KASPERSKY lab

Kaspersky Industrial CyberSecurity for Nodes

643.46856491.00093-02 90 02

Руководство пользователя

Версия программы: 2.5.0.235

Уважаемый пользователь!

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

Дата редакции документа: 28.06.2018

Обозначение документа: 643.46856491.00093-02 90 02

https://www.kaspersky.ru
https://support.kaspersky.ru

Содержание

Об этом документе

Настоящий документ представляет собой руководство по эксплуатации программного изделия "Kaspersky Industrial CyberSecurity for Nodes 2.5" (далее также "Kaspersky Industrial CyberSecurity for Nodes 2.5", "программа").

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

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

Источники информации о программе

Указанные источники информации о программе (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

О программе

Средство защиты информации «Kaspersky Industrial CyberSecurity for Nodes» (далее также "программа"), представляющее собой средство антивирусной защиты типа «В» третьего класса защиты, предназначенное для применения на автоматизированных рабочих местах информационных систем.

Основными угрозами, для противостояния которым используется Kaspersky Industrial CyberSecurity for Nodes, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и(или) съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ).

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация программы;
- выполнение проверок обращений к интерфейсам взаимодействия с другими системами;
- мониторинг целостности данных, хранимых на программируемых логических контроллерах;
- контроль запуска программ;
- контроль доступа к недоверенным wi-fi сетям;
- контроль выполнения файловых операций;
- защита от эксплойтов.

Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию о правах на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 и службами Windows, которые регистрирует программа, а также инструкции по настройке этих прав.

В этом разделе

О правах на управление Kaspersky Industrial CyberSecurity for Nodes 2.5

По умолчанию доступ ко всем функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, пользователи группы KICS Administrators, созданной на защищаемом компьютере при установке Kaspersky Industrial CyberSecurity for Nodes 2.5, а также системная группа SYSTEM.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Industrial CyberSecurity for Nodes 2.5, могут предоставлять доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Kaspersky Industrial CyberSecurity for Nodes 2.5, он не может открыть Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.

Вы можете выбрать для пользователя или группы пользователей один из следующих предустановленных уровней доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5, параметры работы компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5, права пользователей Kaspersky Industrial CyberSecurity for Nodes 2.5, а также просматривать статистику работы Kaspersky Industrial CyberSecurity for Nodes 2.5.
- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5, параметры работы компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5.
- **Чтение** – возможность просматривать общие параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5, параметры работы компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5, статистику работы Kaspersky Industrial CyberSecurity for Nodes 2.5 и права пользователей Kaspersky Industrial CyberSecurity for Nodes 2.5.

Вы также можете настроить расширенные права доступа: разрешить или запретить доступ к конкретным функциям Kaspersky Industrial CyberSecurity for Nodes 2.5.

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Таблица 1. Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Industrial CyberSecurity for Nodes 2.5.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: • Импортировать в конфигурационный файл параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5. • Редактировать настройки программы.
Чтение параметров	Возможности: • просматривать общие параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5 и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5; • 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 2.5.
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Industrial CyberSecurity for Nodes 2.5.
Удаление программы	Возможность удалить Kaspersky Industrial CyberSecurity for Nodes 2.5.
Чтение прав	Возможность просматривать список пользователей Kaspersky Industrial CyberSecurity for Nodes 2.5 и права доступа каждого пользователя.
Изменение прав	Возможности: • изменять список пользователей, имеющих доступ к управлению программой; • изменять права доступа пользователей к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5.

О правах на управление регистрируемыми службами

Подробная информация о регистрируемых службах Windows и настройке доступа к регистрируемым службам содержится в *Руководстве администратора Kaspersky Industrial CyberSecurity for Nodes 2.5.*

При установке Kaspersky Industrial CyberSecurity for Nodes 2.5 регистрирует в Windows службу Kaspersky Security (KAVFS), службу управления программой Kaspersky Security Management (KAVFSGT) и службу Kaspersky Security Exploit Prevention (KAVFSSLP).

Служба Kaspersky Security

По умолчанию доступ к управлению службой Kaspersky Security имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, а также системные группы SERVICE и INTERACTIVE с правами на чтение и системная группа SYSTEM с правами на чтение и исполнение.

Пользователи, которые имеют доступ к функции уровня Изменение прав (см. раздел "Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью пароля" на стр. 17), могут предоставлять доступ к управлению Kaspersky Security Service другим пользователям, зарегистрированным на защищаемом компьютере или входящим в домен.

