour>] [/VIRTUAL-SPAN-ENABLE] [/VIRTUAL-SPAN-DISABLE] [/VIRTUAL-SPAN-ADD-RULES:<subnet IDs>] [/VIRTUAL-SPAN-REMOVE-RULES:<subnet IDs>] /MQTT-SUBSCRIBER-ENABLE /MQTT-SERVER:<address>:<port> [/MQTT-USER:<login name for authorization at the MQTT broker>] [/MQTT-PASSWORD:<password for authorization at the MQTT broker>] [/LOGIN:<user name>] [/PWD:<password>]
```

Параметры команды

Параметр	Описание
`/<ENABLE|DISABLE|SHOW>`	Обязательный параметр. Позволяет включить, выключить или просмотреть статус интеграции Kaspersky Industrial CyberSecurity for Nodes с Kaspersky Industrial CyberSecurity for Networks.
`/SERVERS:<address>:<port>`	Обязательный параметр. Позволяет указать адрес и порт сервера Kaspersky Industrial CyberSecurity for Networks или адрес MQTT-брокера. Диапазон возможных значений порта: 1–65535.
`/KICS-MODE:<TELEMETRY|MQTT-PUBLISHER|UDP-DATA-DIODE>`	Необязательный параметр. Позволяет выбрать режим интеграции приложения с Kaspersky Industrial CyberSecurity for Networks. • `TELEMETRY` – режим отправки телеметрии напрямую на сервер Kaspersky Industrial CyberSecurity for Networks по протоколу TCP; • `MQTT-PUBLISHER` – режим отправки телеметрии на сервер MQTT-брокера; • `UDP-DATA-DIODE` – режим отправки телеметрии через диод данных по протоколу UDP. Значение параметра по умолчанию – `TELEMETRY`.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	Необязательный параметр. Позволяет добавить TLS-сертификат соединения Kaspersky Industrial CyberSecurity for Nodes с сервером Kaspersky Industrial CyberSecurity for Networks.
`/CLIENT-CERTIFICATE:<full path to the crypto-container>`	Необязательный параметр. Позволяет добавить *криптоконтейнер* – файл формата PFX, в котором в зашифрованном виде хранится клиентский сертификат для защиты соединения Kaspersky Industrial CyberSecurity for Nodes с сервером Kaspersky Industrial CyberSecurity for Networks.
`/CLIENT-PASSWORD:<password for the crypto-container>`	Обязательный параметр, если передан параметр `/CLIENT-CERTIFICATE`. Позволяет указать пароль для доступа к криптоконтейнеру.
`/TIMEOUT:<maximum server response timeout>`	Необязательный параметр. Позволяет указать максимальную продолжительность ожидания ответа от сервера Kaspersky Industrial CyberSecurity for Networks в секундах. По истечении времени ожидания Kaspersky Industrial CyberSecurity for Nodes пытается подключиться к другому серверу Kaspersky Industrial CyberSecurity for Networks, если их несколько. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.

`/SYNC-PERIOD:<synchronization request period>`	Необязательный параметр. Позволяет указать интервал между запросами на сервер Kaspersky Industrial CyberSecurity for Networks в минутах. При работе Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-издателя данный параметр задает интервал между запросами к MQTT-брокеру в случае потери соединения с брокером. Диапазон доступных значений: 1–60 мин. Значение по умолчанию – 1 мин.
`/EVENTS-SENT-PERIOD:<maximum delay when sending events>`	Необязательный параметр. Позволяет указать максимальную продолжительность задержки отправки событий на сервер Kaspersky Industrial CyberSecurity for Networks. По истечении указанного времени приложение повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек. При использовании Kaspersky Industrial CyberSecurity for Nodes в качестве MQTT-подписчика не рекомендуется настраивать получение данных телеметрии более чем от 250 устройств с Kaspersky Industrial CyberSecurity for Nodes, настроенном в качестве MQTT-издателя, в случае, если в настройках MQTT-издателей задано минимальное значение параметра `/EVENTS-SENT-PERIOD` – 1 сек. Если значение параметра равно 30 сек. и более, не рекомендуется настраивать получение данных более чем от 1000 MQTT-издателей.
`/EVENTS-LIMIT:<1|0>`	Необязательный параметр. Позволяет включить ограничение количества передаваемых событий. Если количество событий превышает установленные ограничения, приложение прекращает отправлять события.
`/EVENTS-PER-HOUR:<maximum number of events per hour>`	Обязательный параметр, если передан параметр `/EVENTS-LIMIT:1`. Позволяет указать максимальное количество передаваемых событий в час. Диапазон доступных значений: 10–65 535. По умолчанию установлено значение 3000 событий в час.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.
`/VIRTUAL-SPAN-ENABLE`	Необязательный параметр. Позволяет включить режим неизбирательного сбора телеметрии. По умолчанию Kaspersky Industrial CyberSecurity for Nodes собирает сетевой трафик, поступающий на сетевые интерфейсы компьютера и предназначенный компьютеру, на котором установлено приложение. В неизбирательном режиме приложение собирает сетевой трафик для сетевых интерфейсов компьютера с установленным приложением со всех доступных подсетей. На основе собранного сетевого трафика приложение формирует расширенную телеметрию. Не все сетевые адаптеры поддерживают неизбирательный режим сбора телеметрии (англ. Promiscuous mode). На этих сетевых адаптерах сбор расширенной телеметрии не работает.
`/VIRTUAL-SPAN-DISABLE`	Необязательный параметр. Позволяет выключить режим неизбирательного сбора телеметрии.
`/VIRTUAL-SPAN-ADD-RULES:<IPv4 addresses of the computer's network interfaces>`	Необязательный параметр. Позволяет добавить подсети в виде адресов сетевых интерфейсов компьютера (соответствующие подсети приложение определяет по маске подсети сетевого интерфейса), либо адресов сетевых интерфейсов с подсетями в формате IPv4. Приложение собирает сетевой трафик в неизбирательном режиме только для сетевых интерфейсов, настроенных на указанные подсети. Например: `/VIRTUAL-SPAN-ADD-RULES:198.51.100.0; 198.51.100.0/24`.

/VIRTUAL-SPAN-REMOVE-RULES:<subnet IDs>	Необязательный параметр. Позволяет удалить подсети с указанными идентификаторами. Список добавленных подсетей и их идентификаторы можно отобразить с помощью команды KAVSHELL KICS /SHOW.
/MQTT-SUBSCRIBER-ENABLE	Необязательный параметр. Позволяет включить режим MQTT-подписчика для получения телеметрии с диода данных. По умолчанию режим MQTT-подписчика выключен.
/MQTT-SUBSCRIBER-DISABLE	Необязательный параметр. Позволяет выключить режим MQTT-подписчика.
/MQTT-SERVER:<address>:<port>	Обязательный параметр, если передан параметр /KICS-MODE:MQTT-PUBLISHER или параметр /MQTT-SUBSCRIBER:ENABLE. Позволяет указать адрес и порт MQTT-брокера. Значение порта по умолчанию для MQTT-брокера – 1883.
/MQTT-USER:<login>	Обязательный параметр, если на MQTT-брокере настроена авторизация по логину и паролю. Позволяет указать логин для авторизации на MQTT-брокере.
/MQTT-PASSWORD:<password>	Обязательный параметр, если на MQTT-брокере настроена авторизация по логину и паролю. Позволяет указать пароль для авторизации на MQTT-брокере.
/UDP-SERVER:<address>:<port>	Обязательный параметр, если передан параметр /KICS-MODE:UDP-DATA-DIODE. Позволяет указать адрес и порт сервера Kaspersky Industrial CyberSecurity for Networks.
/UDP-ENCRYPTION-ENABLE	Необязательный параметр. Позволяет включить шифрование при передаче данных по протоколу UDP.
/UDP-ENCRYPTION-DISABLE	Необязательный параметр. Позволяет выключить шифрование при передаче данных по протоколу UDP.
/UDP-ENCRYPTION-KEY:<full path to the encryption key>	Обязательный параметр, если передан параметр /UDP-ENCRYPTION-ENABLE. Позволяет указать путь к файлу ключа шифрования с расширением .PEM.
/UDP-ENCRYPTION-PASSWORD:<password to the encryption key>	Обязательный параметр, если передан параметр /UDP-ENCRYPTION-ENABLE. Позволяет указать пароль для ключа шифрования.

Пример

```
KAVSHELL KICS /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx /PWD:p@ssw0rd
KAVSHELL KICS /DISABLE /PWD:p@ssw0rd
KAVSHELL KICS /SHOW
KAVSHELL KICS /VIRTUAL-SPAN-ENABLE /PWD:p@ssw0rd
KAVSHELL KICS /VIRTUAL-SPAN-REMOVE-RULES:1,2,3 /PWD:p@ssw0rd
KAVSHELL KICS /VIRTUAL-SPAN-ADD-RULES:192.168.73.0/24;192.168.73.0/24 /PWD:p@ssw0rd
KAVSHELL KICS /ENABLE /KICS-MODE:MQTT-PUBLISHER /MQTT-SERVER:1.2.3.4:1218 /MQTT-USER:User /MQTT-PASSWORD:p@ssw0rd
/PWD:p@ssw0rd
KAVSHELL KICS /ENABLE /KICS-MODE:TELEMETRY /SERVERS:123.4.5.6:8080 /MQTT-SUBSCRIBER-ENABLE /MQTT-
SERVER:1.2.3.4:1218 /MQTT-USER:User /MQTT-PASSWORD:p@ssw0rd /PWD:p@ssw0rd
KAVSHELL KICS /MQTT-SUBSCRIBER-DISABLE
KAVSHELL KICS /ENABLE /KICS-MODE:UDP-DATA-DIODE /UDP-SERVER:1.2.3.4:1234 /UDP-ENCRYPTION-ENABLE /UDP-ENCRYPTION-
KEY:c:\user\username\123e4567-e89b-12d3-a456-426655440990.pem /UDP-ENCRYPTION-PASSWORD:p@ssw0rd
```

Коды возврата команды:

- 0 – команда выполнена успешно.
- -3 – недостаточно прав для выполнения команды.
- -5 – синтаксическая ошибка.

ISOLATION. Управление Сетевой изоляцией

Команда `KAVSHELL ISOLATION` позволяет локально управлять Сетевой изоляцией устройства.

Синтаксис команды

```
KAVSHELL ISOLATION [/DISABLE] [/SHOW] [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/DISABLE`	Обязательный параметр, если не передан параметр `/SHOW`. Выключение сетевой изоляции устройства.
`/SHOW`	Обязательный параметр, если не передан параметр `/DISABLE`. Отображение в консоли текущих параметров сетевой изоляции на устройстве.
`/PWD:<password>`	Обязательный параметр для команды `KAVSHELL ISOLATION /DISABLE`. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Коды возврата команды:

- 0 – операция выполнена успешно.
- -3 – недостаточно прав для выполнения команды.
- -5 – синтаксическая ошибка.
- -6 – неверная операция (например, попытка выключить компонент, если компонент уже выключен).
- -7 – служба не зарегистрирована.
- -8 – автоматический запуск службы отключен.
- -9 – неудачная попытка запустить управляемое устройство под другой учетной записью.
- -99 – неизвестная ошибка.

KSN. Использование KSN/KPSN

Команда `KAVSHELL KSN` позволяет выбирать решение "Лаборатории Касперского" для определения репутации файлов или сайтов. Kaspersky Industrial CyberSecurity for Nodes поддерживает следующие инфраструктурные решения для работы с репутационными базами "Лаборатории Касперского":

- *Kaspersky Security Network (KSN)* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от "Лаборатории Касперского", а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз.

- *Kaspersky Private Security Network (KPSN)* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Industrial CyberSecurity for Nodes или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам "Лаборатории Касперского", а также другим статистическим данным, не отправляя данные в "Лабораторию Касперского" со своих компьютеров. KPSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к сети Интернет;

  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Синтаксис команды

```
KAVSHELL KSN /GLOBAL|/PRIVATE <settings-file> /PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/GLOBAL`	Переключение на использование Kaspersky Security Network.
`/PRIVATE <settings-file>`	Переключение на использование Kaspersky Private Security Network. Укажите имя конфигурационного файла с параметрами Kaspersky Private Security Network. Файл имеет разрешение .PKCS7 или .PEM.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL KSN /GLOBAL /PWD:p@ssw0rd
KAVSHELL KSN /PRIVATE c:\settings.pkcs7 /PWD:p@ssw0rd
```

LICENSE. Активация приложения

Команда `KAVSHELL LICENSE` позволяет управлять ключами и кодами активации Kaspersky Industrial CyberSecurity for Nodes.

Синтаксис команды

```
KAVSHELL LICENSE [/ADD:<key_file | activation code> [/R]|/DEL:<license key serial number>|/REFRESH:<license id>]
/PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
Параметры не указаны.	Команда возвращает следующую информацию о добавленных ключах: • Ключ. • Тип лицензии (коммерческая). • Срок действия связанной с ключом лицензии. • Статус ключа (активный или дополнительный). Если значение статуса *, ключ добавлен в качестве дополнительного.
`/ADD:<key_file | activation code>`	Активация Kaspersky Industrial CyberSecurity for Nodes с помощью файла ключа. Если приложение уже активировано, ключ будет добавлен в качестве резервного.
`/R`	Если передан параметр `/R`, код активации или ключ добавляется в качестве резервного.
`/DEL:<license key serial number>`	Удаление указанного ключа или кода активации.
`/REFRESH:<license id>`	Обновление статуса указанной лицензии.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Коды возврата команды:

- 0 – операция выполнена успешно.
- -2 – служба не запущена.
- -3 – недостаточно прав для выполнения команды.
- -4 – ключ с указанным номером не найден.
- -5 – синтаксическая ошибка.
- -6 – неверная операция (ключ уже добавлен).
- -99 – неизвестная ошибка.
- -301 – лицензия недействительна.
- -303 – лицензия распространяется на другое приложение.

MDR. Настройка интеграции с Managed Detection and Response

Команда `KAVSHELL MDR` позволяет настроить интеграцию Kaspersky Industrial CyberSecurity for Nodes с решением Managed Detection and Response.

Синтаксис команды

```
KAVSHELL MDR /ENABLE /BLOB:<path to pkcs7> [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/BLOB:<path to pkcs7>] [/PWD:<password>] [/LOGIN:<user name>] | /SHOW
```

Параметры команды

Параметр	Описание
`MDR /<enable|disable|show>`	Обязательный параметр. Позволяет включить, выключить или просмотреть текущие настройки компонента Managed Detection and Response (Industrial CyberSecurity).
`/BLOB:<full path to the MDR configuration file>`	Обязательный параметр. Позволяет указать путь к конфигурационному файлу MDR.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL MDR /ENABLE /BLOB:C:\some\folder\blob.pkcs7 /PWD:p@ssw0rd
KAVSHELL MDR /DISABLE /PWD:p@ssw0rd
KAVSHELL MDR /SHOW
```

NETWORKBLOCKING. Управление Блокировкой соединений

Команда `KAVSHELL NETWORKBLOCKING` позволяет локально выключить блокировку сетевых соединений устройства. Подробнее о блокировке соединений см. в справке Kaspersky Industrial CyberSecurity for Networks.

Синтаксис команды

```
KAVSHELL NETWORKBLOCKING /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/DISABLE`	Обязательный параметр. Выключает блокировку сетевых соединений устройства.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Коды возврата команды:

- 0 – команда выполнена успешно.
- -3 – недостаточно прав для выполнения команды.
- -5 – синтаксическая ошибка.
- -6 – неверная операция (например, попытка выключить компонент, если компонент уже выключен).
- -9 – неудачная попытка запустить управляемое устройство под другой учетной записью.
- -99 – неизвестная ошибка.

OMSINFO. Создание JSON-файла с информацией о приложении

Команда `KAVSHELL OMSINFO` позволяет создавать JSON-файл с информацией о текущем статусе приложения и обнаруженных угрозах, который в дальнейшем может быть загружен в системы мониторинга.

Синтаксис команды

```
KAVSHELL OMSINFO <oms_info_json_file_name>
```

Параметры команды

Параметр	Описание
`<oms_info_json_file_name>`	Полный путь к JSON-файлу, включая его имя и расширение.

Пример

```
KAVSHELL OMSINFO "C:\Dumps and others\omsinfo.json"
```

PASSWORD. Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля

Команда `KAVSHELL PASSWORD` позволяет управлять защитой доступа к функциям Kaspersky Industrial CyberSecurity for Nodes с помощью пароля. Если функция включена, приложение будет запрашивать имя и пароль пользователя при удалении/изменении/восстановлении приложения и при выполнении действий в командной строке, которые могут привести к снижению уровня защиты устройства.

Синтаксис команды

```
KAVSHELL PASSWORD /SET /NEW:<new password> | /RESET /PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/SET`	Позволяет включить функцию запроса пароля для подтверждения критических действий.

`/NEW:<new password>`	Обязательный параметр, если передан параметр `/SET`.
	Позволяет установить новый пароль.
	При создании пароля рекомендуется выполнить следующие условия:
	• Пароль не должен содержать имя учетной записи и имя компьютера.
	• Длина пароля должна составлять не менее 8 символов.
	• Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
	  • заглавные латинские буквы (A–Z);
	  • строчные латинские буквы (a–z);
	  • цифры (0–9);
	  • символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

`/RESET`	Позволяет выключить функцию запроса пароля для подтверждения критических действий.
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

PATCHCOMPATIBILITYRESET. Удаление патча из списка несовместимых патчей

Команда `KAVSHELL PATCHCOMPATIBILITYRESET` позволяет удалить патч с указанным GUID из списка несовместимых патчей. Вы можете указать несколько GUID через пробел.

Синтаксис команды

```
KAVSHELL PATCHCOMPATIBILITYRESET <GUID> [GUID...]
```

Пример

```
KAVSHELL PATCHCOMPATIBILITYRESET 01234567-890A-BCDE-F012-34567890ABCD
```

PERFANALYZER. Экспорт результатов задачи Анализатор производительности

Команда `KAVSHELL PERFANALYZER` позволяет экспортировать результаты выполнения задачи *Анализатор производительности* в файл формата JSON.

Синтаксис команды

```
KAVSHELL PERFANALYZER /EXPORT:<path to destination directory> [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/EXPORT:<path to destination directory>`	Обязательный параметр. Укажите путь к папке, в которую приложение экспортирует файл с расширением .JSON
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL PERFANALYZER /EXPORT:C:\PerfAnalyzer
```

Коды возврата команды:

- 0 – команда выполнена успешно.
- -2 – служба не запущена.
- -4 – объект не найден.
- -5 – синтаксическая ошибка.
- -99 – неизвестная ошибка.

PREVENTION. Запрет запуска объектов

Команда `KAVSHELL PREVENTION` позволяет управлять запретом запуска объектов.

Синтаксис команды

```
KAVSHELL PREVENTION /SHOW | /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание

`/SHOW`	Обязательный параметр, если не задан параметр `/DISABLE`.
	Вывод текущих параметров запрета запуска объектов. В результате выполнения команды вы получите следующий ответ:
	`prevention.enabled=true|false`
	`prevention.mode=audit|prevent`
	`prevention.rules`
	`id: <rule ID>`
	`target: script|process|document`
	`md5: <MD5 hash of the file>`
	`sha256: <SHA256 hash of the file>`
	`pattern: <path to the object>`
	`case-sensitive: true|false`

`/DISABLE`	Обязательный параметр, если не задан параметр `/SHOW`. Выключение запрета запуска объектов.
`/PWD:<password>`	Обязательный параметр для команды `KAVSHELL PREVENTION /DISABLE`. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL PREVENTION /DISABLE /LOGIN:Admin /PWD:p@ssw0rd
```

Коды возврата команды:

- 0 – операция выполнена успешно.
- -3 – недостаточно прав для выполнения команды.

- -5 – синтаксическая ошибка.
- -6 – неверная операция (например, попытка выключить компонент, если компонент уже выключен).
- -7 – служба не зарегистрирована.
- -8 – автоматический запуск службы отключен.
- -9 – неудачная попытка запустить управляемое устройство под другой учетной записью.
- -99 – неизвестная ошибка.

REMOTEACCESS. Управление настройками удаленного подключения Консоли приложения

Команда `KAVSHELL REMOTEACCESS` позволяет управлять настройками удаленного подключения Консоли приложения к устройству с установленным Kaspersky Industrial CyberSecurity for Nodes.

Синтаксис команды

```
KAVSHELL REMOTEACCESS /SET /PORT=<new_port> [/PWD:<password>] [/LOGIN:<user name>] | /RESET UIKLPORT [/PWD:
<password>] [/LOGIN:<user name>] | /SHOW
```

Параметры команды

Параметр	Описание
`/SET [UIPORT | UIKLPORT]`	Настройка номера порта: • `UIPORT` – порт для подключения с учетными данными Windows. • `UIKLPORT` – порт для подключения с учетными данными вручную созданных пользователей.
`/PORT=<new_port>`	Обязательное значение, если передан параметр `/SET`. Номер порта. Диапазон возможных значений: 1–65535.
`/RESET UIKLPORT`	Закрыть порт для подключения с учетными данными вручную созданных пользователей.
`/SHOW`	Вывод текущих значений номеров портов.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL REMOTEACCESS /SET UIPORT /PORT=50000
KAVSHELL REMOTEACCESS /RESET UIKLPORT
KAVSHELL REMOTEACCESS /SHOW
```

RESETMDRMACHINEID. Сброс идентификатора устройства

Команда `KAVSHELL RESETMDRMACHINEID` позволяет сбросить идентификатор устройства, используемый решением Managed Detection and Response.

Синтаксис команды

```
KAVSHELL RESETMDRMACHINEID [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

RESTORE. Восстановление файлов

Команда `KAVSHELL RESTORE` позволяет восстанавливать файлы из резервного хранилища и карантина.

Синтаксис команды

```
KAVSHELL RESTORE <filename> [/REPLACE][/QUARANTINE][/BACKUP]/PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`<file name>`	Обязательный параметр. Полный путь к восстанавливаемому файлу.
`/REPLACE`	Необязательный параметр. Переписать существующий файл. Если параметр не передан, файл будет восстановлен только при отсутствии конфликта.
`/QUARANTINE`	Необязательный параметр. Восстановление файла из карантина.
`/BACKUP`	Необязательный параметр. Восстановление файла из резервного хранилища (значение по умолчанию).
`/PWD:<password>`	Обязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.

`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Синтаксис команды

```
KAVSHELL RESTORE /REPLACE C:\\eicar.com
KAVSHELL RESTORE /QUARANTINE C:\\test\eicar.com /PWD=1234 /LOGIN=user
```

Коды возврата команды:

- 0 – операция выполнена успешно.
- -3 – недостаточно прав для выполнения команды.
- -5 – синтаксическая ошибка.
- -6 – неверная операция.
- -7 – служба не зарегистрирована.
- -8 – автоматический запуск службы отключен.
- -9 – неудачная попытка запустить управляемое устройство под другой учетной записью.
- -99 – неизвестная ошибка.

ROLLBACK. Откат последнего обновления

Команда `KAVSHELL ROLLBACK` позволяет запустить задачу *Откат последнего обновления*.

Синтаксис команды

```
KAVSHELL ROLLBACK [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL ROLLBACK
```

Коды возврата команды:

- 0 – операция выполнена успешно.
- -2 – служба не запущена.
- -3 – недостаточно прав для выполнения команды.
- -99 – неизвестная ошибка.
- -221 – резервная копия баз не найдена.
- -222 – резервная копия баз повреждена.

RTP. Постоянная защита файлов

Команда `KAVSHELL RTP` позволяет включать и выключать компонент Постоянная защита файлов.

Синтаксис команды

```
KAVSHELL RTP </START|/STOP> [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`</START|/STOP>`	Включить или выключить компонент Постоянная защита файлов: • `/START` – включить компонент; • `/STOP` – выключить компонент.
`/PWD:<password>`	Обязательный параметр для команды `KAVSHELL RTP /STOP`. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL RTP STOP /PWD:p@ssw0rd
```

SCAN. Проверка по требованию

Команда `KAVSHELL SCAN` позволяет создавать и запускать задачу *Проверка по требованию*. Чтобы запустить из командной строки существующую задачу проверки по требованию, используйте команду `KAVSHELL TASK`.

Синтаксис команды

```
KAVSHELL SCAN <scan_scope> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<file_name>][/F<A|C|E>]
[/NEWONLY][/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|DELETE]
```

```
[/E:<ABMSPO>] [/EM:<"masks">] [/ES:<size>] [/ET:<s>][/TZOFF] [/NOICHECKER][/NOISWIFT][/NOCHECKMSSIGN]
[/ANALYSERLEVEL] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

Параметры команды

Параметр	Описание
`<scan_scope>`	Обязательный параметр. Список файлов, папок, сетевых путей или стандартных областей для сканирования через пробел. Стандартные области проверки: • `/MEMORY` – проверка всех процессов памяти; • `/SHARED` – проверка папок общего доступа папок; • `/STARTUP` – проверка объектов автозапуска; • `/REMDRIVES` – проверка всех съемных дисков; • `/FIXDRIVES` – проверка всех локальных жестких дисков; • `/MYCOMP` – проверка всего компьютера. Вы можете указать несколько значений через пробел.
`/L:<file_name>`	Необязательный параметр. Путь к файлу со списком областей сканирования. Файл должен быть создан вручную и сохранен в формате TXT. Файл должен быть сохранен в кодировке UTF-8 без BOM.
`/F<A|C|E>`	Необязательный параметр. Объекты, которые требуется включить в область проверки: • `/FA` – проверять все объекты. Приложение проверяет все файлы без исключения (любых форматов и расширений). • `/FC` – проверять объекты по формату. Приложение проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам. • `/FE` – проверять объекты по расширению. Приложение проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.
`/NEWONLY`	Необязательный параметр. Проверять только новые и измененные файлы. Если данный параметр не передан, Kaspersky Industrial CyberSecurity for Nodes будет проверять все объекты.
`/AI:` `<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>`	Необязательный параметр. Действие, которое приложение будет выполнять над зараженными и другими обнаруженными объектами: • `DISINFECT` – Лечить. Информировать, если лечение невозможно. • `DISINFDEL` – Лечить. Удалять, если лечение невозможно. • `DELETE` – Удалять. • `REPORT` (значение по умолчанию) – Информировать. • `AUTO` – Рекомендуемый.
`/AS:<QUARANTINE|DELETE|REPORT|AUTO>`	Необязательный параметр. Действие, которое приложение будет выполнять над возможно зараженными объектами: • `QUARANTINE` – Поместить на карантин. • `DELETE` – Удалять. • `REPORT` (значение по умолчанию) – Информировать. • `AUTO` – Рекомендуемый.

Параметр	Описание
`/E:<ABMSPO>`	Исключение указанных типов объектов. Допустимые значения параметра: • `A` – архивы ZIP, CAB, RAR, ARJ и других форматов; • `B` – файлы почтовых баз Microsoft Outlook и Microsoft Outlook Express; • `M` – файлы почтовых форматов, таких как сообщения Microsoft Outlook и Microsoft Outlook Express; • `S` – самораспаковывающиеся архивы; • `P` – исполняемые файлы, упакованные программами-упаковщиками двоичного кода, такими как UPX, ASPack и др; • `O` – встроенные в файлы объекты (таких как макросы Microsoft Word или вложения в сообщения электронной почты). Вы можете указать несколько значений.
`/EM=<file mask>`	Исключение из проверки файлов по маске. Например: • Маска *.exe будет включать все пути к файлам с расширением EXE. • Маска example* будет включать все пути к файлам с именем EXAMPLE.
`/ET=<scan duration in seconds>`	Исключение из проверки файлов, длительность проверки которых превышает установленное значение в секундах. Значение по умолчанию – 60 сек.
`/ES=<size in megabytes>`	Исключение из проверки файлов, размер которых превышает установленное значение в мегабайтах. Значение по умолчанию – 100 МБ.
`/TZOFF`	Не применять исключения Доверенной зоны.
`/NOICHECKER`	Отключение использование технологии iChecker (по умолчанию включено).
`/NOISWIFT`	Отключение использование технологии iSwift (по умолчанию включено).
`/NOCHECKMSSIGN`	Не проверять файлы, подписанные цифровой подписью Microsoft.
`/ANALYSERLEVEL`	Включить использование эвристического анализатора, настроить уровень анализа. Доступны следующие уровни эвристического анализа: • `1` – поверхностный; • `2` – средний; • `3` – глубокий. Если параметр не передан, приложение не будет использовать эвристический анализатор.
`/EXCLUDE=<list of exlusion`	Список файлов, папок или сетевых путей, которые будут исключены из области действия задачи проверки. Вы можете указать несколько значений через пробел.
`/W=<file path>`	Путь и имя файла журнала задачи. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.
`/ANSI`	Запись событий в журнал выполнения задачи в кодировке ANSI. Параметр `/ANSI` не будет применяться, если не передан параметр `/W`. Если параметр `/ANSI` не указан, то журнал выполнения задачи формируется в кодировке Unicode.
`/ALIAS:<alternate name>`	Присвоение задаче временного названия, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды `KAVSHELL TASK`. Альтернативное название задачи должно быть уникальным среди всех альтернативных названий задач приложения. Если этот параметр не задан, название задаче присваивается следующим образом: scan_<kavshell_pid>. Например: scan_1234.

Пример

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\003.exe "\\another server\Shared\"
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER
/NOISWIFT /W:log.log
KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

Коды возврата команды:

- 0 – операция выполнена успешно (угроз не обнаружено).
- 1 – операция отменена.
- -2 – служба не запущена.
- -3 – недостаточно прав для выполнения команды.
- -4 – объект не найден (не найден файл со списком областей проверки).
- -5 – синтаксическая ошибка или не определена область проверки.
- -80 – обнаружены зараженные объекты.
- -81 – обнаружены возможно зараженные объекты.
- -82 – во время проверки возникли ошибки обработки объектов.
- -83 – обнаружены непроверенные объекты.
- -84 – обнаружены поврежденные объекты.
- -85 – не удалось создать журнал выполнения задачи.
- -99 – неизвестная ошибка.
- -301 – лицензия недействительна.

SCAN-IOC. Поиск IOC

Команда `KAVSHELL SCAN-IOC` позволяет настраивать и запускать задачу *Поиск IOC*.

Синтаксис команды

```
KAVSHELL SCAN-IOC <full path to IOC file> [/PATH:<path to folder with IOC files>] [/PROCESS=no] [/HINT=<full path
to the executable file of the process|full path to file>]
[/REGISTRY=no] [/DNSENTRY=no] [/ARPENTRY=no] [/PORTS=no] [/SERVICES=no] [/SYSTEM=no] [/USERS=no] [/VOLUMES=no]
[/EVENTLOG=no] [/DATETIME=<event publication date>] [/CHANNELS=<list of channels>]
[/FILES=no] [/DRIVES=<all|system|critical|custom>] [/NETWORK=no] [/URL=no] [/EMAIL=no] [/ROUTE=no] [/RETRO]
[/DEPTH=<1-14>] [/EXCLUDES=<list of exclusions>] [/SCOPE=<configurable list of folders>]
```

Параметры команды

Параметры	Описание
`<full path to IOC file>`	Полный путь к IOC-файлу с расширением ioc или xml, по которому требуется выполнять поиск. Обязательный параметр, если не задан параметр `/PATH:<path to the folder with IOC files>`.
`/PATH:<path to the folder with IOC files>`	Путь к папке с IOC-файлами, по которым требуется выполнять поиск. Обязательный параметр, если не задан параметр `<full path to IOC file>`.

`/PROCESS=no`	Необязательный параметр. Параметр выключает анализ данных о процессах при проверке. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не учитывает запущенные на устройстве процессы при выполнении проверки. Если в IOC-файле указаны IOC-термины IOC-документа ProcessItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes проверяет данные о процессах, только если IOC-документ ProcessItem описан в переданном на проверку IOC-файле.
`/HINT=<full path to the executable file of the process|full path to the file>`	Необязательный параметр. Параметр позволяет сузить область анализируемых данных для проверки IOC-документов ProcessItem и FileItem, путем указания конкретного файла. В качестве значения параметра может быть задан: • `<full path to executable file of the process (ProcessItem)>` – ProcessItem • `<full path to file>` – FileItem Параметр может быть передан только совместно с аргументами `/PROCESS=yes` и `/FILES=yes`.
`/REGISTRY=no`	Необязательный параметр. Параметр выключает анализ разделов реестра (IOC-документ RegistryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не анализирует разделы реестра. Если в IOC-файле указаны термины IOC-документа RegistryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes анализирует реестр, только если IOC-документ RegistryItem описан в переданном на проверку IOC-файле.
`/DNSENTRY=no`	Необязательный параметр. Параметр выключает анализ данных о записях в локальном кеше DNS (IOC-документ DnsEntryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не проверяет локальный кеш DNS. Если в IOC-файле указаны термины IOC-документа DnsEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes проверяет локальный кеш DNS, только если IOC-документ DnsEntryItem описан в переданном на проверку IOC-файле.
`/ARPENTRY=no`	Необязательный параметр. Параметр выключает анализ данных о записях в ARP-таблице (документ ArpEntryItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не проверяет таблицу ARP. Если в IOC-файле указаны термины IOC-документа ArpEntryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes проверяет ARP-таблицу, только если IOC-документ ArpEntryItem описан в переданном на проверку IOC-файле.
`/PORTS=no`	Необязательный параметр. Параметр выключает анализ данных о портах, открытых на прослушивание (документ PortItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не проверяет таблицу активных соединений на устройстве. Если в IOC-файле указаны термины IOC-документа PortItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes проверяет таблицу активных соединений, только если IOC-документ PortItem описан в переданном на проверку IOC-файле.

`/SERVICES=no`	Необязательный параметр. Параметр выключает анализ данных о службах, установленных на устройстве (документ ServiceItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не проверяет данные о службах, установленных на устройстве. Если в IOC-файле указаны термины IOC-документа ServiceItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes проверяет данные о службах, только если IOC-документ ServiceItem описан в переданном на проверку IOC-файле.
`/SYSTEM=no`	Необязательный параметр. Параметр выключает анализ данных об окружении (IOC-документ SystemInfoItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не анализирует данные об окружении. Если в IOC-файле указаны термины IOC-документа SystemInfoItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes анализирует данные об окружении, только если IOC-документ SystemInfoItem описан в переданном на проверку IOC-файле.
`/USERS=no`	Необязательный параметр. Параметр выключает анализ данных о пользователях (IOC-документ UserItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не анализирует данные о пользователях, созданных в системе. Если в IOC-файле указаны термины IOC-документа UserItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes анализирует данные о пользователях, созданных в системе, только если IOC-документ UserItem описан в переданном на проверку IOC-файле.
`/VOLUMES=no`	Необязательный параметр. Параметр выключает анализ данных о томах (документ VolumeItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не проверяет данные о томах на устройстве. Если в IOC-файле указаны термины IOC-документа VolumeItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes проверяет данные о томах, только если IOC-документ VolumeItem описан в переданном на проверку IOC-файле.
`/EVENTLOG=no`	Необязательный параметр. Параметр выключает анализ данных о записях в журнале событий Windows (документ EventLogItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не проверяет записи в журнале событий Windows. Если в IOC-файле указаны термины IOC-документа EventLogItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes проверяет записи в журнале событий Windows, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле. При указании значения IOC-термина EventLogItem\source вам необходимо использовать значение параметра Provider Name из XML-схемы события.

`/DATETIME=<event publication date>`	Необязательный параметр. Параметр позволяет включать и выключать учет даты публикации события в журнале событий Windows при определении области поиска IOC для соответствующего IOC-документа. При поиске IOC Kaspersky Industrial CyberSecurity for Nodes будет обрабатывать только события, опубликованные в период с указанного времени и даты и до момента выполнения задачи. В качестве значения параметра Kaspersky Industrial CyberSecurity for Nodes позволяет задать дату публикации события. Проверка будет выполняться только для событий, опубликованных в журнале событий Windows после указанной даты и до момента выполнения проверки. Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes проверяет события с любой датой публикации. Параметр используется, только если IOC-документ EventLogItem описан в переданном на проверку IOC-файле.
`/CHANNELS=<list of channels>`	Необязательный параметр. Параметр позволяет передать список имен каналов (журналов), для которых требуется выполнить поиск IOC. Если этот параметр передан, при выполнении задачи поиска IOC Kaspersky Industrial CyberSecurity for Nodes будет учитывать только события, опубликованные в указанных журналах. Имя журнала задается в формате строки, в соответствии с именем журнала (канала), указанного в свойствах этого журнала (параметр Full Name) или в свойствах события (параметр <Channel></Channel> в xml-схеме события). По умолчанию (в том числе, если параметр не передан) поиск IOC выполняется для каналов Application, System, Security. Параметру может быть передано несколько значений (через пробел). Параметр используется только в том случае, если IOC-документ EventLogItem описан в переданном на проверку IOC.
`/FILES=no`	Необязательный параметр. Параметр выключает анализ данных о файлах (IOC-документ FileItem) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не анализирует данные о файлах. Если в IOC-файле указаны термины IOC-документа FileItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes анализирует данные о файлах, только если IOC-документ FileItem описан в переданном на проверку IOC-файле.
`/DRIVES=<all|system|critical|custom>`	Необязательный параметр. Параметр позволяет задать область поиска IOC при анализе данных для IOC-документа FileItem. Можно задать одно из следующих значений параметра: • `all` – программа проверяет все доступные файловые области. • `system` – программа проверяет только файлы, расположенные в папках, в которых установлена ОС. • `critical` – программа проверяет только временные файлы в пользовательских и системных папках. • `custom` – программа проверяет только файлы в указанных пользователем областях. Если параметр не передан, проверка выполняется в критических областях.
`/NETWORK=no`	Необязательный параметр. Параметр выключает поиск угроз на основе IOC-документа Network при поиске IOC. Если параметр передан со значением <no>, Kaspersky Industrial CyberSecurity for Nodes не выполняет поиск угроз на основе IOC-документа Network. Если в IOC-файле указаны термины IOC-документа Network, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes включает поиск угроз на основе IOC-документа Network, только если IOC-документ Network описан в переданном на проверку IOC-файле.

`/URL=no`	Необязательный параметр. Параметр выключает поиск угроз на основе IOC-документа UrlHistoryItem при поиске IOC. Если параметр передан со значением <no>, Kaspersky Industrial CyberSecurity for Nodes не выполняет поиск угроз на основе IOC-документа UrlHistoryItem. Если в IOC-файле указаны термины IOC-документа UrlHistoryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes включает поиск угроз на основе IOC-документа UrlHistoryItem, только если IOC-документ UrlHistoryItem описан в переданном на проверку IOC-файле.
`/EMAIL=no`	Необязательный параметр. Параметр выключает анализ почтовых объектов (IOC-документ Email) при поиске IOC. Если параметр передан со значением `<no>`, Kaspersky Industrial CyberSecurity for Nodes не анализирует почтовые объекты. Если в IOC-файле указаны термины IOC-документа Email, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes анализирует почтовые объекты, только если IOC-документ Email описан в переданном на проверку IOC-файле.
`/ROUTE=no`	Необязательный параметр. Параметр включает поиск угроз на основе IOC-документа RouteEntryItem при поиске IOC. Если параметр передан со значением <no>, Kaspersky Industrial CyberSecurity for Nodes не выполняет поиск угроз на основе IOC-документа RouteEntryItem. Если в IOC-файле указаны термины IOC-документа UrlHistoryItem, они игнорируются (определяются как отсутствие совпадения). Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes включает поиск угроз на основе IOC-документа RouteEntryItem, только если IOC-документ RouteEntryItem описан в переданном на проверку IOC-файле.
`/RETRO`	Необязательный параметр. Параметр передается для запуска задачи в режиме *Ретроспективный поиск IOC*. Дополнительно с этим параметром можно передать временной интервал, в рамках которого программа должна выполнять ретроспективный поиск IOC, при помощи параметра `/DEPTH=<interval in days>`. Максимальное значение – 14 дней. Время отсчитывается начиная с момента запуска задачи. Пример: `KAVSHELL SCAN-IOC /PATH=<path to a folder with IOC files> /RETRO /DEPTH=2` Если временной интервал не передан, то используется значение по умолчанию – 1 день.
`/EXCLUDES=<list of exclusions>`	Необязательный параметр. Параметр позволяет задать области исключений при анализе данных для IOC-документа FileItem. В параметре можно передать несколько путей через пробел. Если параметр не передан, проверка выполняется без исключений.
`/SCOPE=<configurable list of folders>`	Необязательный параметр. Параметр становится обязательным, если передан параметр `/DRIVES=custom`. Параметр позволяет задать список областей проверки. В параметре можно передать несколько путей через пробел.

Если команда была выполнена успешно (код `0`) и в процессе выполнения были обнаружены индикаторы компрометации, Kaspersky Industrial CyberSecurity for Nodes выводит в командную строку следующие данные о результатах выполнения задачи:

Данные, которые приложение выводит в командную строку при обнаружении IOC

`Uuid`	Идентификатор IOC-файла из заголовка структуры IOC-файла (тег `<ioc id="">`)
`Name`	Описание IOC-файла из заголовка структуры IOC-файла (тег `<description></description>`)
`Matched Indicator Items`	Перечень идентификаторов всех сработавших индикаторов.
`Matched objects`	Данные о каждом документе IOC, в котором было найдено совпадение.
`Date`	Дата создания файла, в котором обнаружены индикаторы компрометации.
`Created`	Только для FileItem. Время создания объекта, в котором обнаружены индикаторы компрометации.

`Pid`	Идентификатор процесса, для которого обнаружены индикаторы компрометации.
`Upid`	Уникальный идентификатор процесса, для которого обнаружены индикаторы компрометации.
`ParentPid`	Идентификатор родительского объекта, содержащего процесс, для которого обнаружены индикаторы компрометации.
`Username`	Имя пользователя, который вносил изменения в объект сканирования.
`StartTime`	Время запуска процесса, для которого обнаружены индикаторы компрометации.

SCAN-OVAL. Аудит безопасности

Команда `KAVSHELL SCAN-OVAL` позволяет настраивать и запускать задачу *Аудит безопасности*. Вы можете настраивать и запускать задачу аудита безопасности через интерфейс командной строки для следующих источников правил:

- **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП**;
- **Конфигурации безопасности и соответствий стандартам для операционных систем**;
- **Пользовательская база правил из файла**.