Служба Kaspersky Security Management

Чтобы управлять программой через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, установленную на другом компьютере, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Industrial CyberSecurity for Nodes 2.5, имела полный доступ к службе Kaspersky Security Management на защищаемом компьютере.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу "Администраторы" на защищаемом компьютере, и пользователи группы KICS Administrators, созданной на защищаемом компьютере при установке Kaspersky Industrial CyberSecurity for Nodes 2.5.

Вы можете управлять Kaspersky Security Management только через оснастку Службы Microsoft Windows.

Настройка прав доступа на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 и службой Kaspersky Security

Вы можете изменить список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 и управлению службой Kaspersky Security, а также изменять права доступа этих пользователей и групп пользователей.

► *Чтобы добавить в список или удалить из списка пользователя или группу, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:
   - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Industrial CyberSecurity for Nodes 2.5.
   - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению службой Kaspersky Security.

     Откроется окно **Разрешения для группы "Kaspersky Industrial CyberSecurity for Nodes 2.5".**
2. В открывшемся окне выполните следующие действия:
   - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.
   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.
3. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

► *Чтобы изменить права доступа на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 и службой Kaspersky Security, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:
   - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите настроить права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5.
   - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите настроить права доступа к службе Kaspersky Security.

     Откроется окно **Разрешения для группы "Kaspersky Industrial CyberSecurity for Nodes 2.5".**
2. В открывшемся окне в списке **Группы или пользователи** выберите пользователя или группу пользователей, права которых вы хотите изменить.
3. В блоке **Разрешения для группы "<Пользователь (Группа)>"** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
   - Выберите пункт **Изменить права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Industrial CyberSecurity for Nodes 2.5.
   - Выберите пункт **Изменить права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для группы "Kaspersky Industrial CyberSecurity for Nodes 2.5"**.
4. В открывшемся окне в списке **Группы или пользователи** выберите пользователя или группу пользователей, права которых вы хотите изменить.

5. В блоке **Разрешения для группы "<Пользователь (Группа)>"** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:
   - **Полный контроль**: полный набор прав на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 или службой Kaspersky Security.
   - **Чтение**:
     - Следующие разрешения на управление Kaspersky Industrial CyberSecurity for Nodes 2.5: **Чтение статистики**, **Чтение параметров**, **Чтение журналов** и **Чтение прав**.
     - Следующие разрешения на управление службой Kaspersky Security: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Перечисление зависимых служб**, **Чтение прав**.
   - **Изменение**:
     - все права на управление Kaspersky Industrial CyberSecurity for Nodes 2.5, кроме **Изменение прав**;
     - Следующие разрешения на управление службой Kaspersky Security: **Изменение параметров службы**, **Чтение прав**.
   - **Исполнение**: следующие права на управление службой Kaspersky Security: **Запуск службы, Остановка службы**, **Приостановка / возобновление службы**, **Чтение прав**, **Определенные пользователем запросы к службе**.
6. Если вы хотите выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.
   a. В открывшемся окне **Дополнительные параметры безопасности для Kaspersky Industrial CyberSecurity for Nodes 2.5** выберите нужного пользователя или группу.
   b. Нажмите на кнопку **Изменить**.
   c. В раскрывающемся списке в верхней части окна выберите тип контроля доступа (**Разрешить** или **Запретить**).
   d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или группе.
   e. Нажмите на кнопку **OK**.
   f. В окне **Дополнительные параметры безопасности для Kaspersky Industrial CyberSecurity for Nodes 2.5** нажмите на кнопку **OK**.
7. В окне **Разрешения для группы "Kaspersky Industrial CyberSecurity for Nodes"** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 или службой Kaspersky Security будут сохранены.

Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью пароля

Более подробную информацию о защите паролем см. в разделе "Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью пароля" *Руководства администратора*.

Вы можете ограничивать доступ к управлению программой и регистрируемыми службами с помощью настройки прав пользователей (см. раздел "Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 43). Вы также можете дополнительно защитить доступ к выполнению критичных операций, установив защиту паролем в параметрах Kaspersky Industrial CyberSecurity for Nodes 2.5.

► *Чтобы защитить доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:
   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
2. На закладке **Безопасность и надежность** в блоке **Параметры применения пароля** установите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** станут активными.
3. В поле **Пароль** введите значение, которое вы хотите использовать для защиты доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5.
4. В поле **Подтверждение пароля** введите пароль повторно.
5. Нажмите на кнопку **ОК**.

Установленный пароль невозможно восстановить. Утеря пароля ведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого компьютера.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет отключена, и контрольная сумма старого пароля будет удалена. Повторите процесс ввода пароля с новым паролем.

Интерфейс Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию об основных элементах интерфейса программы.

В этом разделе

О Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять программой через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, установленную на защищаемом компьютере или на другом компьютере в сети организации.

Подробную информацию об установке и настройке Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 см. в *Руководстве пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5*.

Если Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 и программа установлены на разных компьютерах, принадлежащих к разным доменам, возможны ограничения в доставке информации от Kaspersky Industrial CyberSecurity for Nodes 2.5 в Консоль. Например, после запуска какой-либо задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 статус этой задачи может не обновиться в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

При установке Консоли мастер установки сохраняет файл kavfs.msc в папке установки и добавляет оснастку Kaspersky Industrial CyberSecurity for Nodes 2.5 в список изолированных оснасток Microsoft® Windows.

Вы можете открыть Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 из меню **Пуск**. Вы можете запустить msc-файл оснастки Kaspersky Industrial CyberSecurity for Nodes 2.5 или добавить оснастку программы в Microsoft Management Console как новый элемент в дереве.

В 64-разрядной версии Microsoft Windows вы можете добавить оснастку Kaspersky Industrial CyberSecurity for Nodes 2.5 только в Microsoft Management Console 32-разрядной версии. Для этого откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

Вы можете добавить несколько оснасток Kaspersky Industrial CyberSecurity for Nodes 2.5 в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких компьютеров, на которых установлена программа Kaspersky Industrial CyberSecurity for Nodes 2.5.

Интерфейс Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 отображается в дереве Microsoft Management Console в виде узла с именем Kaspersky Industrial CyberSecurity for Nodes.

После подключения к программе Kaspersky Industrial CyberSecurity for Nodes 2.5, установленной на другом компьютере, в название узла добавляется имя компьютера, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Industrial CyberSecurity for Nodes <имя компьютера> как <имя учетной записи>**. При подключении к программе Kaspersky Industrial CyberSecurity for Nodes 2.5, установленной на том же компьютере, что и Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, название узла имеет вид Kaspersky Industrial CyberSecurity for Nodes.

По умолчанию окно Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 содержит следующие элементы:

- Дерево Консоли;
- Панель результатов;
- Панель быстрого доступа;
- Панель инструментов.

Также вы можете включить отображение в окне Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 области описания и панели действия.

Дерево Консоли

В дереве Консоли отображается узел Kaspersky Industrial CyberSecurity for Nodes и вложенные в него узлы функциональных компонентов программы.

Узел **Kaspersky Industrial CyberSecurity for Nodes** включает следующие вложенные узлы:

- **Постоянная защита компьютера**: управление задачами Постоянная защита файлов, Защита от шифрования и Использование KSN. Узел Постоянная защита компьютера позволяет управлять следующими задачами:
  - **Постоянная защита файлов**
  - **Использование KSN**
  - **Защита от шифрования**
- **Контроль компьютера**: контроль подключаемых устройств, а также контроль программ, запускаемых на защищаемом компьютере. Узел **Контроль компьютера** позволяет настраивать следующие задачи:
  - **Контроль запуска программ**
  - **Контроль устройств**
  - **Контроль Wi-Fi**
  - **Управление сетевым экраном**

- **Автоматическое формирование правил**: настройка автоматического формирования групповых и системных правил для задач 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 (см. раздел "Категории задач Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 60) создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.
- **Диагностика системы**: настройка контроля файловых операций и анализа системного журнала операционной системы.
  - **Мониторинг файловых операций**
  - **Анализ журналов**
- **Защита промышленной сети**: получает информацию о защищаемых ПЛК и проверяет их целостность.
  - **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 объектов на карантине**
  - **Проверка целостности программы**
  - Пользовательские задачи **<Имена задач>** (если есть).

  В узле отображаются системные задачи (см. раздел "Категории задач Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 60), созданные при установке программы, добавленные пользовательские задачи, а также групповые задачи проверки по требованию, сформированные и переданные на компьютер с помощью Kaspersky Security Center.
- **Обновление**: управление обновлением баз и модулей Kaspersky Industrial CyberSecurity for Nodes 2.5, а также копированием обновлений для сохранения их в папке локального источника обновлений. Узел содержит вложенные узлы для управления каждой задачей обновления и последней задачей Отката обновления баз программы:
  - **Обновление баз программы**
  - **Обновление модулей программы**
  - **Копирование обновлений**
  - **Откат обновления баз программы**

  В узле отображаются все пользовательские и групповые задачи (см. раздел "Категории задач Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 60) обновления, сформированные и переданные на компьютер с помощью Kaspersky Security Center.