Синтаксис команды

```
KAVSHELL SCAN-OVAL [/SOURCE:<kl|kl-compl|file>] [/REPOSITORY:show] [/PATH:<full path to the folder>] [/EXTERNAL-VARS:<full path and name of ZIP archive with external variables>] [/MODE:<all|exclude|include>] [/DEFINITIONS:<vuln_type_01;...;vuln_type_N>] /RESULT-PATH:<path to the folder with the report> [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/SOURCE:<kl|kl-compl|file>`	Необязательный параметр. Источник правил, которые необходимы для аудита безопасности: • `kl` – база данных уязвимостей Kaspersky ICS CERT для АСУ ТП, входящая в поставку. Доступна для обращения через командную строку после успешного обновления баз и модулей Kaspersky Industrial CyberSecurity for Nodes. • `kl-compl` – конфигурации безопасности и соответствий стандартам для операционных систем, входящие в поставку. Доступны для обращения через командную строку после успешного обновления баз и модулей Kaspersky Industrial CyberSecurity for Nodes. • `file` – пользовательская база правил из файла. Если значение параметра не указано, по умолчанию используется источник **База данных уязвимостей Kaspersky ICS CERT для АСУ ТП** (`/SOURCE=kl`).
`/REPOSITORY:show`	Необязательный параметр. Параметр доступен, если в качестве источника правил выбраны конфигурации безопасности и соответствия стандартам для операционных систем (`/SOURCE=kl-compl`). Если параметр указан, то вместо выполнения задачи аудита безопасности Kaspersky Industrial CyberSecurity for Nodes сохраняет в папку отчета (определяется параметром `/RESULT-PATH`) XML-файл, в котором перечислены названия имеющихся конфигураций безопасности.
`/PATH:<full path to the folder>`	Необязательный параметр. Параметр указывает полный путь к архиву с XML-файлом, содержащим OVAL-правила, или к архиву с XML-файлами с OVAL- и XCCDF-правилами для источников **Конфигурации безопасности и соответствий стандартам для операционных систем** (`/SOURCE=kl-compl`) и **Пользовательская база правил из файла** (`/SOURCE=file`). OVAL- и XCCDF-правила должны быть сохранены в кодировке UTF-8 без BOM.

`/EXTERNAL-VARS:<full path and name of ZIP archive with external variables>`	Необязательный параметр. Параметр указывает полный путь и имя ZIP-архива с XML-файлом, содержащим внешние переменные для OVAL-правил. Параметр доступен, если источник содержит только OVAL-правила.
`/MODE:<all|exclude|include>`	Необязательный параметр. Параметр определяет режим проверки на уязвимости. Параметр доступен, если источник содержит только OVAL-правила. Доступные значения параметра: • `all` – выполняется проверка на все уязвимости, указанные в источнике. • `exclude` – выполняется проверка на уязвимости, указанные в источнике, кроме указанных с помощью параметра `/definitions`. • `include` – выполняется проверка на уязвимости, которые указаны с помощью параметра `/definitions`. Если значение параметра не задано, по умолчанию используется режим `all`.
`/DEFINITIONS:<vuln_type_01;...;vuln_type_N>`	Необязательный параметр. Параметр определяет список типов уязвимостей, разделенных точкой с запятой, которые необходимо проверить или исключить из проверки. Параметр доступен, если источник содержит только OVAL-правила. Например: `oval:org.mitre.oval.test:def:998;oval:org.mitre.oval.test:def:999`. Используется совместно с параметром `/MODE=include` или `/MODE=exclude`.
`/RESULT-PATH`	Обязательный параметр. Параметр указывает путь к папке, куда будет записан отчет сканирования в формате XML. Имя файла содержит имя узла, дату и время выполнения задачи. Если параметр не задан, выполнение задачи завершается с ошибкой.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL SCAN-OVAL /SOURCE:kl /RESULT-PATH:c:\storage\reports
KAVSHELL SCAN-OVAL /SOURCE:kl-comp /REPOSITORY:show /RESULT-PATH:c:\storage\reports
```

SCANCRITICAL. Проверка важных областей

Команда `KAVSHELL SCANCRITICAL` позволяет запускать задачу *Проверка важных областей*.

Синтаксис команды

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>] [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/W`	Необязательный параметр. Укажите имя файла с расширением .LOG для экспорта журнала выполнения. Также вы можете указать путь к файлу. Если в команде указано только имя файла, приложение выполнит попытку разместить файл в папке установки приложения. Если механизмы самозащиты приложения включены, экспорт завершится с ошибкой, так как самозащита приложения заблокирует создание нового файла в папке приложения. Для экспорта журнала укажите путь к файлу.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

SERVERBINDINGDISABLE. Выключение защиты подключения к Серверу администрирования

Команда `KAVSHELL SERVERBINDINGDISABLE` предназначена для локального выключения защиты подключения к Серверу администрирования. Команда запускает задачу *Защита подключения к Серверу администрирования*, которая удаляет пароль для подключения компьютера к Серверу администрирования.

Синтаксис команды

```
KAVSHELL SERVERBINDINGDISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

SIEM. Интеграция с SIEM-системами

Команда `KAVSHELL SIEM` позволяет настраивать параметры интеграции с SIEM-системами для отправки телеметрии

Синтаксис команды

```
KAVSHELL SIEM /ENABLE /TLS /SERVERS=<protocol://server:port;protocol://server:port...> /TIMEOUT=<seconds> /PWD:
<password> /LOGIN:<user name> /PINNED-CERTIFICATE=<path> /CLIENT-CERTIFICATE=<path> /CLIENT-PASSWORD=<password>
/MAXIMUM-DATA-TRANSFER-TIME=<seconds> | /DISABLE | /SHOW
```

Параметры команды

Параметр	Описание
`/<ENABLE|DISABLE|SHOW>`	Обязательный параметр. Включение, выключение или просмотр настроек компонента Интеграция с SIEM.
`/TLS`	Необязательный параметр. Включение шифрования соединения между Kaspersky Industrial CyberSecurity for Nodes и серверами SIEM.
`/SERVERS=<protocol://server:port;protocol://server:port...>`	Обязательный параметр. Позволяет указать адрес и порт сервера. Диапазон возможных значений порта: 1–65535.
`/TIMEOUT=<seconds>`	Необязательный параметр. Максимальное время ожидания ответа от сервера SIEM в секундах. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию – 30 сек.
`/PINNED-CERTIFICATE=<path>`	Обязательный параметр, если передан параметр `/TLS`. TLS-сертификат для установки доверенного соединения Kaspersky Industrial CyberSecurity for Nodes с сервером SIEM.
`/CLIENT-CERTIFICATE=<path>`	Необязательный параметр. Позволяет добавить *криптоконтейнер* – файл формата PFX, в котором в зашифрованном виде хранится клиентский сертификат для защиты соединения Kaspersky Industrial CyberSecurity for Nodes с сервером SIEM.
`/CLIENT-PASSWORD=<password>`	Обязательный параметр, если передан параметр `/CLIENT-CERTIFICATE`. Позволяет указать пароль для доступа к криптоконтейнеру.
`/MAXIMUM-DATA-TRANSFER-TIME=<seconds>`	Максимальное время ожидания ответа от сервера SIEM в секундах. По истечении указанного времени Kaspersky Industrial CyberSecurity for Nodes повторно пробует подключиться к тому же серверу или подключается к следующему в списке серверу, если их несколько. Диапазон доступных значений: 1–3600 сек. Значение по умолчанию 5 секунд.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.

`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL SIEM /ENABLE /SERVERS="tcp://server1:1234;udp://server2:5678;http://server3:9012" /TIMEOUT=10 /MAXIMUM-DATA-TRANSFER-TIME=20"
KAVSHELL SIEM /DISABLE
KAVSHELL SIEM /SHOW
```

SIGMA. Обнаружение аномалий с помощью Sigma-правил

Команда `KAVSHELL SIGMA` позволяет управлять компонентом Обнаружение аномалий с помощью Sigma-правил.

Синтаксис команды

```
KAVSHELL SIGMA /<ENABLE|DISABLE|ADD|REMOVE|SHOW> [/COLLECTION:<rat|deltav|uac|siemens|yokogawa|nfta|custom>] [/NAME:<collection name>] [/SOURCE:<full path to the folder with the YAML files>] [/PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/<ENABLE|DISABLE|ADD|REMOVE|SHOW>`	Обязательный параметр. Указывает на одно из следующих действий: • `ENABLE` – включить обнаружение аномалий с помощью Sigma-правил; • `DISABLE` – выключить обнаружение аномалий с помощью Sigma-правил; • `ADD` – добавить коллекцию Sigma-правил; • `REMOVE` – удалить коллекцию Sigma-правил; • `SHOW` – отобразить текущие параметры обнаружения аномалий с помощью Sigma-правил.
`/COLLECTION:` `<rat|deltav|uac|siemens|yokogawa|nfta|custom>`	Параметр обязателен, если указано `SIGMA /<ADD|REMOVE>`. Указывает коллекцию Sigma-правил, которую нужно добавить или удалить: • `rat` – Обнаружение средств удаленного администрирования (RAT); • `deltaV` – Обнаружение аномалий для Emerson DeltaV; • `uac` – Контроль учетных записей пользователей (UAC); • `siemens` – Обнаружение аномалий для Siemens SIMATIC WinCC, Siemens TIA Portal, Siemens SIMATIC STEP 7; • `yokogawa` – Обнаружение аномалий для Yokogawa CENTUM VP; • `nfta` – Аудит обмена файлами по сети и через съемные носители; • `custom` – Коллекция пользовательских правил. Возможно также указать `test`. Будет добавлено или удалено одно правило, предназначенное для внутреннего тестирования в АО "Лаборатория Касперского".
`/NAME:<collection name>`	Параметр обязателен, если указано `SIGMA /<ADD|REMOVE>` и `/COLLECTION:custom`. Указывает имя коллекции пользовательских Sigma-правил.

Параметр	Описание
`/SOURCE:<full path to the folder with the YAML files>`	Параметр обязателен, если указано `SIGMA /ADD` и `/COLLECTION:custom`. Указывает полный путь к папке с YAML-файлами, в которых описаны пользовательские Sigma-правила.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL SIGMA /ENABLE
KAVSHELL SIGMA /ADD /COLLECTION:deltav
KAVSHELL SIGMA /REMOVE /COLLECTION:custom /NAME:rules.yaml
```

START. Запуск службы приложения

Команда `KAVSHELL START` позволяет запустить службу Kaspersky Industrial CyberSecurity for Nodes Service.

Синтаксис команды

```
KAVSHELL START
```

STARTPOLICY. Включение политики

Команда `KAVSHELL STARTPOLICY` позволяет включить политику Kaspersky Security Center на защищаемом устройстве. Параметры приложения будут настроены в соответствии с политикой.

Синтаксис команды

```
KAVSHELL STARTPOLICY
```

STOP. Остановка службы приложения

Команда `KAVSHELL STOP` позволяет остановить службу Kaspersky Industrial CyberSecurity for Nodes Service.

Синтаксис команды

```
KAVSHELL STOP [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Коды возврата команды:

- 0 – операция выполнена успешно.
- -3 – недостаточно прав для выполнения команды.
- -5 – синтаксическая ошибка.
- -6 – неверная операция (служба Kaspersky Industrial CyberSecurity for Nodes Service уже остановлена).
- -7 – служба не зарегистрирована.
- -8 – автоматический запуск службы отключен.
- -9 – неудачная попытка запустить управляемое устройство под другой учетной записью.
- -99 – неизвестная ошибка.

TASK. Управление задачами

Команда `KAVSHELL TASK` позволяет управлять задачами Kaspersky Industrial CyberSecurity for Nodes: запускать, приостанавливать, возобновлять и останавливать задачу, а также просматривать ее текущее состояние и статистику.

Синтаксис команды

```
KAVSHELL TASK [<alternative name> </START | /STOP | /STATE | /STATISTICS>] /PWD:<password> [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
Без параметров	Возврат списка всех существующих задач Kaspersky Industrial CyberSecurity for Nodes. Список содержит следующие поля: альтернативное название задачи (дополнительное сокращенное название, которое Kaspersky Industrial CyberSecurity for Nodes для Windows присваивает задачам), категория задачи (системная или пользовательская) и текущий статус задачи.
`<alternative name>`	Альтернативное название задачи, которой вы хотите управлять. Чтобы просмотреть альтернативные названия задач Kaspersky Industrial CyberSecurity for Nodes, введите команду `KAVSHELL TASK` без параметров.
`/START`	Запуск задачи.
`/STOP`	Остановка задачи.
`/STATE`	Вывод текущего состояния задачи.
`/STATISTICS`	Вывод статистики выполнения задачи.

`/PWD:<password>`	Обязательный параметр для команды `KAVSHELL TASK /STOP`. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Синтаксис команды

```
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-critical /STATE
```

Коды возврата команды:

- 0 – операция выполнена успешно.
- -2 – служба не запущена.
- -3 – недостаточно прав для выполнения команды.
- -4 – объект не найден (задача не найдена).
- -5 – синтаксическая ошибка или не определена область проверки.
- -6 – неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена).
- -99 – неизвестная ошибка.
- -301 – лицензия недействительна.
- 401 – задача не запущена (для команды `KAVSHELL TASK <task name> /STATE`).
- 402 – задача уже запущена (для команды `KAVSHELL TASK <task name> /STATE`).
- 403 – задача уже приостановлена (для команды `KAVSHELL TASK <task name> /STATE`).
- -404 – сбой выполнения операции (изменение состояния задачи привело к сбою).

TELEMETRYFILTERS. Экспорт и импорт правил фильтрации событий телеметрии

Команда `KAVSHELL TELEMETRYFILTERS` позволяет экспортировать и импортировать правила фильтрации событий телеметрии.

Синтаксис команды

```
KAVSHELL TELEMETRYFILTERS [/IMPORT /EXPORT] <file_path> [/PWD:<password>] [/LOGIN:<user name>]
```

Параметры команды

Параметр	Описание
`/IMPORT <file_path>`	Обязательный параметр, если не передан параметр `/EXPORT`. Импорт правил фильтрации событий телеметрии из файла. Укажите полный путь к JSON-файлу с правилами, включая его имя и расширение. Если на компьютере уже есть правила фильтрации событий, Kaspersky Industrial CyberSecurity for Nodes заменит их при импорте.
`/EXPORT <file_path>`	Обязательный параметр, если не передан параметр `/IMPORT`. Экспорт правил фильтрации событий телеметрии в файл формата JSON. • Если в команде указано только имя файла, приложение выполнит попытку разместить файл в папке установки приложения. Если механизмы самозащиты приложения включены, экспорт завершится с ошибкой, так как самозащита приложения заблокирует создание нового файла в папке приложения. Для экспорта правил укажите путь к файлу.
`/PWD: <password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL TELEMETRYFILTERS /IMPORT "C:\some\folder\telemetry_filers.json" /LOGIN:Admin /PWD:p@ssw0rd
```

TOKEN. Управление блокировкой доступа к защищенным съемным дискам

Команда `KAVSHELL TOKEN` позволяет управлять блокировкой доступа к защищенным съемным дискам, а также просматривать информацию о подключенных к устройству защищенных съемных дисках.

Синтаксис команды

```
KAVSHELL TOKEN [/ENUMERATE | /PROTECTION:<status|enable|disable>]
```

Параметры команды

Параметр	Описание
`/ENUMERATE`	Вывод списка подключенных защищенных съемных дисков.
`/PROTECTION:<status|enable|disable>]`	Управление блокировкой доступа к защищенным съемным дискам: • `status` – отображение текущего статуса защиты. • `enable` – включение защиты. • `disable` – отключение защиты.

Пример

```
KAVSHELL TOKEN /ENUMERATE
KAVSHELL TOKEN /PROTECTION:status
KAVSHELL TOKEN /PROTECTION:enable
KAVSHELL TOKEN /PROTECTION:disable
```

TRACE. Трассировка работы приложения

Команда `KAVSHELL TRACE` позволяет включать и выключать трассировку работы приложения.

Синтаксис команды

```
KAVSHELL TRACE </ON /F:<traces_folder:>[/S:<traces_size_in_MB>] [/LVL:<debug|info|warning|error|critical>] /R:<max trace files to rotate> | /OFF > [/LOGIN:<user name>] [/PWD:<password>]
```

Параметры команды

Параметр	Описание
`</ON | /OFF>`	Обязательный параметр. Включить или выключить трассировку работы приложения.
`/F:<traces_folder>`	Обязательный параметр, если передан параметр `/ON`. Путь к папке, в которой будут сохраняться файлы трассировки.
`/S:<traces_size_in_MB>`	Необязательный параметр. Максимальный размер файла трассировки в МБ. Доступные значения: от 1 до 4095 МБ. Значение по умолчанию – 100 МБ.
`/LVL: <debug|info|warning|error|critical>`	Необязательный параметр. Уровень детализации отладочной информации. • `critical` – в файле трассировки сохраняются только сообщения о неустранимых ошибках. • `error` – в файле трассировки сохраняются сообщения обо всех ошибках, а также предупреждения. • `warning` – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждения, а также дополнительная информация. • `info` (значение по умолчанию) – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждениях, а также информация о работе приложения в нормальном режиме. • `debug` – в файле трассировки сохраняется вся информация о работе приложения.
`/R:<max trace files to rotate>`	Необязательный параметр. Максимальное количество файлов трассировки в журнале. Доступные значения: от 1 до 999. Значение по умолчанию – 5.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:info /R:50 /PWD:p@ssw0rd
KAVSHELL TRACE /OFF
```

UPDATE. Обновление баз и модулей приложения

Команда `KAVSHELL UPDATE` позволяет управлять задачей *Обновление*.

Синтаксис команды

```
KAVSHELL UPDATE <update_source | /AK | /KL> [/NOUSEKL] [/PROXY:<IP address>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:
<user_name>] [/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE]
[/TIMEOUT:<s>] [/REG:<code_by_iso3166>] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

Параметры команды

Параметр	Описание
`<update_source | /AK | /KL>`	Обязательный параметр. Выбор источника обновлений: • `<update_source>` – использовать пользовательские источники обновления. Вы можете указать путь к папке на защищаемом устройстве, путь к сетевой папке в формате UNC или адрес HTTP- или FTP-сервера, на котором располагается папка с обновлениями. • `/AK` – использовать Сервер администрирования Kaspersky Security Center в качестве источника обновлений. • `/KL` – использовать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений. Вы можете указать несколько значений через пробел.
`/NOUSEKL`	Необязательный параметр. Не использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны (значение по умолчанию).
`/PROXY:<IP address>:<port>`	Необязательный параметр. IP-адрес или символьное имя прокси-сервера и номер порта.
`/AUTHTYPE:<0-2>`	Необязательный параметр. Тип аутентификации на прокси-сервере: • `0` – NTLM-аутентификация с помощью учетной записи текущего пользователя. • `1` – NTLM-аутентификация с помощью учетной записи, имя пользователя и пароль которой заданы параметрами `/PROXYUSER` и `/PROXYPWD`. • `2` – аутентификация с помощью имени пользователя и пароля, заданными параметрами `/PROXYUSER` и `/PROXYPWD`.
`/PROXYUSER:<user_name>`	Обязательный параметр, если переданы параметры `/AUTHTYPE:1` или `/AUTHTYPE:2`. Имя пользователя, используемое для доступа к прокси-серверу. Если указано значение `/AUTHTYPE:0`, то параметры `/PROXYUSER:<user_name>` и `/PROXYPWD:<password>` игнорируются.
`/PROXYPWD:<password>`	Обязательный параметр, если переданы параметры `/AUTHTYPE:1` или `/AUTHTYPE:2`. Пароль пользователя, используемый для доступа к прокси-серверу. Если указано значение `/AUTHTYPE:0`, то параметры `/PROXYUSER:<user_name>` и `/PROXYPWD:<password>` игнорируются. Если указан параметр `/PROXYUSER`, но не указан параметр `/PROXYPWD`, считается, что задан пустой пароль.
`/NOPROXYFORKL`	Необязательный параметр. Не использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского".
`/USEPROXYFORCUSTOM`	Необязательный параметр. Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений.
`/USEPROXYFORLOCAL`	Необязательный параметр. Использовать параметры прокси-сервера для соединения с локальными источниками обновлений.
`/NOFTPPASSIVE`	Необязательный параметр. Если этот параметр передан, Kaspersky Industrial CyberSecurity for Nodes использует активный режим соединения с FTP-сервером. Если параметр не передан, Kaspersky Industrial CyberSecurity for Nodes использует пассивный режим соединения, если это возможно.

`/TIMEOUT:<s>`	Необязательный параметр. Время ожидания при соединении с FTP- или HTTP-сервером в секундах. Значение по умолчанию: 10 секунд.
`/REG:<code_by_iso3166>`	Необязательный параметр. Код страны, в которой расположено защищаемое устройство, в соответствии со стандартом ISO 3166-1. Пример: `/REG:GR`. Если параметр не указан или указан недопустимый код страны, Kaspersky Industrial CyberSecurity for Nodes определяет местоположение в соответствии с региональными параметрами защищаемого устройства, на котором установлена Консоль приложения. Приложение использует информацию о местоположении при выборе сервера обновлений.
`/W=<file path>`	Путь и имя файла журнала задачи. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала.
`/ANSI`	Запись событий в журнал выполнения задачи в кодировке ANSI. Параметр `/ANSI` не будет применяться, если не передан параметр `/W`. Если параметр `/ANSI` не указан, то журнал выполнения задачи формируется в кодировке Unicode.
`/ALIAS:<alternate name>`	Присвоение задаче временного названия, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды `KAVSHELL TASK`. Альтернативное название задачи должно быть уникальным среди всех альтернативных названий задач приложения. Если этот параметр не задан, название задаче присваивается следующим образом: update_<kavshell_pid>. Например: update_1234.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Синтаксис команды

```
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /USEPROXYFORCUSTOM /PROXY:proxy.company.com:8080
/AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd /TIMEOUT:100 /REG:ru /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /NOUSEKL /USEPROXYFORCUSTOM
/PROXY:proxy.company.com:8080 /AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
KAVSHELL UPDATE /AK /NOUSEKL
KAVSHELL UPDATE /KL /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE /AK /W:"C:\KAVREPORTS\daily update.log"
```

Коды возврата команды:

- 0 – операция выполнена успешно.
- 200 – все объекты актуальны.
- -2 – служба не запущена.
- -3 – недостаточно прав для выполнения команды.
- -5 – синтаксическая ошибка.
- -99 – неизвестная ошибка.
- -206 – файлы обновлений отсутствуют в указанном источнике или имеют неизвестный формат.
- -209 – ошибка подключения к источнику обновлений.

- -232 – ошибка аутентификации при подключении к прокси-серверу.
- -234 – ошибка подключения к Kaspersky Security Center.
- -235 – Kaspersky Industrial CyberSecurity for Nodes не прошел проверку подлинности при соединении с источником обновлений.
- -236 – базы приложения повреждены.
- -301 – лицензия недействительна.

YARA. Запуск YARA-проверки

Команда `KAVSHELL YARA` позволяет запустить YARA-проверку.

Синтаксис команды

```
KAVSHELL YARA <full path to a YARA file> | /PATH=<path to a folder with YARA files> [<additional arguments>]
```

Параметры команды

Обязательный параметр	Описание
`<full path to a YARA file>`	Полный путь к YARA-файлу, по которому требуется выполнить поиск. Вы можете указать пути к нескольким YARA-файлам через пробел. Обязательный параметр, если не передан параметр `/PATH`. Пример: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/PATH=<path to a folder with YARA files>`	Полный путь к папке с YARA-файлами, по которым требуется выполнить поиск. Обязательный параметр, если не передан параметр `<full path to a YARA file>`. Пример: `/PATH=C:\Users\Admin\Desktop\YARA`
`/FASTSCAN=<on|off>`	Необязательный параметр. Быстрая YARA-проверка. Для каждого объекта приложение фиксирует в журнале одно вхождение обнаруженного маркера. При этом приложение скрывает дубликаты обнаруженных маркеров в журнале. Быстрая YARA-проверка позволяет сократить время проверки больших файлов. Если параметр не задан, приложение выполняет стандартную YARA-проверку. В этом режиме приложение отображает дубликаты обнаруженных маркеров в журнале.
`/MAXRULES=<maximum number of scan rules>`	Необязательный параметр. Ограничение количества уникальных сработавших правил, при превышении которого приложение прекращает YARA-проверку. Если значение параметра не задано или равно `0`, приложение выполняет YARA-проверку без ограничений.
`/TIMEOUT=<N seconds>`	Необязательный параметр. Ограничение длительности YARA-проверки в секундах. По истечении указанного времени приложение останавливает YARA-проверку. Если значение параметра не задано или равно `0`, приложение выполняет YARA-проверку без ограничений.
`/RECURSIVE=<on|off>`	Необязательный параметр. Параметр запускает рекурсивную проверку вложенных папок в рамках выборочной проверки (`/SCANFOLDERS`).

`/SCANFOLDERS=<path to folders for the YARA scan>`	Необязательный параметр. Параметр запускает YARA-проверку файлов по указанному списку папок. Вы можете указать несколько значений через пробел. Kaspersky Industrial CyberSecurity for Nodes поддерживает символы `*` и `?` для ввода маски пути к папке. Если значение параметра не задано, приложение выполняет YARA-проверку на всех локальных дисках, кроме сетевых, облачных и подключаемых дисков.
`/SCANMEMORY=<on|off>`	Необязательный параметр. Проверка памяти всех запущенных процессов.
`/SCANPROCESS=<full paths to executable files of processes>`	Необязательный параметр. Проверка памяти только для указанных процессов. Необходимо через пробел указать пути к исполняемым файлам процессов вместе с названиями файлов. Вы можете также использовать символы `*` и `?` для ввода маски.
`/MAXSIZE=<size in bytes>`	Необязательный параметр. Ограничение размера файлов для YARA-проверки. Приложение пропускает файлы большего размера.
`/INCLUDES=<list of objects for the YARA scan>`	Необязательный параметр. Формирование области проверки. Вы можете указать несколько значений через пробел. Доступны следующие значения: • имя файла; • маска имени файла. Область проверки необходимо задавать с параметром `/SCANFOLDERS`. Пример: `/SCANFOLDERS C:\*.* /includes=*.exe *.dll` – приложение проверит все файлы с расширением .EXE и .DLL на диске C.
`/EXCLUDES=<paths to objects to be excluded from the YARA scan>`	Необязательный параметр. Исключение файлов из YARA-проверки. Вы можете указать несколько значений через пробел. Доступны следующие значения: • путь к файлу; • маска пути к файлу. Исключения необходимо задавать с параметром `/SCANFOLDERS`. Пример: `/SCANFOLDERS C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – приложение пропускает файл readme.txt, все файлы из папки C:\trusted, а также все файлы с расширением .XML в корневой папке на диске C.
`/SCANAUTORUNS=<on|off>`	Необязательный параметр. YARA-проверка объектов точек автозапуска.
`/EXCLUDEAUTORUNS=<list of autorun point objects to exclude from the YARA scan>`	Необязательный параметр. Исключение объектов точек автозапуска из области проверки. Необходимо через пробел указать пути к исполняемым файлам процессов вместе с названиями файлов. Вы можете также использовать символы `*` и `?` для ввода маски.
`/LOGFOLDER=<path for saving scan results>`	Необязательный параметр. Если указан путь к папке, приложение сохраняет результаты сканирования по указанному пути в файле yara_<имя компьютера>_<время завершения сканирования>.txt. Если указан путь к конкретному TXT-файлу, приложение сохраняет результаты сканирования в нем. Например: `/LOGFOLDER=C:\test` или `/LOGFOLDER=C:\test\abc.txt`. Результаты проверки будут выведены в командной строке независимо от того, указано ли значение параметра `/LOGFOLDER`.
`/PWD:<password>`	Необязательный параметр. Пароль учетной записи KLAdmin или учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести пароль в следующей строке.
`/LOGIN:<user name>`	Необязательный параметр. Имя учетной записи пользователя с необходимыми разрешениями. Если значение параметра не указано, приложение предложит ввести имя учетной записи в следующей строке. Значение параметра не нужно указывать, если вы ввели пароль от учетной записи KLAdmin.

Пример

```
KAVSHELL YARA C:\rule.yara /SCANFOLDERS=c:\scanFolder\ /RECURSIVE=on
KAVSHELL YARA /PATH=c:\rules\ /SCANFOLDERS=c:\scanFolder\ /FASTSCAN=on
KAVSHELL YARA c:\rules\rule1.yara c:\rules\rule2.yara /SCANFOLDERS=c:\scanFolder\ /LOGFOLDER=c:\yara_logs\
KAVSHELL YARA /PATH=c:\rules\ /SCANFOLDERS=c:\scanFolder\ c:\scanFolder2\ /LOGFOLDER=c:\yara_logs\
```

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Industrial CyberSecurity for Nodes, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Industrial CyberSecurity for Nodes.

Kaspersky предоставляет поддержку Kaspersky Industrial CyberSecurity for Nodes в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Предоставление расширенной диагностической информации специалистам Службы технической поддержки

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить параметры программы. Для этого может потребоваться выполнение следующих действий:

- Активировать функциональность обработки и сохранения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения и отправки сохраняемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Специалисты Службы технической поддержки сообщат всю необходимую для выполнения перечисленных действий информацию (описание последовательности шагов, изменяемые настройки, файлы конфигурации, скрипты, дополнительные функции командной строки, отладочные модули, специализированные утилиты и т. д.), а также состав данных, анализируемых в целях отладки. Расширенная диагностическая информация хранится на компьютере пользователя. Автоматическая передача сохраненных данных в "Лабораторию Касперского" не выполняется.

После того как вы сообщите специалистам Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией о работе Kaspersky Industrial CyberSecurity for Nodes и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать файл трассировки, отправить файл дампа памяти и предоставить отчет утилиты Kaspersky Get System Info.

В результате анализа присланных вами данных специалисты Службы технической поддержки могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие угроз, проверять компьютер на наличие угроз, лечить / удалять зараженные файлы и создавать отчеты о результатах проверки компьютера.

Перечисленные выше действия могут выполняться только под руководством специалистов Службы технической поддержки в соответствии с полученными от них инструкциями. Самостоятельное изменение параметров программы способами, не описанными в документации к программе или отличными от рекомендаций специалистов Службы технической поддержки, может привести к замедлению работы и сбоям в операционной системе, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

Трассировка работы приложения

Трассировка приложения – это подробная запись действий, выполняемых приложением, и сообщений о событиях, происходящих во время работы приложения. В процессе трассировки приложение создает комплект файлов с данными о работе разных компонентов приложения.

Выполняйте трассировку приложения под руководством Службы технической поддержки "Лаборатории Касперского".

Файлы трассировки позволяют отследить процесс пошагового выполнения команд приложения и обнаружить, на каком этапе работы приложения возникает ошибка.

Как включить и настроить трассировку работы приложения в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Диагностика сбоев**.
4. В блоке **Настройки диагностики сбоев** нажмите на кнопку **Настройка**.

   Откроется окно **Настройки диагностики сбоев** на вкладке **Настройки трассировок приложения**.
5. Используйте флажок **Включить трассировку**, чтобы включить или выключить трассировку работы приложения.

   По умолчанию трассировка работы приложения выключена.
6. Если необходимо, измените заданную по умолчанию папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки. Для этого укажите полный путь к локальной папке в поле **Папка файлов трассировки**.

   Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

Kaspersky Industrial CyberSecurity for Nodes создаст в выбранной папке подпапку для хранения файлов трассировки с названием logs-Kaspersky Industrial CyberSecurity for Nodes-<uid>, где <uid> – уникальный восьмизначный идентификатор.

7. Выберите уровень детализации отладочной информации:

   - **Обычный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждениях, а также информация о работе приложения в нормальном режиме (значение по умолчанию).
   - **Критический** – в файле трассировки сохраняются только сообщения о неустранимых ошибках.
   - **Диагностический** – в файле трассировки сохраняются сообщения обо всех ошибках, а также предупреждения.
   - **Важный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждения, а также дополнительная информация.
   - **Детальный** – в файле трассировки сохраняется вся информация о работе приложения.

   Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.

8. Для удаления старых файлов трассировки включите функцию **Заменять старые файлы трассировки более новыми**.

   Если функция включена, настройте максимальный размер и количество файлов трассировок:

   a. Укажите **Максимальный размер файла трассировки (МБ)**.

      Доступные значения: от 1 до 4095 МБ. Значение по умолчанию – 100 МБ.

   b. Укажите значение **Максимальное количество файлов трассировки в журнале**.

      Доступные значения: от 1 до 999. Значение по умолчанию – 5.

9. Сохраните внесенные изменения.

Как включить и настроить трассировку работы приложения в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:

   - В панели результатов узла перейдите по ссылке **Свойства приложения**.
   - В контекстном меню узла выберите пункт **Свойства приложения**.

   Откроется окно **Свойства приложения**.

2. Выберите вкладку **Диагностика сбоев**.

3. В блоке **Настройки диагностики сбоев** нажмите на кнопку **Настройка**.

   Откроется окно **Настройки диагностики сбоев**.

4. Выберите вкладку для настройки трассировки:

   - **Настройки трассировок приложения**. Kaspersky Industrial CyberSecurity for Nodes запускает трассировки для приложения.

   - **Настройки трассировок Консоли приложения**. Если вы установили Консоль приложения и Kaspersky Industrial CyberSecurity for Nodes на разные компьютеры, то вы можете запустить трассировку только для Консоли приложения.

5. Используйте флажок **Включить трассировку**, чтобы включить или выключить трассировку работы приложения.

   По умолчанию трассировка работы приложения выключена.

6. Если необходимо, измените заданную по умолчанию папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки. Для этого нажмите на кнопку **Обзор** и выберите нужную папку.

   > Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

   Kaspersky Industrial CyberSecurity for Nodes создаст в выбранной папке подпапку для хранения файлов трассировки с названием logs-Kaspersky Industrial CyberSecurity for Nodes-<uid>, где <uid> – уникальный восьмизначный идентификатор.

7. Выберите уровень детализации отладочной информации:

   - **Обычный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждениях, а также информация о работе приложения в нормальном режиме (значение по умолчанию).

   - **Критический** – в файле трассировки сохраняются только сообщения о неустранимых ошибках.

   - **Диагностический** – в файле трассировки сохраняются сообщения обо всех ошибках, а также предупреждения.

   - **Важный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждения, а также дополнительная информация.

   - **Детальный** – в файле трассировки сохраняется вся информация о работе приложения.

   Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.

8. Для удаления старых файлов трассировки включите функцию **Заменять старые файлы трассировки более новыми**.

   Если функция включена, настройте максимальный размер и количество файлов трассировок:

   a. Укажите **Максимальный размер файла трассировки (МБ)**.

      Доступные значения: от 1 до 4095 МБ. Значение по умолчанию – 100 МБ.

   b. Укажите значение **Максимальное количество файлов трассировки в журнале**.

      Доступные значения: от 1 до 999. Значение по умолчанию – 5.

9. Сохраните внесенные изменения.

Как включить и настроить трассировку работы приложения в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Диагностика сбоев**.
5. В блоке **Настройки диагностики сбоев** используйте флажок **Включить трассировку приложения**, чтобы включить или выключить трассировку работы приложения.

   По умолчанию трассировка работы приложения выключена.
6. Если необходимо, измените заданную по умолчанию папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки. Для этого укажите полный путь к локальной папке в поле **Папка файлов трассировки (полный путь к папке, например, C:\\Traces\\)**.

   > Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

   Kaspersky Industrial CyberSecurity for Nodes создаст в выбранной папке подпапку для хранения файлов трассировки с названием logs-Kaspersky Industrial CyberSecurity for Nodes-<uid>, где <uid> – уникальный восьмизначный идентификатор.
7. Выберите уровень детализации отладочной информации:

   - **Обычный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждениях, а также информация о работе приложения в нормальном режиме (значение по умолчанию).
   - **Критический** – в файле трассировки сохраняются только сообщения о неустранимых ошибках.
   - **Диагностический** – в файле трассировки сохраняются сообщения обо всех ошибках, а также предупреждения.
   - **Важный** – в файле трассировки сохраняются сообщения обо всех ошибках, предупреждения, а также дополнительная информация.
   - **Детальный** – в файле трассировки сохраняется вся информация о работе приложения.

   Уровень детализации, требуемый для решения возможных проблем, определяется специалистом Службы технической поддержки.
8. Для удаления старых файлов трассировки включите функцию **Использовать вытеснение старых файлов журнала трассировки**.

   Если функция включена, настройте максимальный размер и количество файлов трассировок:

   a. Укажите **Максимальный размер файлов трассировки (МБ)**.

      Доступные значения: от 1 до 4095 МБ. Значение по умолчанию – 100 МБ.

b. Укажите значение **Максимальное количество файлов журнала трассировки**.

Доступные значения: от 1 до 999. Значение по умолчанию – 5.

9. Сохраните внесенные изменения.

Вы также можете включить и настроить трассировку работы приложения в Диагностическом окне и из командной строки.

О составе и хранении файлов трассировки

Вы сами несете ответственность за обеспечение безопасности полученной информации и, в частности, за контроль и ограничение доступа к полученной информации, хранимой на компьютере, до ее передачи в "Лабораторию Касперского".

Файлы трассировки хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения.

Файлы трассировки хранятся в папке %ProgramData%\Kaspersky Lab\KICS.5.0\Traces.

Файлы трассировки называются следующим образом: KICS<5.0_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.

Вы можете просмотреть данные, записанные в файлы трассировки.

Все файлы трассировки содержат следующие общие данные:

- Время события.
- Номер потока выполнения.
- Компонент приложения, в результате работы которого произошло событие.
- Степень важности события (информационное, предупреждение, критическое, ошибка).
- Описание события выполнения команды компонента приложения и результата выполнения этой команды.

Содержание файлов трассировки SRV.log, GUI.log и ALL.log

В файлы трассировки SRV.log, GUI.log и ALL.log, помимо общих данных, может записываться следующая информация:

- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на локальном компьютере.
- Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке интернет-трафика.
- Имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
- Имя учетной записи для входа в Microsoft Windows, если имя учетной записи является частью имени файла.

- Адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
- Адрес прокси-сервера, имя компьютера, порт, IP-адрес, имя пользователя, используемое при авторизации на прокси-сервере. Эти данные записываются в файлы трассировки, если приложение использует прокси-сервер.
- Внешние IP-адреса, с которыми было установлено соединение с вашего компьютера.
- Данные о сетевом трафике. Эти данные записываются в файлы трассировки, если включены компоненты мониторинга трафика.
- Данные, полученные с серверов "Лаборатории Касперского" (например, версия антивирусных баз).
- Статусы компонентов Kaspersky Industrial CyberSecurity for Nodes и сведения об их работе.
- Данные о действиях пользователя в приложении.
- События операционной системы.

Содержание файлов трассировки HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Файл трассировки HST.log, помимо общих данных, содержит информацию о выполнении задачи обновления баз и модулей приложения.

Файл трассировки BL.log, помимо общих данных, содержит информацию о событиях, возникающих во время работы приложения, а также данные, необходимые для устранения неполадок в работе приложения. Этот файл создается, если приложение запускается с параметром avp.exe –bl.

Файл трассировки Dumpwriter.log, помимо общих данных, содержит служебную информацию, необходимую для устранения неполадок, возникающих при записи файла дампа приложения.

Файл трассировки WD.log, помимо общих данных, содержит информацию о событиях, возникающих в процессе работы службы avpsus, в том числе события обновления модулей приложения.

Файл трассировки AVPCon.dll.log, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файла трассировки компонента AMSI-защита

Файл трассировки AMSI.log, помимо общих данных, содержит информацию о результатах проверок, запрошенных сторонними приложениями.

Содержание файлов трассировки веб-плагина приложения

Файлы трассировки веб-плагина приложения хранятся на компьютере, на котором развернута Kaspersky Security Center Web Console, в папке Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

Файлы трассировки веб-плагина приложения называются следующим образом: logs-kics_windows-<type of trace file>.DESKTOP-<date of file update>.log. Web Console начинает записывать данные после установки и удаляет файлы трассировки после удаления Web Console.

Файлы трассировки веб-плагина приложения, помимо общих данных, содержат следующую информацию:

- Пароль пользователя KLAdmin для разблокировки интерфейса Kaspersky Industrial CyberSecurity for Nodes.
- Временный пароль для разблокировки интерфейса Kaspersky Industrial CyberSecurity for Nodes.
- Имя пользователя и пароль для почтового SMTP-сервера.
- Имя пользователя и пароль для прокси-сервера.
- Имя пользователя и пароль для задачи *Изменение состава компонентов приложения*.
- Учетные данные и пути, указанные в свойствах политики и в задачах Kaspersky Industrial CyberSecurity for Nodes.

Запись дампов памяти

Файл дампа памяти содержит всю информацию о рабочей памяти процессов Kaspersky Industrial CyberSecurity for Nodes на момент сбоя в работе приложения.

Файлы дампов памяти хранятся на вашем компьютере в течение всего времени использования приложения и безвозвратно удаляются при удалении приложения.

Сохраненные дампы могут содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту файлов дампов памяти.

По умолчанию файлы дампов памяти хранятся в папке %ProgramData%\Kaspersky Lab\KICS.5.0\Traces.

Как включить или выключить запись дампов памяти в Консоли администрирования Kaspersky Security Center

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.
2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
3. В открывшемся окне свойств политики перейдите в раздел **Диагностика сбоев**.
4. В блоке **Настройки диагностики сбоев** нажмите на кнопку **Настройка**.

   Откроется окно **Настройки диагностики сбоев** на вкладке **Настройки трассировок приложения**.
5. Выберите вкладку **Настройки дампов приложения**.
6. Используйте флажок **Создавать во время сбоя файл дампа**, чтобы включить или выключить трассировку работы приложения.

   По умолчанию запись дампов выключена.

7. Если необходимо, измените заданную по умолчанию папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки. Для этого укажите полный путь к локальной папке в поле **Папка файлов дампа**.

   Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

8. Сохраните внесенные изменения.

Как включить или выключить запись дампов памяти в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:

   - В панели результатов узла перейдите по ссылке **Свойства приложения**.
   - В контекстном меню узла выберите пункт **Свойства приложения**.

   Откроется окно **Свойства приложения**.

2. Выберите вкладку **Диагностика сбоев**.

3. В блоке **Настройки диагностики сбоев** нажмите на кнопку **Настройка**.

   Откроется окно **Настройки диагностики сбоев**.

4. Выберите вкладку для настройки записи дампов:

   - **Настройки дампов приложения**. Kaspersky Industrial CyberSecurity for Nodes записывает все дампы приложения.
   - **Настройки дампов Консоли приложения**. Если вы установили Консоль приложения и Kaspersky Industrial CyberSecurity for Nodes на разные компьютеры, то вы можете записать дампы только для Консоли приложения.

5. Используйте флажок **Создавать во время сбоя файл дампа**, чтобы включить или выключить трассировку работы приложения.

   По умолчанию запись дампов выключена.

6. Если необходимо, измените заданную по умолчанию папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки. Для этого нажмите на кнопку **Обзор** и выберите нужную папку.

   Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.

7. Сохраните внесенные изменения.

Как включить или выключить запись дампов памяти в Web Console

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Диагностика сбоев**.
5. В блоке **Настройки файла дампа** используйте флажок **Создавать во время сбоя файл дампа**, чтобы включить или выключить трассировку работы приложения.

   По умолчанию запись дампов выключена.
6. Если необходимо, измените заданную по умолчанию папку, в которую Kaspersky Industrial CyberSecurity for Nodes будет сохранять файлы трассировки. Для этого укажите полный путь к локальной папке в поле **Папка файла дампа (полный путь к папке, например, C:\\Dumps\\)**.

   > Папка должна быть создана заранее и доступна на запись для учетной записи SYSTEM. Нельзя указать сетевую папку, диск или переменные среды.
7. Сохраните внесенные изменения.

Вы также можете включить или выключить запись дампов памяти в Диагностическом окне.

Защита файлов дампов и файлов трассировки

Файлы дампов и файлы трассировки содержат информацию об операционной системе, а также могут содержать данные пользователя. Чтобы предотвратить несанкционированный доступ к этим данным, вы можете включить защиту файлов дампов и файлов трассировки.

Если защита файлов дампов и файлов трассировки включена, доступ к файлам имеют следующие пользователи:

- К файлам дампов имеют доступ системный и локальный администраторы, а также пользователь, включивший запись файлов дампов и файлов трассировки.
- К файлам трассировки имеют доступ только системный и локальный администраторы.

Как включить защиту файлов дампов и файлов трассировки в Консоли администрирования Kaspersky Security Center

1. В главном окне Web Console выберите **Управление активами → Политики**.
2. Нажмите на название политики Kaspersky Industrial CyberSecurity for Nodes.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры приложения**.
4. Выберите раздел **Диагностика сбоев**.

5. Используйте флажок **Включить защиту файлов дампов и файлов трассировки**, чтобы включить или выключить защиту файлов дампов и файлов трассировки.

6. Сохраните внесенные изменения.

1. В дереве Консоли администрирования Kaspersky Security Center выберите папку **Политики**.

2. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.

3. В открывшемся окне свойств политики перейдите в раздел **Диагностика сбоев**.

4. В блоке **Настройки диагностики сбоев** нажмите на кнопку **Настройка**.

5. Откроется окно **Настройки диагностики сбоев**.

6. Используйте флажок **Включить защиту файлов дампов и файлов трассировки**, чтобы включить или выключить защиту файлов дампов и файлов трассировки.

7. Сохраните внесенные изменения.

Как включить защиту файлов дампов и файлов трассировки в Консоли приложения

1. В дереве Консоли приложения выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:

   - В панели результатов узла перейдите по ссылке **Свойства приложения**.
   - В контекстном меню узла выберите пункт **Свойства приложения**.

   Откроется окно **Свойства приложения**.

2. Выберите вкладку **Диагностика сбоев**.

3. В блоке **Настройки диагностики сбоев** нажмите на кнопку **Настройка**.

   Откроется окно **Настройки диагностики сбоев**.

4. Используйте флажок **Включить защиту файлов дампов и файлов трассировки**, чтобы включить или выключить защиту файлов дампов и файлов трассировки.

5. Сохраните внесенные изменения.

Вы также можете включить или выключить защиту файлов дампов и файлов трассировки в Диагностическом окне.

Файлы дампов и файлы трассировки, записанные при включенной защите, остаются защищенными после отключения этой функции.

Получение данных об ОС (Kaspersky Get System Info)

После установки приложения Kaspersky Industrial CyberSecurity for Nodes могут возникнуть ситуации, при которых операционная система или приложение работают некорректно. Происходит конфликт приложения с программным обеспечением или с драйверами комплектующих компьютера.

Чтобы выяснить причину проблемы, технической поддержке "Лаборатории Касперского" требуется отчет утилиты Kaspersky Get System Info (далее GSI). Подробную информацию о работе с утилитой см. в Базе знаний "Лаборатории Касперского".

Источники информации о Kaspersky Industrial CyberSecurity for Nodes

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Industrial CyberSecurity for Nodes:

- страница Kaspersky Industrial CyberSecurity for Nodes на веб-сайте "Лаборатории Касперского";
- страница приложения на веб-сайте Службы технической поддержки (База знаний);
- онлайн-справка;
- обсуждение приложения на Форуме.

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Просмотр онлайн-справки может быть недоступен в браузерах, не поддерживающих современные протоколы шифрования.

Если вы не нашли решения своей проблемы, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Страница Kaspersky Industrial CyberSecurity for Nodes на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Industrial CyberSecurity for Nodes можно ознакомиться с общей информацией о программе, ее возможностях и особенностях работы.

Страница Kaspersky Industrial CyberSecurity for Nodes содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Industrial CyberSecurity for Nodes в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Industrial CyberSecurity for Nodes в Базе знаний приведены статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний содержат информацию, относящуюся не только к Kaspersky Industrial CyberSecurity for Nodes, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Онлайн-справка Kaspersky Industrial CyberSecurity for Nodes

В онлайн-справке вы можете найти информацию о настройке и использовании Kaspersky Industrial CyberSecurity for Nodes.

Обсуждение приложения на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Расширения файлов для быстрой проверки

com – исполняемый файл приложения размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст приложения dBase™, Clipper или Microsoft Visual FoxPro®, приложение пакета WAVmaker;

bin – бинарный файл;

bat – файл пакетного задания;

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – приложение, работающее в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о приложении;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых приложений;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовое приложение для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

msg – сообщение электронной почты Microsoft Mail;

plg – сообщение электронной почты;

mbx – сохраненное сообщение электронной почты Microsoft Office Outlook;

doc* – документы Microsoft Office Word, такие как: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Office Word, такие как: dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – приложение баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Windows Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave® Flash;

jpg, jpeg – файл графического формата хранения сжатых изображений;

emf – файл формата Enhanced Metafile;

ico – файл значка объекта;

ov? – исполняемые файлы Microsoft Office Word;

xl* – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft Office PowerPoint®, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint 2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Office Access®, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

Учетные записи пользователей в правилах компонентов приложения

Для настройки работы некоторых компонентов приложения нужно добавить специальные правила, в которых можно выбрать пользователей, для которых приложение будет применять это правило.

Правила необходимо добавлять для настройки следующих компонентов приложения:

- Контроль запуска программ;
- Контроль устройств;
- Защита от шифрования;
- Контроль целостности системы.

Вы можете добавить пользователей следующими способами:

- выбрать из Active Directory (рекомендуется);
- выбрать из списка пользователей в Kaspersky Security Center;
- добавить вручную.

Специалисты "Лаборатории Касперского" рекомендуют использовать локальные учетные записи только в тех случаях, когда использовать доменные учетные записи невозможно. Подробнее о рисках безопасности локальных учетных записей см. в Базе знаний Microsoft. Вы сами несете ответственность за обеспечение безопасности компьютера при использовании локальных учетных записей, в частности, за контроль и ограничение доступа к настройкам приложения.

Для идентификации пользователей приложение использует SID пользователя (Security Identifier). При использовании учетных записей из Active Directory или списка пользователей в Kaspersky Security Center приложение определяет SID на Сервере администрирования. Таким образом, приложение не оказывает дополнительную нагрузку на компьютер для идентификации пользователя. Если вы добавили в правило приложения более 1000 локальных учетных записей, то для идентификации пользователя приложение обращается к контроллеру домена. Таким образом, возрастает нагрузка на компьютер. Для оптимизации нагрузки на компьютер рекомендуется использовать учетные записи из Active Directory или списка пользователей в Kaspersky Security Center.

Kaspersky Industrial CyberSecurity for Nodes поддерживает в правилах встроенные учетные записи пользователей и групп (например, группа "Все"). Из-за особенностей определения SID пользователя приложение позволяет использовать встроенные учетные записи, добавленные только из Active Directory или списка пользователей в Kaspersky Security Center. Правила, в которых встроенная учетная запись добавлена вручную, не работают.

Юридическая информация

Предоставление данных

Этот раздел содержит информацию о данных, которые приложение Kaspersky Industrial CyberSecurity for Nodes может сохранять на устройстве и передавать в автоматическом режиме в "Лабораторию Касперского" в ходе своей работы.

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

Предоставление данных в рамках Лицензионного соглашения

Принимая условия Лицензионного соглашения, вы соглашаетесь отправлять в автоматическом режиме следующие данные в "Лабораторию Касперского":

- для поддержки механизма получения обновлений – данные об установленной программе и лицензионном сертификате: идентификатор устанавливаемой программы и ее полная версия, включая номер сборки, тип и идентификатор лицензии, идентификатор установки, уникальный идентификатор задачи обновления;

- для управления согласием на обработку данных – данные о статусе согласия с условиями Лицензионного соглашения и других документов, оговаривающих условия отправки данных: идентификатор и версия Лицензионного соглашения или другого документа, в рамках которого принимаются или отклоняются условия обработки данных; атрибут, обозначающий действие пользователя (подтверждение или отмена принятия условий); дата и время изменения статуса принятия условий обработки данных;

- Для активации программы с помощью кода активации – данные о типе, версии и локализации установленного приложения, версия установленных обновлений, идентификатор защищаемого устройства и идентификатор установки программы на защищаемом устройстве, код активации и уникальный идентификатор текущей лицензии, тип, версия и разрядность операционной системы, имя виртуальной среды при установке программы в виртуальной среде и идентификаторы компонентов программы, активных в момент предоставления информации.

Данные, получаемые от вас "Лабораторией Касперского" во время использования программы, защищаются и обрабатываются в соответствии с требованиями, установленными законодательством и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи. Более подробная информация об обработке, хранении и уничтожении информации, получаемой в процессе использования программы и передаваемой в "Лабораторию Касперского", приведена в Политике конфиденциальности на сайте www.kaspersky.com/Products-and-Services-Privacy-Policy.

Локальная обработка данных

В процессе выполнения основных функций программы, описанных в настоящем Руководстве, Kaspersky Industrial CyberSecurity for Nodes локально обрабатывает и хранит ряд данных на защищаемом устройстве.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Industrial CyberSecurity for Nodes данных, содержащихся в отчетах.

Функциональная область	Аудит.
Тип использования	Kaspersky Industrial CyberSecurity for Nodes хранит данные локально и передает данные на Сервер администрирования. В базе данных Сервера администрирования хранится информация о событиях программы, произошедших на управляемых защищаемых устройствах.
Хранилище	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<версия продукта>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • База данных Сервера администрирования
Меры безопасности	Список контроля доступа (Access-control list).
Период хранения	Kaspersky Industrial CyberSecurity for Nodes хранит данные до момента удаления Kaspersky Industrial CyberSecurity for Nodes. При удалении Kaspersky Industrial CyberSecurity for Nodes будут удалены все данные Kaspersky Industrial CyberSecurity for Nodes, хранящиеся на защищаемом устройстве.
Назначение	Обеспечение основных функций.

Kaspersky Industrial CyberSecurity for Nodes не удаляет события в журнале событий Windows.

Kaspersky Industrial CyberSecurity for Nodes локально обрабатывает и хранит в отчетах следующие данные:

- Имена и атрибуты обрабатываемых файлов и полные пути к ним на проверяемом носителе.
- Действия, выполняемые над проверяемыми файлами программой Kaspersky Industrial CyberSecurity for Nodes.
- Действия, выполняемые пользователями над проверяемыми файлами на защищаемом устройстве.
- Информация об учетных записях пользователей, выполняющих действия в защищаемой сети или на защищаемом устройстве.
- Значения путей к экземплярам устройств, добавленных в правила контроля устройств.
- Информация о процессах и скриптах, запущенных в системе: контрольные суммы (MD5, SHA-256) и полные пути к исполняемым файлам, информация о цифровых сертификатах.
- Параметры брандмауэра Windows.
- Записи журнала событий Windows.
- Имена учетных записей пользователей, выполняющих действия над проверяемыми файлами на защищаемом устройстве.
- Экземпляры запущенных исполняемых файлов, а также типы, имена, контрольные суммы и атрибуты этих файлов.
- Информация о сетевой активности: IP-адреса заблокированных внешних устройств, идентификаторы скомпрометированных сеансов входа, во время которых был выполнен доступ к общим защищаемым ресурсам.
- Информация о сетях Wi-Fi, к которым подключается защищаемое устройство: сетевые имена и сетевые идентификаторы.

- Информация о проектах ПЛК, добавленных в область защиты, включая параметры подключения ПЛК (IP-адреса, номера шин и слотов) и контрольные суммы микропрограммного обеспечения.
- Информация о статусе USN-журнала Windows.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Industrial CyberSecurity for Nodes данных о параметрах, указанных пользователями.

Kaspersky Industrial CyberSecurity for Nodes обрабатывает и хранит данные только о параметрах, указанных пользователями.

Обработка и хранение данных о параметрах, указанных пользователями

Функциональная область	Автообновление, интеграция с изолированной средой.
Тип использования	Kaspersky Industrial CyberSecurity for Nodes хранит данные о параметрах локально и передает данные на Сервер администрирования. В базе данных Сервера администрирования хранится информация о параметрах управляемых защищаемых устройств.
Хранилище	%ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<product version>\
Меры безопасности	Список контроля доступа (Access-control list).
Период хранения	Kaspersky Industrial CyberSecurity for Nodes хранит данные до момента удаления Kaspersky Industrial CyberSecurity for Nodes. При удалении Kaspersky Industrial CyberSecurity for Nodes будут удалены все данные Kaspersky Industrial CyberSecurity for Nodes, хранящиеся на защищаемом устройстве.
Назначение	Обеспечение основных функций.

Kaspersky Industrial CyberSecurity for Nodes не удаляет данные о параметрах, экспортируемых в конфигурационный файл.

Kaspersky Industrial CyberSecurity for Nodes не удаляет объекты на карантине и в резервном хранилище, если установлены флажки **Экспортировать объекты на карантине** и **Экспортировать объекты резервного хранилища** в мастере установки.

Kaspersky Industrial CyberSecurity for Nodes локально обрабатывает и хранит следующие данные о параметрах, указанных пользователями:

- Информация об объектах, помещенных на карантин или в резервное хранилище.
- Информация о параметрах, настроенных через Консоль программы или Плагин управления, например:
  - Пароль Kaspersky Industrial CyberSecurity for Nodes, имена учетных записей пользователей, с правами которых запускаются задачи Kaspersky Industrial CyberSecurity for Nodes.
  - Имя учетной записи пользователя, используемое для аутентификации на прокси-сервере.
  - Адреса сетевых папок или папок на HTTP- или FTP-серверах, используемых в качестве пользовательских источников обновлений.
  - Информация о сетях Wi-Fi.
  - Информация о проектах ПЛК, добавленных в область защиты, включая параметры подключения ПЛК и контрольные суммы микропрограммного обеспечения.

- IP-адреса и идентификаторы заблокированных сеансов входа.
- Параметры брандмауэра Windows.
- Контрольные суммы (MD5, SHA-256) и пути к исполняемым файлам, добавленным в правила задачи Контроль запуска программ.
- Значения путей к экземплярам устройств, добавленных в правила контроля устройств.
- Информация о папках, включенных в области задач Kaspersky Industrial CyberSecurity for Nodes.
- Информация о событиях в журнале событий Windows.
- Информация о файлах, обнаруженных с использованием технологий iSwift и iChecker.
- Контрольные суммы (MD5, SHA-256) и пути к файлам, добавленным в доверенную зону.
- Информация о добавленных лицензионных ключах.
- Информация о цифровых сертификатах.
- Контрольные суммы файлов, данные цифровых сертификатов, полные пути к файлам (база данных SDC, файлы для задачи Мониторинг целостности файлов на основе эталона).
- Временные файлы, создаваемые программой при проверке архивов.
- Информация в %SystemRoot%.

- Данные о файлах, обработанных Kaspersky Industrial CyberSecurity for Nodes, например, контрольные суммы (MD5, SHA-256) файлов, информация о цифровых сертификатах, полные пути к файлам.

Kaspersky Industrial CyberSecurity for Nodes обрабатывает и хранит данные в рамках основной функциональности программы, в том числе для регистрации событий программы и получения диагностических данных. Обработка и защита локально обрабатываемых данных выполняются в соответствии с настроенными и применяющимися параметрами программы.

Kaspersky Industrial CyberSecurity for Nodes позволяет настроить уровень защиты данных, обрабатываемых локально: вы можете изменять права пользователей на доступ к обрабатываемым данным, изменять сроки хранения таких данных, частично или полностью отключать функциональность, в рамках которой выполняется регистрация данных, а также изменять путь к папке на диске, в которую выполняется запись данных, и ее атрибуты.

Детальная информация по настройке функциональности программы, в рамках которой выполняется обработка данных, содержится в соответствующих разделах настоящего Руководства.

Локальная обработка данных вспомогательными компонентами программы

В пакет установки Kaspersky Industrial CyberSecurity for Nodes включены вспомогательные компоненты программы, которые могут быть установлены на устройстве, даже если на нем не установлена программа Kaspersky Industrial CyberSecurity for Nodes.

При выполнении основных функций программы, описанных в настоящем Руководстве, вспомогательные компоненты программы локально обрабатывают и хранят набор данных на защищаемом устройстве, на котором они установлены, даже если они установлены отдельно от Kaspersky Industrial CyberSecurity for Nodes.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Industrial CyberSecurity for Nodes данных, записываемых в файлы дампов и файлы трассировки.

По умолчанию, Kaspersky Industrial CyberSecurity for Nodes не записывает файлы дампов и файлы трассировки.

Обработка и хранение данных, записываемых в файлы дампов и файлы трассировки

Хранилище	По умолчанию папка, в которую сохраняются файлы дампов и файлы трассировки, не указана. Можно указать папку.
Меры безопасности	Kaspersky Industrial CyberSecurity for Nodes не ограничивает доступ к файлам дампов и файлам трассировки.
Период хранения	Kaspersky Industrial CyberSecurity for Nodes не удаляет файлы дампов и файлы трассировки.
Назначение	Обеспечение технической поддержки.

Kaspersky Industrial CyberSecurity for Nodes локально обрабатывает и хранит следующие данные, записанные в файлы дампов и файлы трассировки:

- Информация о действиях, выполняемых программой Kaspersky Industrial CyberSecurity for Nodes на защищаемом устройстве.
- Информация об объектах, обработанных программой Kaspersky Industrial CyberSecurity for Nodes.
- Информация об ошибках, возникших во время работы программы Kaspersky Industrial CyberSecurity for Nodes.

Данные, обрабатываемые вспомогательными компонентами программы, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы.

По умолчанию все данные, локально обрабатываемые вспомогательными компонентами программы в ходе работы, удаляются после удаления этих компонентов.

Исключение составляют файлы трассировки вспомогательных компонентов программы. Рекомендуется самостоятельно удалить эти файлы.

Вы можете найти детальную информацию по работе с файлами, содержащими диагностические данные вспомогательных компонентов программы, в соответствующих разделах настоящего Руководства.

Предоставление данных при использовании решений Detection and Response

На компьютерах с установленным приложением Kaspersky Industrial CyberSecurity for Nodes хранятся данные, подготовленные для автоматической отправки на серверы решений Detection and Response. Файлы хранятся на компьютерах в открытом незашифрованном виде.

Конкретный состав данных зависит от решения, в составе которого используется Kaspersky Industrial CyberSecurity for Nodes.

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Industrial CyberSecurity for Nodes.

Данные о результатах выполнения задачи Поиск IOC (стандартная задача)

Kaspersky Industrial CyberSecurity for Nodes автоматически передает данные о результатах выполнения задач *Поиск IOC* в Kaspersky Security Center.

Данные в результатах выполнения задач *Поиск IOC* могут содержать следующую информацию:

- IP-адрес из ARP-таблицы.
- Физический адрес из ARP-таблицы.
- Тип и имя записи DNS.
- IP-адрес защищаемого компьютера.
- Физический адрес (MAC) защищаемого компьютера.
- Идентификатор записи в журнале событий.
- Имя источника данных в журнале.
- Имя журнала.
- Время события.
- MD5 и SHA256-хеши файла.
- Полное имя файла (включая путь).
- Размер файла.
- Удаленные IP-адрес и порт, с которыми было установлено соединение в момент проверки.
- IP-адрес локального адаптера.
- Порт, открытый на локальном адаптере.
- Протокол в виде числа (в соответствии со стандартом IANA).
- Имя процесса.
- Аргументы процесса.
- Путь к файлу процесса.

- Windows идентификатор процесса (PID).
- Windows идентификатор родительского процесса (PID).
- Имя учетной записи пользователя, запустившего процесс.
- Дата и время запуска процесса.
- Имя службы.
- Описание службы.
- Путь и имя DLL-службы (для svchost).
- Путь и имя исполняемого файла службы.
- Windows идентификатор службы (PID).
- Тип службы (например, драйвер ядра или адаптер).
- Статус службы.
- Режим запуска службы.
- Имя учетной записи пользователя.
- Наименование тома.
- Буква тома.
- Тип тома.
- Значение реестра Windows.
- Значение куста реестра.
- Путь к ключу реестра (без куста и без имени значения).
- Параметр реестра.
- Система (окружение).
- Имя и версия операционной системы, установленной на компьютере.
- Сетевое имя защищаемого компьютера.
- Домен или группа, к которому принадлежит защищаемый компьютер.
- Имя браузера.
- Версия браузера.
- Время последнего обращения к веб-ресурсу.
- URL из HTTP-запроса.

- Имя учетной записи, под которой выполнен HTTP-запрос.
- Имя файла процесса, выполнившего HTTP-запрос.
- Полный путь к файлу процесса, выполнившего HTTP-запрос.
- Windows идентификатор (PID) процесса, выполнившего HTTP-запрос.
- HTTP referer (URL источника HTTP-запроса).
- URI ресурса, запрошенного по протоколу HTTP.
- Информация о HTTP агенте пользователя (приложении, выполнившем HTTP-запрос).
- Время выполнения HTTP-запроса.
- Уникальный идентификатор процесса, выполнившего HTTP-запрос.

Данные для построения цепочки развития угрозы

Данные для построения цепочки развития угрозы по умолчанию хранятся семь дней. Эти данные автоматически передаются в Kaspersky Security Center.

Данные для построения цепочки развития угрозы могут содержать следующую информацию:

- Дата и время инцидента.
- Имя обнаружения.
- Режим проверки.
- Статус последнего действия, связанного с обнаружением.
- Причина неудачной обработки обнаружения.
- Тип обнаруженного объекта.
- Имя обнаруженного объекта.
- Статус угрозы после обработки объекта.
- Причина неудачного выполнения действий над объектом.
- Действия, выполняемые для отката вредоносных действий.
- Об обрабатываемом объекте:
  - Уникальный идентификатор процесса.
  - Уникальный идентификатор родительского процесса.
  - Уникальный идентификатор файла процесса.
  - Идентификатор процесса Windows (PID).

- Командная строка процесса.
- Имя учетной записи пользователя, запустившего процесс.
- Код сеанса входа в систему, в котором запущен процесс.
- Тип сеанса, в котором запущен процесс.
- Уровень целостности обрабатываемого процесса.
- Принадлежность учетной записи пользователя, запустившего процесс, к привилегированным локальным и доменным группам.
- Идентификатор обрабатываемого объекта.
- Полное имя обрабатываемого объекта.
- Идентификатор защищаемого устройства.
- Полное имя объекта (имя локального файла или веб-адрес загружаемого файла).
- MD5 и SHA256-хеши обрабатываемого объекта.
- Тип обрабатываемого объекта.
- Дата создания обрабатываемого объекта.
- Дата последнего изменения обрабатываемого объекта.
- Размер обрабатываемого объекта.
- Атрибуты обрабатываемого объекта.
- Организация, подписавшая обрабатываемый объект.
- Результат проверки цифрового сертификата обрабатываемого объекта.
- Идентификатор безопасности (SID) обрабатываемого объекта.
- Идентификатор часового пояса обрабатываемого объекта.
- Веб-адрес загрузки обрабатываемого объекта (только для файла на диске).
- Название приложения, загрузившего файл.
- MD5 и SHA256-хеши приложения, загрузившего файл.
- Название приложения, последний раз изменившего файл.
- MD5 и SHA256-хеши приложения, последний раз изменившего файл.
- Количество запусков обрабатываемого объекта.
- Дата и время первого запуска обрабатываемого объекта.

- Уникальный идентификатор файла.
- Полное имя файла (имя локального файла или веб-адрес загружаемого файла).
- Путь к обрабатываемой переменной реестра Windows.
- Имя обрабатываемой переменной реестра Windows.
- Значение обрабатываемой переменной реестра Windows.
- Тип обрабатываемой переменной реестра Windows.
- Показатель принадлежности обрабатываемого ключа реестра к точке автозапуска.
- Веб-адрес обрабатываемого веб-запроса.
- Источник ссылок обрабатываемого веб-запроса.
- Агент пользователя обрабатываемого веб-запроса.
- Тип обрабатываемого веб-запроса (`GET` или `POST`).
- Локальный IP-порт для обрабатываемого веб-запроса.
- Удаленный IP-порт для обрабатываемого веб-запроса.
- Направление соединения (входящее или исходящее) обрабатываемого веб-запроса.
- Идентификатор процесса, в который произошло внедрение вредоносного кода.

Kaspersky Endpoint Detection and Response Expert (on-premises)

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Industrial CyberSecurity for Nodes.

Служебные данные

Встроенный агент Kaspersky Industrial CyberSecurity for Nodes хранит локально следующие данные:

- Данные, необходимые для интеграции с компонентом EDR Expert (on-premises):
  - Адрес и порт для подключения к серверу KATA Central Node.
  - Адрес и порт для подключения к серверу передачи телеметрии.
  - Адрес и порт для подключения к серверу реагирования.
  - Информация о сертификатах для интеграции с KATA Central Node.

    - Информация о сертификатах для интеграции с сервером передачи телеметрии.
    - Информация о сертификатах для интеграции с сервером реагирования.
- Файлы на карантине.

Данные из передаваемых событий телеметрии

- **Данные телеметрии.**
    - Данные о файлах:
        - Уникальный идентификатор файла.
        - Тип файла.
        - Полный путь к файлу.
        - Размер файла.
        - Атрибуты файла.
        - Идентификатор зоны.
        - Дата и время создания файла.
        - Дата и время последнего изменения файла.
        - Исходное имя файла.
        - Имя приложения.
        - Версия приложения.
        - Производитель приложения.
        - Описание файла.
        - Версия файла.
        - MD5 и SHA256-хеши объекта.
        - Результат проверки подписи файла.
        - Имя издателя сертификата.
        - Имя владельца сертификата.
        - Серийный номер сертификата.

- Данные об AMSI проверке:
  - Уникальный идентификатор процесса, инициировавшего активность.
  - Тип содержимого объекта, которое передается в AMSI.
  - Содержимое объекта, которое передается в AMSI.
  - Имя объекта.
  - MD5 и SHA256-хеши объекта.
- Данные о блокировке приложений:
  - Уникальный идентификатор процесса, инициировавшего блокировку приложения.
  - Уникальный идентификатор родительского процесса.
  - Уникальный системный идентификатор процесса.
  - Команда, используемая для запуска процесса.
  - Идентификатор сеанса входа.
  - Уровень целостности процесса.
  - Статус процесса.
  - Уникальный идентификатор файла процесса.
  - Командная строка процесса.
  - Список уникальных идентификаторов интерпретируемых файлов.
- Данные о блокировке открытии файлов:
  - Уникальный идентификатор процесса, инициировавшего открытие файла.
  - Уникальный идентификатор файла.
- Данные о загрузке драйверов:
  - Уникальный идентификатор загруженного драйвера.
- Данные о событиях:
  - Уникальный идентификатор события.
  - Дата и время события.
- Данные об изменении файлов:
  - Уникальный идентификатор процесса, инициировавшего изменение файла.
  - Уникальный идентификатор файла.

    - Тип операции изменения.
    - Флаг, указывающий, что файл помечен к удалению после перезагрузки.
    - Уникальный идентификатор модифицированного файла.
    - Уникальный идентификатор файла до изменения.
    - Набор битовых флагов, которые определяют как файл был открыт.
    - Данные об операциях над списком контроля доступа.
    - Данные о смене владельца файла или его исходной группы.
- Данные о сессии входа:
    - Идентификатор сессии входа.
    - Имя пользователя, который осуществил вход.
    - Тип аккаунта пользователя.
    - Тип сессии.
- Данные о сетевых соединениях:
    - Уникальный идентификатор процесса, инициировавшего соединение.
    - Локальный IP-адрес, через который инициировано соединение.
    - Удаленный IP-адрес конечной точки соединения.
    - Направление соединения.
    - Протокол передачи данных.
    - HTTP метод.
    - Путь без имени хоста.
    - Имя хоста.
    - Динамическое состояние процесса в момент соединения.
    - Флаг, указывающий, что соединение открыто на уровне сырого сокета.
    - Версия TLS, использованная в сеансе соединения.
    - Имя TLS сервера.
    - MD5 и SHA1-хеши сертификата TLS сервера.
    - Список Subject Alternative Names (SAN) сертификата.
    - Имя издателя TLS сертификата.

    - Серийный номер сертификата.
    - Используемый шифровальный набор.
    - Начало и окончание действие сертификата.
    - JA3 отпечаток клиентского TLS клиента.
    - JA3S отпечаток сервера.
- Данные при прослушивании сетевого порта:
    - Уникальный идентификатор процесса, инициировавшего соединение.
- Данные при консольном вводе:
    - Уникальный идентификатор процесса, инициировавший консольный ввод.
    - Тип консольного ввода.
    - Текст, который был введен пользователем или процессом.
- Данные о создании процесса:
    - Уникальный идентификатор процесса.
    - Уникальный идентификатор родительского процесса.
    - Уникальный системный идентификатор процесса.
    - Команда, используемая для запуска процесса.
    - Идентификатор сеанса входа.
    - Уровень целостности процесса.
    - Уникальный идентификатор файла процесса.
    - Список уникальных идентификаторов интерпретируемых файлов.
    - Тип процесса.
- Данные о загрузке модуля процессом:
    - Уникальный идентификатор процесса, который произвел загрузку.
    - Полный путь к файлу, который был загружен в процесс.
    - Уникальный идентификатор файла-модуля.
    - Полное квалифицированное имя .NET-сборки, если загруженный файл является .NET-модулем.
    - Флаги .NET-сборки, определяемые в ее манифесте.

- Данные о завершении процесса:
  - Уникальный идентификатор завершенного процесса.
- Данные об изменении реестра:
  - Уникальный идентификатор процесса, который инициировал изменение реестра.
  - Тип операции над реестром.
  - Полный путь к ключу реестра.
  - Имя значения внутри ключа реестра.
  - Тип данных, которые записаны в значение ключа реестра.
  - Данные, записанные в значение ключа реестра.
  - Предыдущее имя ключа до переименования.
  - Информация о смене владельца или основной группы ключа.
  - Список изменений в списке контроля доступа (ACL) ключа.
- Данные об обнаруженной угрозе и ее обработке:
  - Флаг, указывающий, что обнаружение угрозы прошло в фоновом режиме.
  - Вердикт, присвоенный угрозе.
  - Наименование вердикта.
  - Уникальный идентификатор записи в базе.
  - Время, когда запись об угрозе была сохранена в базе.
  - Режим обработки угрозы.
  - Тип зараженного объекта.
  - Имя зараженного объекта.
  - MD5 и SHA256-хеши объекта.
  - Уникальный идентификатор зараженного объекта.
  - Уникальный идентификатор процесса, скачавшего зараженный объект из интернета.
  - URL, по которому был скачан зараженный объект.
  - Электронный адрес отправителя, приславшего зараженный объект.
  - Сетевой протокол, через который был получен зараженный объект.
  - Локальный адрес, с которого был получен зараженный объект.

    - Внешний адрес, с которого был получен зараженный объект.
    - Тип содержимого объекта.
    - Содержание объекта.
- Данные о доступе к процессам:
    - Уникальный идентификатор процесса совершившего попытку доступа.
    - Уникальный идентификатор целевого процесса, к которому осуществлялся доступ.
    - Набор прав, запрошенных у целевого процесса.
    - Тип операции.
    - Набор вызовов в момент обращения к процессу.
    - Дескриптор процесса-источника.
    - Дескриптор целевого процесса.
- Данные о DNS:
    - Уникальный идентификатор процесса, который инициировал DNS-запрос.
    - IP-адрес DNS сервера.
    - Флаги, управляющие поведением DNS запроса.
    - Статус выполнения запроса.
    - Полное доменное имя, указанное в DNS запросе.
    - Тип данных в DNS запросе.
    - Ответы DNS сервера.
- Данные о внедрении кода:
    - Уникальный идентификатор процесса, который пытался внедрить код.
    - Использованный способ доступа.
    - Набор вызовов в момент обнаружения внедренного кода.
    - Уникальный идентификатор целевого процесса, в который был загружен код.
    - Данные об изменении командного ряда целевого процесса.
    - Адрес целевого процесса.
    - Имя DLL-библиотеки, которая была загружена в целевой процесс.
    - Полный путь к DLL-файлу.

- Данные об операциях с именованными каналами:
  - Уникальный идентификатор процесса, который создал или подключился к каналу.
  - Полное имя именованного канала.
  - Тип операции (создание или подключение).
- Данные о запросах WMI:
  - Уникальный идентификатор процесса, который инициировал WMI-операцию.
  - Тип WMI-операции.
  - Имя целевого устройства для WMI-запроса.
  - Учетная запись, от имени которой выполнен WMI-запрос.
  - Текст WMI-запроса.
  - Пространство имен, в котором выполняется WMI-запрос.
  - Имя WMI-фильтра.
  - Имя объекта-потребителя.
  - Текст, описывающий действие объекта-потребителя.
- Данные о LDAP запросах:
  - Уникальный идентификатор процесса, выполнившего LDAP-запрос.
  - Область поиска в LDAP запросах.
  - LDAP фильтр.
  - Параметр, указывающий, к какому разделу Active Directory был направлен запрос.
  - Атрибуты LDAP поиска.
- Данные о подключенных USB устройствах:
  - Тип операции USB устройства.
  - Тип USB устройства.
  - Идентификатор USB устройства.
  - Имя USB устройства.
  - Путь к USB устройству.
  - Флаг, указывающий, что USB устройство является системным диском.
- Данные о создании, удалении и изменении задачи по расписанию.

- Данные о создании, удалении и изменении служб.
- Данные о монтировании / размонтировании файловой системы.
- Данные о работе EDR Expert on-premise компонента:
  - Информация о запуске / остановке агента.
  - Информация об установке / удалении агента.
  - Уникальный идентификатор запуска агента.
  - Системный идентификатор процесса агента.
  - Уникальный идентификатор процесса агента.
  - Причина завершения работы агента.
  - Код завершения процесса агента.
- Параметры фильтрации событий:
  - Имена модулей.
  - Полные пути к объектам.
  - MD5 и SHA256-хеши объектов.
  - Идентификаторы записей в журнале событий Windows.
  - Параметры цифровых сертификатов.
  - Направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам.
  - Имена пользователей.
  - Типы входа пользователей.
  - Типы событий телеметрии, для которых применяются фильтры.

Данные из запросов от EDR Expert к встроенному агенту Kaspersky Industrial CyberSecurity for Nodes

- Общие параметры задач:
  - Типы задач.
  - Параметры расписания запуска задач.
  - Имена и пароли учетных записей, под которыми необходимо запускать задачи.
  - Версии параметров.
  - Идентификаторы объектов на карантине.

- Пути к объектам.
- MD5 и SHA256-хеши объектов.
- Командная строка запуска процесса с аргументами.
- Флаги дополнительных действий, выполняемых по завершении задачи.
- Идентификаторы IOC-файлов, которые нужно получить с сервера.
- IOC-файлы.
- Наименование служб.
- Тип запуска служб.
- Папки, для которых необходимо получить результаты задачи *Сбор форензик*.
- Маски имен объектов и расширений для задачи *Сбор форензик*.

- Параметры Сетевой изоляции:
  - Типы параметров.
  - Версии параметров.
  - Списки исключений из Сетевой изоляции и параметры исключений: направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам.
  - Флаги дополнительных действий.
  - Время автоматического отключения изоляции.
- Параметры Запрета запуска объектов:
  - Типы параметров.
  - Версии параметров.
  - Списки правил Запрета запуска объектов и параметры правил: пути к объектам, типы объектов, MD5 и SHA256-хеши объектов.
  - Флаги дополнительных действий.

Данные из запросов от Kaspersky Industrial CyberSecurity for Nodes к компоненту EDR Expert

При интеграции с решением EDR Expert (on-premises) следующие данные хранятся локально на компьютерах.

- В запросах на синхронизацию:
  - Уникальный идентификатор.
  - Базовая часть веб-адреса сервера.

- Имя компьютера.
- IP-адрес компьютера.
- MAC-адрес компьютера.
- Локальное время на компьютере.
- Статус самозащиты Kaspersky Industrial CyberSecurity for Nodes.
- Имя и версия операционной системы, установленной на компьютере.
- Версия Kaspersky Industrial CyberSecurity for Nodes.
- Версии параметров приложения и параметров задач.
- Состояние задач (идентификаторы задач, статусы выполнения, коды ошибок).

- В запросах на получение файлов с сервера:
  - Уникальные идентификаторы файлов.
  - Уникальный идентификатор Kaspersky Industrial CyberSecurity for Nodes.
  - Уникальные идентификаторы задач.
  - Базовая часть веб-адреса сервера с компонентом Central Node.
  - IP-адрес узла.
- В отчетах о результатах выполнения задач:
  - IP-адрес узла.
  - Информация об объектах, обнаруженных при поиске IOC или YARA-проверке.
  - Флаги дополнительных действий, выполняемых по завершении задач.
  - Ошибки выполнения задач и коды возврата.
  - Статусы, с которыми завершались задачи.
  - Время завершения выполнения задач.
  - Версии параметров, с которыми выполнялись задачи.
  - Информация об объектах, переданных на сервер, помещенных на карантин, восстановленных из карантина: пути к объектам, MD5 и SHA256-хеши объектов, идентификаторы объектов на карантине.
  - Информация о процессах, запущенных или остановленных на компьютере по запросу сервера: PID и UniquePID, код ошибки, MD5 и SHA256-хеши объектов.
  - Информация о службах, запущенных или остановленных на компьютере по запросу сервера (имя службы, тип запуска, код ошибки, MD5 и SHA256-хеши файловых образов служб).

- Информация об объектах, для которых был снят дамп памяти для YARA-проверки (пути, идентификатор файла дампа).
- Файлы, запрошенные сервером.

- Данные о запущенных процессах:
  - Имя исполняемого файла, включая полный путь и расширение.
  - Параметры автозапуска процесса.
  - Идентификатор процесса.
  - Код сеанса входа в систему.
  - Имя сеанса входа в систему.
  - Дата и время запуска процесса.
  - MD5 и SHA256-хеши объекта.
- Данные о файлах:
  - Путь к файлу.
  - Имя файла.
  - Размер файла.
  - Атрибуты файла.
  - Дата и время создания файла.
  - Дата и время последнего изменения файла.
  - Описание файла.
  - Название компании.
  - MD5 и SHA256-хеши объекта.
  - Раздел реестра (для точек автозапуска).
- Данные в ошибках получения информации об объектах:
  - Полное имя объекта, при обработке которого возникла ошибка.
  - Код ошибки.
- Данные о результатах YARA-проверки:

  Встроенный агент Kaspersky Industrial CyberSecurity for Nodes автоматически передает данные результатов YARA-проверки в Kaspersky Anti Targeted Attack Platform для построения цепочки развития угрозы.

Данные временно хранятся локально в очереди отправки результатов выполнения задач на сервер Kaspersky Anti Targeted Attack Platform. После отправки данные удаляются.

- MD5 и SHA256-хеши файла.
- Полное имя файла.
- Путь к файлу.
- Размер файла.
- Имя процесса.
- Аргументы процесса.
- Путь к файлу процесса.
- Windows идентификатор процесса (PID).
- Windows идентификатор родительского процесса (PID).
- Имя учетной записи пользователя, запустившего процесс.
- Дата и время запуска процесса.

- Данные о результатах IOC проверки:
  - IP-адрес из ARP-таблицы.
  - Физический адрес из ARP-таблицы.
  - Имя DNS-записи.
  - Тип DNS-записи.
  - Имя хоста.
  - IP-адрес.
  - Идентификатор события в журнале.
  - Имя источника данных в журнале.
  - Имя журнала.
  - Имя пользователя.
  - Дата и время генерации события в формате ISO.
  - MD5 и SHA256-хеши файла.
  - Полное имя файла.
  - Размер файла.

- Удаленный IP и порт, с которым установлено соединение в момент проверки.
- IP и порт локального адаптера.
- Протокол.
- Имя процесса.
- Аргументы процесса.
- Путь к файлу процесса.
- Windows идентификатор процесса (PID).
- Windows идентификатор родительского процесса (PID).
- Имя учетной записи пользователя, запустившего процесс.
- Дата и время запуска процесса.
- Путь к ключу реестра.
- Имя ключа реестра.
- Текстовое значение ключа реестра.
- Имя сервиса.
- Описание сервиса.
- Путь и имя DLL сервиса.
- Путь и имя исполняемого файла сервиса.
- Windows идентификатор сервиса (PID).
- Тип сервиса.
- Статус сервиса.
- Режим запуска сервиса.
- Название операционной системы.
- Версия операционной системы.
- Сетевое имя компьютера без домена.
- Домен или рабочая группа.
- Имя пользователя.
- Имя тома.

- Буква тома.
- Тип тома.

Интеграция с Kaspersky Industrial CyberSecurity for Networks

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Industrial CyberSecurity for Nodes.

Служебные данные

Встроенный агент Kaspersky Industrial CyberSecurity for Nodes хранит локально следующие данные:

- Данные, необходимые для интеграции с Kaspersky Industrial CyberSecurity for Networks:
  - Адрес и порт для подключения к серверу Kaspersky Industrial CyberSecurity for Networks.
  - Информация о сертификатах для интеграции с Kaspersky Industrial CyberSecurity for Networks.
- Файлы на карантине.

Данные из передаваемых событий телеметрии

- **Данные о файлах**
  - Уникальный идентификатор файла.
  - Тип файла.
  - Полный путь к файлу.
  - Размер файла.
  - Атрибуты файла.
  - ZoneId.
  - Дата и время создания файла.
  - Дата и время последнего изменения файла.
  - Дата и время изменения атрибутов файла.
  - Исходное имя файла.
  - Имя приложения.
  - Версия приложения.
  - Производитель приложения.

- Описание файла.
- Версия файла.
- MD5 и SHA256-хеши объекта.
- Результат проверки подписи файла.
- Дата и время создания подписи файла.
- Цепочки сертификатов, примененные в файле подписи:
  - Тип цепочки сертификатов.
  - Информация о сертификатах в цепочке:
    - Имя издателя сертификата.
    - Имя владельца сертификата.
    - Серийный номер сертификата.
    - Алгоритм отпечатка сертификата.
    - Отпечаток сертификата.
    - Период действия сертификата.

- **Данные о HTTP-запросах**
  - Уникальный идентификатор процесса, отправившего запрос.
  - Локальный IP-адрес и порт.
  - Удаленный IP-адрес и порт.
  - Протокол передачи данных.
  - Направление соединения.
  - Информация о HTTP-запросе:
    - HTTP-метод.
    - Путь без доменного имени.
    - Имя хоста.
    - Список HTTP-заголовков:
      - Имя.
      - Значение.

- **Детали алерта**
  - Идентификатор обнаружения.
  - Дата и время обнаружения.
  - Наименование обнаружения.
  - Режим сканирования.
  - Статус последнего действия, связанного с обнаружением.
  - Причина неудачной обработки обнаружения.
  - Тип объекта.
  - Имя объекта.
  - MD5- и SHA256-хеши объекта.
  - Действия по устранению угрозы.
  - Информация о репутации объекта в Kaspersky Security Network:
    - Группа, в которую помещено приложение.
    - Количество пользователей Kaspersky Security Network, использующих приложение.
    - Страны, в которых приложение наиболее распространено.
    - Дата и время первого появления приложения в Kaspersky Security Network.
    - Дата и время получения информации из Kaspersky Security Network.
- **Данные о сеансах входа в систему**
  - Идентификатор сеанса.
  - Имя учетной записи пользователя, от имени которой осуществлен вход.
  - Тип учетной записи пользователя.
  - Тип сеанса.
  - IP-адрес устройства, с которого была выполнена попытка входа.
  - IP-адрес устройства, для которого была выполнена попытка входа.
  - Информация о том, что этот сеанс имеет повышенные права и администратора.
  - Информация о связанных сеансах входа в систему.
  - Прикладной протокол для удаленного сеанса.
  - Протокол сеанса удаленного доступа.

- **Данные о завершении сеанса**
  - Идентификатор сеанса.
  - Имя учетной записи пользователя, от имени которой осуществлен вход.
  - Тип учетной записи пользователя.
  - Тип сеанса.
  - IP-адрес устройства, с которого была выполнена попытка входа.
  - IP-адрес устройства, для которого была выполнена попытка входа.
  - Информация о том, что этот сеанс имеет повышенные права и администратора.
  - Информация о связанных сеансах входа в систему.
  - Прикладной протокол для удаленного сеанса.
  - Протокол сеанса удаленного доступа.
  - Идентификатор сеанса.
- **Данные о сетевых коммуникациях**
  - Начало и конец временного интервала, за который собирались данные.
  - Список соединений:
    - Локальный IP-адрес компьютера.
    - Локальный MAC-адрес компьютера.
    - Удаленный IP-адрес компьютера.
    - Удаленный MAC-адрес компьютера.
    - IP-адрес шлюза.
    - Количество отправленных пакетов данных.
    - Количество принятых пакетов данных.
    - Общее количество переданных байт.
    - Протокол передачи данных.
    - EtherType.
    - Префикс полезной нагрузки первого пакета в интервале.
    - IPv4-адрес сетевого интерфейса, через который была зафиксирована коммуникация.

- **Данные о сетевых соединениях**
  - Уникальный идентификатор процесса, инициировавшего соединение.
  - Протокол передачи данных.
  - Локальный IP-адрес, через который инициировано соединение.
  - Удаленный IP-адрес конечной точки соединения.
  - Информация о HTTP-запросе:
    - HTTP-метод.
    - Путь без доменного имени.
    - Имя хоста.
    - Список HTTP-заголовков:
      - Имя.
      - Значение.
  - Динамическое состояние процесса в момент соединения.
  - Направление соединения.
  - Состояние динамического процесса.
  - EtherType.
- **Данные, получаемые при прослушивании сетевого порта**
  - Уникальный идентификатор процесса, инициировавшего соединение.
  - Протокол передачи данных.
  - Локальный адрес.
  - Динамическое состояние процесса в момент соединения.
- **Результаты проверки соединения**
  - Сетевые настройки хоста:
    - Описание сетевого интерфейса.
    - DNS-имя домена.
    - Локальный MAC-адрес компьютера.
    - Номер метрики IP-соединения.

- Список IP-адресов:
  - IP-адрес.
  - Сетевая маска.
  - IP-адрес шлюза.
  - MAC-адрес шлюза.
- Список установленных патчей:
  - Номер патча.
  - Дата установки патча.
- Модель устройства.
- Производитель устройства.
- ID хоста в Kaspersky Security Center.
- Описание установленного антивирусного продукта "Лаборатории Касперского":
  - Наименование компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Версия компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Версия базы данных компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Дата последнего обновления базы данных компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Статус компонента установленного антивирусного продукта "Лаборатории Касперского".
  - Список лицензионных ключей:
    - Серийный номер ключа.
    - Тип ключа.
    - Дата истечения срока действия ключа.
    - Статус ключа.
- **Данные о создании процесса**
  - Уникальный идентификатор процесса.
  - Уникальный идентификатор родительского процесса.
  - Уникальный системный идентификатор процесса.
  - Команда, используемая для запуска процесса.

- Идентификатор сеанса входа.
- Идентификатор терминального сеанса.
- Уникальный идентификатор файла процесса.
- Уровень целостности процесса.
- Список прав в токене:
  - Права.
  - Атрибуты прав.
- Список уникальных идентификаторов интерпретируемых файлов.
- Статус процесса.
- Команда, используемая для запуска процесса.

- **Данные о завершении процесса**
  - Уникальный идентификатор зараженного объекта.
- **Данные об обнаруженной угрозе**
  - Информация об угрозе:
    - Вердикт, присвоенный угрозе.
    - Номер записи AMR.
    - Версия антивирусной базы данных.
    - Режим обнаружения угрозы.
    - UUID угрозы.
    - Технология защиты.
    - Уникальный идентификатор угрозы.
    - Технология защиты.
  - Информация о зараженном объекте:
    - Тип зараженного объекта.
    - Имя зараженного объекта.
    - MD5- и SHA256-хеши объекта.
    - Уникальный идентификатор зараженного процесса.
    - Уникальный идентификатор зараженного объекта.

        - Уникальный идентификатор процесса, скачавшего зараженный объект из интернета.
        - URL, по которому был скачан зараженный объект.
        - Электронный адрес отправителя, приславшего зараженный объект.
        - Тип сетевого протокола (по IANA).
        - Локальный сетевой адрес.
        - Внешний сетевой адрес, с которого был получен зараженный объект.
        - Тип содержимого объекта.
        - Контекст обнаруженной угрозы.
        - Содержание объекта.
    - Флаг, указывающий, что обнаружение угрозы прошло в фоновом режиме.
    - Локальный физический адрес.
    - Физический адрес, с которого был получен зараженный объект.
- **Данные об обработке угрозы**
    - Информация об угрозе:
        - Вердикт, присвоенный угрозе.
        - Номер записи AMR.
        - Версия антивирусной базы данных.
        - Режим обнаружения угрозы.
        - UUID угрозы.
        - Технология защиты.
    - Информация о зараженном объекте:
        - Тип зараженного объекта.
        - Имя зараженного объекта.
        - MD5- и SHA256-хеши объекта.
        - Уникальный идентификатор зараженного процесса.
        - Уникальный идентификатор зараженного объекта.
        - Тип сетевого протокола (по IANA).

        - Внешний сетевой адрес, с которого был получен зараженный объект.
        - Локальный сетевой адрес.
    - Статус обработки угрозы.
    - Причина невозможности исправления угрозы.
    - Локальный физический адрес.
- **Данные о пользователях**
    - SID пользователя.
    - Идентификатор пользователя.
    - Имя пользователя.
    - Полное имя пользователя.
    - Описание пользователя.
    - Включена или выключена учетная запись.
    - Заблокирована ли учетная запись.
    - Истекает или нет срок действия пароля.
    - Требуется ли смена пароля.
    - Доступна ли для пользователя возможность смены пароля.
    - Тип учетной записи пользователя.
    - Включен ли автоматический вход под данной учетной записью.
    - Список групп, к которым принадлежит пользователь.
    - Дата последней смены пароля.
    - Дата последнего завершения сеанса.

Данные из запросов от Kaspersky Industrial CyberSecurity for Networks к встроенному агенту Kaspersky Industrial CyberSecurity for Nodes

- Общие параметры задач:
    - Типы задач.
    - Параметры расписания запуска задач.
    - Имена и пароли учетных записей, под которыми необходимо запускать задачи.
    - Версии параметров.

- Идентификаторы объектов на карантине.
- Пути к объектам.
- MD5 и SHA256-хеши объектов.
- Командная строка запуска процесса с аргументами.
- Флаги дополнительных действий, выполняемых по завершении задачи.
- Наименование служб.
- Тип запуска служб.

- Параметры Сетевой изоляции:
  - Типы параметров.
  - Версии параметров.
  - Списки исключений из Сетевой изоляции и параметры исключений: направление трафика, IP-адреса, порты, протоколы, полные пути к исполняемым файлам.
  - Флаги дополнительных действий.
  - Время автоматического отключения изоляции.
- Параметры Запрета запуска объектов:
  - Типы параметров.
  - Версии параметров.
  - Списки правил Запрета запуска объектов и параметры правил: пути к объектам, типы объектов, MD5 и SHA256-хеши объектов.
  - Флаги дополнительных действий.

Данные из запросов от Kaspersky Industrial CyberSecurity for Nodes к Kaspersky Industrial CyberSecurity for Networks

При интеграции с Kaspersky Industrial CyberSecurity for Networks следующие данные хранятся локально на компьютерах.

- В запросах на синхронизацию:
  - Уникальный идентификатор.
  - Базовая часть веб-адреса сервера.
  - Имя компьютера.
  - IP-адрес компьютера.

- MAC-адрес компьютера.
- Локальное время на компьютере.
- Статус самозащиты Kaspersky Industrial CyberSecurity for Nodes.
- Имя и версия операционной системы, установленной на компьютере.
- Версия Kaspersky Industrial CyberSecurity for Nodes.
- Версии параметров приложения и параметров задач.
- Состояние задач (идентификаторы задач, статусы выполнения, коды ошибок).

- В запросах на получение файлов с сервера:
  - Уникальные идентификаторы файлов.
  - Уникальный идентификатор Kaspersky Industrial CyberSecurity for Nodes.
  - Уникальные идентификаторы задач.
  - Базовая часть веб-адреса сервера с компонентом Central Node.
  - IP-адрес узла.
- В отчетах о результатах выполнения задач:
  - IP-адрес узла.
  - Флаги дополнительных действий, выполняемых по завершении задач.
  - Ошибки выполнения задач и коды возврата.
  - Статусы, с которыми завершались задачи.
  - Время завершения выполнения задач.
  - Версии параметров, с которыми выполнялись задачи.
  - Информация об объектах, переданных на сервер, помещенных на карантин, восстановленных из карантина: пути к объектам, MD5 и SHA256-хеши объектов, идентификаторы объектов на карантине.
  - Информация о процессах, запущенных или остановленных на компьютере по запросу сервера: PID и UniquePID, код ошибки, MD5 и SHA256-хеши объектов.
  - Информация о службах, запущенных или остановленных на компьютере по запросу сервера (имя службы, тип запуска, код ошибки, MD5 и SHA256-хеши файловых образов служб).
  - Файлы, запрошенные сервером.

- Данные о запущенных процессах:
  - Имя исполняемого файла, включая полный путь и расширение.
  - Параметры автозапуска процесса.
  - Идентификатор процесса.
  - Код сеанса входа в систему.
  - Имя сеанса входа в систему.
  - Дата и время запуска процесса.
  - MD5 и SHA256-хеши объекта.
- Данные о файлах:
  - Путь к файлу.
  - Имя файла.
  - Размер файла.
  - Атрибуты файла.
  - Дата и время создания файла.
  - Дата и время последнего изменения файла.
  - Описание файла.
  - Название компании.
  - MD5 и SHA256-хеши объекта.
  - Раздел реестра (для точек автозапуска).
- Данные в ошибках получения информации об объектах:
  - Полное имя объекта, при обработке которого возникла ошибка.
  - Код ошибки.

Интеграция с SIEM

Все данные, которые приложение хранит локально на компьютере, будут удалены с компьютера при удалении Kaspersky Industrial CyberSecurity for Nodes.

При интеграции с SIEM-системами передаются данные о настройках подключения, а также все события, зарегистрированные в журналах Windows.

Основные журналы событий Windows: System, Security, Application, ForwardedEvents и HardwareEvents. Также пользователи могут создавать и работать с индивидуальными журналами в соответствии со своими требованиями.

Предоставление данных при использовании Kaspersky Security Network

Набор данных, которые Kaspersky Industrial CyberSecurity for Nodes передает в "Лабораторию Касперского", зависят от типа лицензии и параметров использования Kaspersky Security Network.

Использование KSN по лицензии не более чем на 4 компьютера

Принимая Положение о Kaspersky Security Network, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

- информацию об обновлении конфигурации KSN: идентификатор действующей конфигурации, идентификатор полученной конфигурации, код ошибки обновления конфигурации;
- информацию о проверяемых файлах и URL-адресах: контрольные суммы проверяемого файла (MD5, SHA2-256, SHA1) и паттернов файла (MD5), размер паттерна, тип обнаруженной угрозы и ее название согласно классификации Правообладателя, идентификатор антивирусных баз, URL-адрес, по которому запрашивается репутация, а также URL-адрес страницы, с которой осуществлен переход на проверяемый URL-адрес, идентификатор протокола соединения и номер используемого порта;
- идентификатор задачи проверки, в которой обнаружена угроза;
- информацию об используемых цифровых сертификатах, необходимую для проверки их подлинности: контрольные суммы (SHA256) сертификата, которым подписан проверяемый объект, и открытого ключа сертификата;
- идентификатор компонента ПО, выполняющего сканирование;
- идентификаторы антивирусных баз и записей в антивирусных базах;
- информацию об активации ПО на Компьютере: подписанный заголовок тикета от службы активации (идентификатор регионального центра активации, контрольную сумму кода активации, контрольную сумму тикета, дату создания тикета, уникальный идентификатор тикета, версию тикета, статус лицензии, дату и время начала / окончания действия тикета, уникальный идентификатор лицензии, версию лицензии), идентификатор сертификата, которым подписан заголовок тикета, контрольную сумму (MD5) файла ключа;
- информацию о ПО Правообладателя: полную версию, тип, версию используемого протокола соединения с сервисами "Лаборатории Касперского".

Использование KSN по лицензии на 5 компьютеров и более

Принимая Положение о Kaspersky Security Network, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

Если флажок **Kaspersky Security Network** установлен, а флажок **Включить расширенный режим KSN** снят, приложение передает следующую информацию:

- информацию об обновлении конфигурации KSN: идентификатор действующей конфигурации, идентификатор полученной конфигурации, код ошибки обновления конфигурации;
- информацию о проверяемых файлах и URL-адресах: контрольные суммы проверяемого файла (MD5, SHA2-256, SHA1) и паттернов файла (MD5), размер паттерна, тип обнаруженной угрозы и ее название согласно классификации Правообладателя, идентификатор антивирусных баз, URL-адрес, по которому запрашивается репутация, а также URL-адрес страницы, с которой осуществлен переход на проверяемый URL-адрес, идентификатор протокола соединения и номер используемого порта;
- идентификатор задачи проверки, в которой обнаружена угроза;
- информацию об используемых цифровых сертификатах, необходимую для проверки их подлинности: контрольные суммы (SHA256) сертификата, которым подписан проверяемый объект, и открытого ключа сертификата;
- идентификатор компонента ПО, выполняющего сканирование;
- идентификаторы антивирусных баз и записей в антивирусных базах;
- информацию об активации ПО на Компьютере: подписанный заголовок тикета от службы активации (идентификатор регионального центра активации, контрольную сумму кода активации, контрольную сумму тикета, дату создания тикета, уникальный идентификатор тикета, версию тикета, статус лицензии, дату и время начала / окончания действия тикета, уникальный идентификатор лицензии, версию лицензии), идентификатор сертификата, которым подписан заголовок тикета, контрольную сумму (MD5) файла ключа;
- информацию о ПО Правообладателя: полную версию, тип, версию используемого протокола соединения с сервисами "Лаборатории Касперского".

Если в дополнение к флажку **Kaspersky Security Network** установлен флажок **Включить расширенный режим KSN**, приложение дополнительно к перечисленному выше передает следующую информацию:

- информацию о результатах категоризации запрашиваемых веб-ресурсов, которая содержит проверяемый URL-адрес и IP-адрес хоста, версию компонента ПО, выполнившего категоризацию, способ категоризации и набор категорий, определенных для веб-ресурса;
- информацию об установленном на Компьютере программном обеспечении: название программного обеспечения и его производителей, используемые ключи реестра и их значения, информацию о файлах компонентов установленного программного обеспечения (контрольные суммы (MD5, SHA2-256, SHA1), имя, путь к файлу на Компьютере, размер, версию и цифровую подпись);
- информацию о состоянии антивирусной защиты Компьютера: версии, даты и время выпуска используемых антивирусных баз, идентификатор задачи и идентификатор ПО, выполняющего сканирование;
- информацию о загружаемых Пользователем файлах: URL- и IP-адреса, откуда была выполнена загрузка, и URL-адрес страницы, с которой был выполнен переход на страницу загрузки файла, идентификатор протокола загрузки и номер порта соединения, признак вредоносности адресов, атрибуты и размер файла и его контрольные суммы (MD5, SHA2-256, SHA1), информацию о процессе, загрузившем файл (контрольные суммы (MD5, SHA2-256, SHA1), дата и время создания и линковки, признак нахождения в автозапуске, атрибуты, имена упаковщиков, информация о подписи, признак исполняемого файла, идентификатор формата, тип учетной записи, от имени которой был запущен процесс), информацию о файле процесса (имя, путь к файлу и размер), имя файла, путь к файлу на Компьютере, цифровая подпись файла и информация о выполнении подписи, URL-адрес, на котором произошло обнаружение, номер скрипта на странице, оказавшегося подозрительным или вредоносным;

- информацию о запускаемых приложениях и их модулях: данные о запущенных процессах в системе (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, приложению и команде, запустившей процесс, а также признак доверенности приложения или процесса, полный путь к файлам процесса и их контрольные суммы (MD5, SHA2-256, SHA1), командная строка запуска, уровень целостности процесса, описание продукта, к которому относится процесс (название продукта и данные об издателе), а также данные об используемых цифровых сертификатах и информацию, необходимую для проверки их подлинности, или данные об отсутствии цифровой подписи файла), также информацию о загружаемых в процессы модулях (имя, размер, тип, дата создания, атрибуты, контрольные суммы (MD5, SHA2-256, SHA1), путь), информация заголовка PE-файлов, названия упаковщика (если файл был упакован);

- информацию обо всех потенциально вредоносных объектах и действиях: название детектируемого объекта и полный путь к объекту на Компьютере, контрольные суммы обрабатываемых файлов (MD5, SHA2-256, SHA1), дата и время обнаружения, названия и размер обрабатываемых файлов и пути к ним, код шаблона пути, признак исполняемого файла, признак, является ли объект контейнером, названия упаковщика (если файл был упакован), код типа файла, идентификатор формата файла, идентификаторы антивирусных баз и записей в антивирусных базах, на основании которых было вынесено решение ПО, признак потенциально вредоносного объекта, название обнаруженной угрозы согласно классификации Правообладателя, степень опасности, статус и способ обнаружения, причина включения в анализируемый контекст и порядковый номер файла в контексте, контрольные суммы (MD5, SHA2-256, SHA1), имя и атрибуты исполняемого файла приложения, через которое прошло зараженное сообщение или ссылка, IP-адреса (IPv4 и IPv6) хоста заблокированного объекта, энтропия файла, признак нахождения файла в автозапуске, время первого обнаружения файла в системе, количество запусков файла с момента последней отправки статистик, тип компилятора, информация о названии, контрольных суммах (MD5, SHA2-256, SHA1) и размере почтового клиента, через который был получен вредоносный объект, идентификатор задачи ПО, которое выполнило проверку, признак проверки репутации или подписи файла, результаты статического анализа содержимого объекта, паттерны объекта, размер паттерна в байтах, технические характеристики по применяемым технологиям детектирования;

- информацию о проверенных объектах: присвоенную группу доверия, в которую помещен и/или из которой перемещен файл, причина, по которой файл помещен в данную категорию, идентификатор категории, информация об источнике категорий и версии базы категорий, признак наличия у файла доверенного сертификата, название производителя файла, версия файла, имя и версия приложения, частью которого является файл;

- информацию об обнаруженных уязвимостях: идентификатор уязвимости в базе уязвимостей, класс опасности уязвимости;

- информацию о выполнении эмуляции исполняемого файла: размер файла и его контрольные суммы (MD5, SHA2-256, SHA1), версия компонента эмуляции, глубина эмуляции, вектор характеристик логических блоков и функций внутри логических блоков, полученный в ходе эмуляции, данные из структуры PE-заголовка исполняемого файла;

- информацию о сетевых атаках: IP-адреса атакующего компьютера (IPv4 и IPv6), номер порта Компьютера, на который была направлена сетевая атака, идентификатор протокола IP-пакета, в котором зафиксирована атака, цель атаки (название организации, веб-сайт), флаг реакции на атаку, весовой уровень атаки, значение уровня доверия;

- информацию об атаках, связанных с подменой сетевых ресурсов, DNS- и IP-адреса (IPv4 или IPv6) посещаемых веб-сайтов;

- DNS- и IP-адреса (IPv4 или IPv6) запрашиваемого веб-ресурса, информацию о файле и веб-клиенте, обращающемся к веб-ресурсу: название, размер, контрольные суммы (MD5, SHA2-256, SHA1) файла, полный путь к нему и код шаблона пути, результат проверки его цифровой подписи и его статус в KSN;

- информацию о выполнении отката деятельности вредоносного приложения: данные о файле, активность которого откатывается (имя файла, полный путь к нему, его размер и контрольные суммы (MD5, SHA2-256, SHA1)), данные об успешных и неуспешных действиях по удалению, переименованию и копированию файлов и восстановлению значений в реестре (имена ключей реестра и их значения), информация о системных файлах, измененных вредоносным приложением, до и после выполнения отката;

- информацию об исключениях для правил компонента Адаптивный контроль аномалий: идентификатор и статус сработавшего правила, действие ПО при срабатывании правила, тип учетной записи, от имени которой процесс или поток выполняет подозрительные действия, информацию о процессе, выполнившем подозрительные действия, и о процессе, в отношении которого были выполнены подозрительные действия (идентификатор скрипта или имя файла процесса, полный путь к файлу процесса, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) файла процесса), информацию об объекте, от имени которого были выполнены подозрительные действия, и об объекте, в отношении которого были выполнены подозрительные действия (название ключа реестра или имя файла, полный путь к файлу, код шаблона пути и контрольные суммы (MD5, SHA2-256, SHA1) файла);

- информацию о загружаемых ПО модулях: название, размер и контрольные суммы (MD5, SHA2-256, SHA1) файла модуля, полный путь к нему и код шаблона пути, параметры цифровой подписи файла модуля, дата и время создания подписи, название субъекта и организации, подписавших файл модуля, идентификатор процесса, в который был загружен модуль, название поставщика модуля, порядковый номер модуля в очереди загрузки;

- информацию о качестве работы ПО с сервисами KSN: дату и время начала и окончания периода формирования статистики, информацию о качестве запросов и соединения с каждым из используемых сервисов KSN (идентификатор сервиса KSN, количество успешных запросов, количество запросов с ответами из кеша, количество неуспешных запросов (сетевые проблемы, выключен KSN в параметрах ПО, неправильная маршрутизация), распределение по времени успешных запросов, распределение по времени отмененных запросов, распределение по времени запросов, превысивших ограничение на время ожидания, количество подключений к KSN, взятых из кеша, количество успешных подключений к KSN, количество неуспешных подключений к KSN, количество успешных транзакций, количество неуспешных транзакций, распределение по времени успешных подключений к KSN, распределение по времени неуспешных подключений к KSN, распределение по времени успешных транзакций, распределение по времени неуспешных транзакций);

- в случае обнаружения потенциально вредоносного объекта предоставляется информация о данных в памяти процессов: элементы иерархии системных объектов (ObjectManager), данные памяти UEFI BIOS, названия ключей реестра и их значения;

- информацию о событиях в системных журналах: время события, название журнала, в котором обнаружено событие, тип и категория события, название источника события и его описание;

- информацию о сетевых соединениях: версия и контрольные суммы (MD5, SHA2-256, SHA1) файла процесса, открывшего порт, путь к файлу процесса и его цифровая подпись, локальный и удаленный IP-адреса, номера локального и удаленного портов соединения, состояние соединения, время открытия порта;

- информацию о дате установки и активации ПО на Компьютере: идентификатор партнера, у которого приобретена лицензия, серийный номер лицензии, подписанный заголовок тикета от службы активации (идентификатор регионального центра активации, контрольную сумму кода активации, контрольную сумму тикета, дату создания тикета, уникальный идентификатор тикета, версию тикета, статус лицензии, дату и время начала / окончания действия тикета, уникальный идентификатор лицензии, версию лицензии), идентификатор сертификата, которым подписан заголовок тикета, контрольную сумму (MD5) файла ключа, уникальный идентификатор установки ПО на Компьютере, тип и идентификатор обновляемого приложения, идентификатор задачи обновления;

- информацию о наборе всех установленных обновлений, а также о наборе последних установленных и/или удаленных обновлений, тип события, служащего причиной отправки информации об обновлениях, период времени, прошедший после установки последнего обновления, информацию о загруженных в момент предоставления информации антивирусных базах;

- информацию о работе ПО на Компьютере: данные по использованию процессора (CPU), данные по использованию памяти (Private Bytes, Non-Paged Pool, Paged Pool), количество активных потоков в процессе ПО и потоков в состоянии ожидания, длительность работы ПО до возникновения ошибки, признак работы ПО в интерактивном режиме;

- количество дампов ПО и дампов системы (BSOD) с момента установки ПО и с момента последнего обновления, идентификатор и версия модуля ПО, в котором произошел сбой, стек памяти в продуктовом процессе и информация об антивирусных базах в момент сбоя;

- данные о дампе системы (BSOD): признак возникновения BSOD на Компьютере, имя драйвера, вызвавшего BSOD, адрес и стек памяти в драйвере, признак длительности сессии ОС до возникновения BSOD, стек памяти падения драйвера, тип сохраненного дампа памяти, признак того, что сессия работы ОС до BSOD длилась более 10 минут, уникальный идентификатор дампа, дата и время возникновения BSOD;

- данные об ошибках или проблемах с производительностью, возникших в работе компонентов ПО: идентификатор состояния ПО, тип, код и причина ошибки, а также время ее возникновения, идентификаторы компонента, модуля и процесса продукта, в котором возникла ошибка, идентификатор задачи или категории обновления, при выполнении которой возникла ошибка, логи драйверов, используемых ПО (код ошибки, имя модуля, имя исходного файла и строка, где произошла ошибка);

- данные об обновлениях антивирусных баз и компонент ПО: имена, даты и время индексных файлов, загруженных в результате последнего обновления и загружаемых в текущем обновлении;

- информацию об аварийных завершениях работы ПО: дату и время создания дампа, его тип, тип события, вызвавшего аварийное завершение работы ПО (непредвиденное отключение питания, падение приложения стороннего правообладателя), дату и время непредвиденного отключения питания;

- информацию о совместимости драйверов ПО с аппаратным и программным обеспечением: информацию о свойствах ОС, накладывающих ограничения на функциональность компонентов ПО (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), тип встроенного ПО загрузки (UEFI, BIOS), признак наличия доверенного платформенного модуля (Trusted Platform Module, TPM), версия спецификации TPM, информацию об установленном на компьютере центральном процессоре (CPU), режим и параметры работы Code Integrity и Device Guard, режим работы драйверов и причина использования текущего режима, версию драйверов ПО, статус поддержки драйверами программных и аппаратных средств виртуализации Компьютера;

- информацию о сторонних приложениях, вызвавших ошибку: их название, версию и локализацию, код ошибки и информацию о ней из системного журнала приложений, адрес возникновения ошибки и стек памяти стороннего приложения, признак возникновения ошибки в компоненте ПО, длительность работы стороннего приложения до возникновения ошибки, контрольные суммы (MD5, SHA2-256, SHA1) образа процесса приложения, в котором произошла ошибка, путь к этому образу процесса приложения и код шаблона пути, информацию из системного журнала ОС с описанием ошибки, связанной с приложением, информацию о модуле приложения, в котором произошла ошибка (идентификатор ошибки, адрес ошибки как смещение в модуле, имя и версию модуля, идентификатор падения приложения в плагине Правообладателя и стек памяти такого падения, время работы приложения до сбоя);

- версию компонента обновления ПО, количество аварийных завершений работы компонента обновления ПО при выполнении задач обновления за время работы компонента, идентификатор типа задачи обновления, количество неуспешных завершений задач обновления компонента обновления ПО;

- информацию о работе компонентов мониторинга системы: полные версии компонентов, дату и время запуска компонентов, код события, которое переполнило очередь событий, и количество таких событий, общее количество переполнений очереди событий, информация о файле процесса-инициатора события (название файла и путь к нему на Компьютере, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) процесса, связанного с файлом, версия файла), идентификатор выполненного перехвата события, полная версия фильтра перехвата, идентификатор типа перехваченного события, размер очереди событий и количество событий между первым событием в очереди и текущим событием, количество просроченных событий в очереди, информация о процессе-инициаторе текущего события (название файла процесса и путь к нему на Компьютере, код шаблона пути, контрольные суммы (MD5, SHA2-256, SHA1) процесса), время обработки события, максимально допустимое время обработки событий, значение вероятности отправки данных, информацию о событиях ОС, время обработки которых ПО превысило ограничение на время ожидания (дата и время получения события, количество повторных инициализаций антивирусных баз, дату и время последней повторной инициализации антивирусных баз после их обновления, время задержки обработки события каждым компонентом мониторинга системы, количество ожидающих событий, количество обработанных событий, количество задержанных событий текущего типа, суммарное время задержки событий текущего типа, суммарное время задержки всех событий);

- информацию от инструмента трассировки событий Windows (Event Tracing for Windows, ETW) при проблемах с производительностью ПО, поставщики событий SysConfig / SysConfigEx / WinSATAssessment от Microsoft: данные о компьютере (модель, производитель, форм-фактор корпуса, версия), данные о метриках производительности Windows (данные WinSAT-оценки, индекс производительности Windows), имя домена, данные о физических и логических процессорах (количество физических и логических процессоров, производитель, модель, степпинг, количество ядер, тактовая частота, идентификатор процессора (CPUID), характеристики кеша, характеристики логического процессора, признаки поддержки режимов и инструкций), данные о модулях оперативной памяти (тип, форм-фактор, производитель, модель, объем, гранулярность выделения памяти), данные о сетевых интерфейсах (IP- и MAC-адреса, название, описание, конфигурация сетевых интерфейсов, распределение числа и объема сетевых пакетов по типам, скорость сетевого обмена, распределение числа сетевых ошибок по типам), конфигурацию IDE-контроллера, IP-адреса DNS-серверов, данные о видеокарте (модель, описание, производитель, совместимость, объем видеопамяти, разрешение экрана, количество бит на пиксель, версия BIOS), данные о подключенных самонастраиваемых (Plug-and-Play) устройствах (название, описание, идентификатор устройства [PnP, ACPI], данные о дисках и накопителях (количество дисков или флеш-накопителей, производитель, модель, объем диска, число цилиндров, число дорожек на цилиндр, число секторов на дорожку, объем сектора, характеристики кеша, порядковый номер, число разделов, конфигурация контролера SCSI), данные о логических дисках (порядковый номер, объем раздела, объем тома, буква тома, тип раздела, тип файловой системы, количество кластеров, размер кластера, число секторов в кластере, число занятых и свободных кластеров, буква загрузочного тома, адрес-смещение раздела относительно начала диска), данные о BIOS материнской платы (производитель, дата выпуска, версия), данные о материнской плате (производитель, модель, тип), данные о физической памяти (общий и свободный объем), данные о службах операционной системы (имя, описание, статус, тег, данные о процессах [имя и идентификатор PID]), параметры энергопотребления компьютера, конфигурацию контролера прерываний, пути к системным папкам Windows (Windows и System32), данные об ОС (версия, сборка, дата выпуска, название, тип, дата установки), размер файла подкачки, данные о мониторах (количество, производитель, разрешение экрана, разрешающая способность, тип), данные о драйвере видеокарты (производитель, дата выпуска, версия);

- информацию от ETW, поставщики событий EventTrace / EventMetadata от Microsoft: данные о последовательности системных событий (тип, время, дата, часовой пояс), метаданные о файле с результатами трассировки (имя, структура, параметры трассировки, распределение числа операций трассировки по типам), данные об ОС (название, тип, версия, сборка, дата выпуска, время старта);

- информацию от ETW, поставщики событий Process / Microsoft-Windows-Kernel-Process / Microsoft-Windows-Kernel-Processor-Power от Microsoft: данные о запускаемых и завершаемых процессах (имя, идентификатор PID, параметры старта, командная строка, код возврата, параметры управления питанием, время запуска и завершения, тип маркера доступа, идентификатор безопасности SID, идентификатор сеанса SessionID, число установленных дескрипторов), данные об изменении приоритетов потоков (идентификатор потока TID, приоритет, время), данные о дисковых операциях процесса (тип, время, объем, число), история изменения структуры и объема используемой процессом памяти;

- информацию от ETW, поставщики событий StackWalk / Perfinfo от Microsoft: данные счетчиков производительности (производительность отдельных участков кода, последовательность вызовов функций, идентификатор процесса PID, идентификатор потока TID, адреса и атрибуты обработчиков прерываний ISR и отложенных вызовов процедур DPC);

- информацию от ETW, поставщик событий KernelTraceControl-ImageID от Microsoft: данные об исполняемых файлах и динамических библиотеках (имя, размер образа, полный путь), данные о PDB-файлах (имя, идентификатор), данные ресурса VERSIONINFO исполняемого файла (название, описание, производитель, локализация, версия и идентификатор приложения, версия и идентификатор файла);

- информацию от ETW, поставщики событий FileIo / DiskIo / Image / Windows-Kernel-Disk от Microsoft: данные о файловых и дисковых операциях (тип, объем, время начала, время завершения, длительность, статус завершения, идентификатор процесса PID, идентификатор потока TID, адреса вызовов функций драйвера, пакет запроса ввода-вывода (I/O Request Packet, IRP), атрибуты файлового объекта Windows), данные о файлах, участвующих в файловых и дисковых операциях (имя, версия, размер, полный путь, атрибуты, смещение, контрольная сумма образа, опции открытия и доступа);

- информацию от ETW, поставщик событий PageFault от Microsoft: данные об ошибках доступа к страницам памяти (адрес, время, объем, идентификатор процесса PID, идентификатор потока TID, атрибуты файлового объекта Windows, параметры выделения памяти);

- информацию от ETW, поставщик событий Thread от Microsoft: данные о создании / завершении потоков, данные о запущенных потоках (идентификатор процесса PID, идентификатор потока TID, размер стека, приоритеты и распределение ресурсов CPU, ресурсов ввода-вывода, страниц памяти между потоками, адрес стека, адрес начальной функции, адрес блока окружения потока (Thread Environment Block, TEB), тег службы Windows);

- информацию от ETW, поставщик событий Microsoft-Windows-Kernel-Memory от Microsoft: данные об операциях управления памятью (статус завершения, время, количество, идентификатор процесса PID), структура распределения памяти (тип, объем, идентификатор сеанса SessionID, идентификатор процесса PID);

- информацию о работе ПО при появлении проблем с производительностью: идентификатор установки ПО, тип и значение снижения производительности, данные о последовательности внутренних событий ПО (время, часовой пояс, тип, статус завершения, идентификатор компонента ПО, идентификатор сценария работы ПО, идентификатор потока TID, идентификатор процесса PID, адреса вызовов функций), данные о проверяемых сетевых соединениях (URL, направление соединения, размер сетевого пакета), данные о PDB-файлах (имя, идентификатор, размер образа исполняемого файла), данные о проверяемых файлах (имя, полный путь, контрольная сумма), параметры мониторинга производительности ПО;

- информацию о неуспешной последней перезагрузке ОС: количество неуспешных перезагрузок с момента установки ОС, данные о дампе системы (код и параметры ошибки, имя, версия и контрольная сумма (CRC32) модуля, вызвавшего ошибку в работе ОС, адрес ошибки как смещение в модуле, контрольные суммы (MD5, SHA2-256, SHA1) дампа системы);

- информацию для проверки подлинности сертификатов, которыми подписаны файлы: отпечаток сертификата, алгоритм вычисления контрольной суммы, публичный ключ и серийный номер сертификата, имя эмитента сертификата, результат проверки сертификата и идентификатор базы сертификатов;

- информацию о процессе, выполняющем атаку на самозащиту ПО: имя и размер файла процесса, его контрольные суммы (MD5, SHA2-256, SHA1), полный путь к нему и код шаблона пути, даты и время создания и компоновки файла процесса, код типа файла процесса, признак исполняемого файла, атрибуты файла процесса, информацию о сертификате, которым подписан файл процесса, тип учетной записи, от имени которой процесс или поток выполняет подозрительные действия, идентификатор операций, которые осуществлялись для доступа к процессу, тип ресурса, с которым выполняется операция (процесс, файл, объект реестра, поиск окна с помощью функции FindWindow), имя ресурса, с которым выполняется операция, признак успешности выполнения операции, статус файла процесса и его подписи в KSN;

- информацию о ПО Правообладателя: полную версию, тип, локализацию и статус работы используемого ПО, версии установленных компонентов ПО и статус их работы, данные об установленных обновлениях ПО, а также значение фильтра TARGET, версию используемого протокола соединения с сервисами Правообладателя;

- информацию об установленном на Компьютере аппаратном обеспечении: тип, название, модель, версию прошивки, характеристики встроенных и подключенных устройств, уникальный идентификатор Компьютера, на котором установлено ПО;

- информацию о версии установленной на Компьютере операционной системы (ОС) и установленных пакетов обновлений, разрядность, редакцию и параметры режима работы ОС, версию и контрольные суммы (MD5, SHA2-256, SHA1) файла ядра ОС, дату и время запуска ОС;

- исполняемые и неисполняемые файлы целиком или частично;

- участки оперативной памяти Компьютера;

- сектора, участвующие в процессе загрузки операционной системы;

- пакеты данных сетевого трафика;

- веб-страницы и электронные письма, содержащие подозрительные и вредоносные объекты;

- описание классов и экземпляров классов WMI хранилища;

- отчеты об активностях приложений:

  - имя, размер и версия отправляемого файла, его описание и контрольные суммы (MD5, SHA2-256, SHA1), идентификатор формата, название его производителя, название продукта, к которому относится файл, полный путь к файлу на Компьютере и код шаблона пути, дата и время создания и модификации файла;

  - даты и время начала и окончания срока действия сертификата, если отправляемый файл имеет ЭЦП, дата и время подписания, имя эмитента сертификата, информация о владельце сертификата, отпечаток и открытый ключ сертификата и алгоритмы их вычисления, серийный номер сертификата;

  - имя учетной записи, от которой запущен процесс;

  - контрольные суммы (MD5, SHA2-256, SHA1) имени Компьютера, на котором запущен процесс;

  - заголовки окон процесса;

  - идентификатор антивирусных баз, название обнаруженной угрозы согласно классификации Правообладателя;

  - информацию об установленной в ПО лицензии, идентификатор лицензии, ее тип и дата истечения;

  - локальное время Компьютера в момент предоставления информации;

- имена и пути к файлам, к которым получал доступ процесс;
- имена ключей реестра и их значения, к которым получал доступ процесс;
- URL- и IP-адреса, к которым обращался процесс;
- URL- и IP-адреса, с которых был получен запускаемый файл.

Соответствие законодательству Европейского союза (GDPR)

Kaspersky Industrial CyberSecurity for Nodes может передавать данные в "Лабораторию Касперского" при выполнении следующих условий:

- Использование Kaspersky Security Network.
- Активация приложения с помощью кода активации.
- Обновление антивирусных баз и модулей приложения.
- Переход по ссылкам в Консоли приложения.

Вне зависимости от классификации и территории, откуда данные были получены, "Лаборатория Касперского" использует высокий уровень стандартов защиты данных и применяет правовые, организационные и технические меры, чтобы защитить данные пользователей, гарантировать безопасность и конфиденциальность, а также обеспечить выполнение прав пользователей, гарантированных применимым законодательством. Текст Политики конфиденциальности входит в комплект поставки приложения и доступен на веб-сайте "Лаборатории Касперского".

Перед использованием Kaspersky Industrial CyberSecurity for Nodes ознакомьтесь с описанием передаваемых данных в рамках Лицензионного соглашения и использования Kaspersky Security Network (перечислены в Положении о Kaspersky Security Network). Если в соответствии с вашим локальным законодательством или стандартом данные, передаваемые из Kaspersky Industrial CyberSecurity for Nodes в рамках любого из описанных сценариев, могут быть классифицированы как персональные, вам необходимо обеспечить законность их обработки и получить согласие конечных пользователей на сбор и передачу этих данных.

Более подробную информацию о получении, обработке, хранении и уничтожении информации об использовании приложения после принятия Лицензионного соглашения и согласия с Положением о Kaspersky Security Network вы можете узнать, прочитав тексты этих документов, а также на веб-сайте "Лаборатории Касперского". Файлы license.txt и ksn_<ID языка>.txt с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки приложения.

Если вы не хотите предоставлять данные в "Лабораторию Касперского", вы можете выключить передачу данных.

Использование Kaspersky Security Network

Используя Kaspersky Security Network, вы соглашаетесь на автоматическую передачу данных, перечисленных в Положении о Kaspersky Security Network. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", используйте Kaspersky Private Security Network (KPSN) или выключите использование KSN.

Активация приложения с помощью кода активации

Используя код активации, вы соглашаетесь на автоматическую передачу данных в рамках Лицензионного соглашения. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", используйте файл ключа для активации Kaspersky Industrial CyberSecurity for Nodes.

Обновление антивирусных баз и модулей приложения

Используя для обновления серверы "Лаборатории Касперского", вы соглашаетесь на автоматическую передачу данных в рамках Лицензионного соглашения. Информация требуется для проверки правомерности использования приложения Kaspersky Industrial CyberSecurity for Nodes. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", используйте Kaspersky Security Center для обновления баз.

Переход по ссылкам в Консоли приложения

Используя ссылки в Консоли приложения, вы соглашаетесь на автоматическую передачу данных в рамках Лицензионного соглашения. Точный перечень данных, передаваемых в каждой конкретной ссылке, зависит от того, где именно расположена ссылка в Консоли приложения и какую проблему она призвана решить. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", выключите отображение пользовательского интерфейса приложения.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Pentium является товарным знаком Intel Corporation или ее дочерних компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Excel, Forefront, Hyper-V, Internet Explorer, JScript, Lync, Outlook, PowerShell, SharePoint, SQL Server, Windows, Windows Server и Windows Vista, Windows XP являются товарными знаками группы компаний Microsoft.

Schneider Electric – товарный знак компании Schneider Electric.

Siemens, Simatic и WinCC – зарегистрированные товарные знаки Siemens AG.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.