- **Хранилища**: управление параметрами карантина, резервного хранилища и заблокированных узлов.
  - **Карантин**
  - **Резервное хранилище**
  - **Заблокированные узлы**
- **Журналы и уведомления**: управление журналами выполнения локальных задач, журналом безопасности и журналом системного аудита Kaspersky Industrial CyberSecurity for Nodes 2.5.
  - **Журнал безопасности**
  - **Журнал системного аудита**
  - **Журналы выполнения задач**
- **Лицензирование**: добавление и удаление ключей Kaspersky Industrial CyberSecurity for Nodes 2.5, просмотр информации о лицензиях.

Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Industrial CyberSecurity for Nodes**, в панели отображается информация о текущем состоянии защиты компьютера (см. раздел "Просмотр состояния защиты и информации о Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 33), информация о Kaspersky Industrial CyberSecurity for Nodes 2.5, состоянии 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** вы можете выполнять следующие операции:

- **Подключиться к другому компьютеру**. Подключитесь к другому компьютеру (см. раздел "Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере" на стр. 51), чтобы управлять установленной на нем программой Kaspersky Industrial CyberSecurity for Nodes 2.5. Для выполнения этой операции вы также можете воспользоваться ссылкой **Подключиться к другому компьютеру** в правом нижнем углу панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes**.
- **Запустить программу** / **Остановить программу**. Запустить или остановить программу или выбранную задачу (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. 61). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.
- **Настройка параметров проверки съемных дисков**. Настроить проверку съемных дисков (см. раздел "Проверка съемных дисков" на стр. 219), подключенных к защищаемому компьютеру через USB-порт.
- **Защита от эксплойтов: общие параметры защиты**. Настроить режим защиты от эксплойтов и профилактические действия (см. раздел "Настройка параметров защиты памяти процессов" на стр. 110).
- **Защита от эксплойтов: параметры защиты процессов**. Добавить процессы, которые нужно защитить (см. раздел "Добавление процессов для защиты" на стр. 111) и выбрать техники защиты от эксплойтов (см. раздел "Техники защиты от эксплойтов" на стр. 113).
- **Настроить параметры доверенной зоны**. Просмотреть и настроить параметры Доверенной зоны (см. раздел "О доверенной зоне Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 53).

- **Изменить права пользователей на управление программой**. Просмотреть и настроить права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. раздел "О правах на управление Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 43).
- **Изменить права пользователей на управление службой Kaspersky Security**. Просмотреть и настроить права пользователя на управление службой Kaspersky Security (см. раздел "Настройка прав доступа на управление Kaspersky Industrial CyberSecurity for Nodes 2.5 и службой Kaspersky Security" на стр. 15).
- **Экспортировать параметры**. Сохранить параметры программы в конфигурационный файл в формате XML (см. раздел "Экспорт параметров" на стр. 67). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Импортировать параметры**. Импортировать параметры программы из конфигурационного файла в формате XML (см. раздел "Импорт параметров" на стр. 68). Выполнение этой операции также доступно в контекстных меню задач программы.
- **Данные о программе и доступных обновлениях**. Перейти к просмотру информации о Kaspersky Industrial CyberSecurity for Nodes 2.5 и текущих доступных обновлениях модулей программы.
- **Обновить**. Обновить содержимое окна Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Выполнение этой операции также доступно в контекстных меню задач программы.
- **Свойства**. Просмотреть и настроить параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5 или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

  Для выполнения этой операции вы также можете воспользоваться ссылкой **Свойства программы** в панели результатов узла Kaspersky Industrial CyberSecurity for Nodes или кнопкой на панели инструментов.

- **Справка**. Перейти к просмотру справочной системы Kaspersky Industrial CyberSecurity for Nodes 2.5. Выполнение этой операции также доступно в контекстных меню задач программы.

Панель быстрого доступа и контекстное меню задач Kaspersky Industrial CyberSecurity for Nodes 2.5

Вы можете управлять задачами программы с помощью элементов контекстного меню каждой задачи в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

С помощью пунктов контекстного меню выбранной задачи вы можете выполнять следующие операции:

- **Возобновить** / **Приостановить**. Возобновить или приостановить выполнение задачи (см. раздел "Запуск / приостановка / возобновление / остановка задачи вручную" на стр. 61). Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты и задач проверки по требованию.
- **Добавить задачу**. Создать новую пользовательскую задачу (см. раздел "Создание задачи проверки по требованию" на стр. 220). Операция доступна для задач проверки по требованию.
- **Открыть журнал выполнения**. Просматривать журнал выполнения задачи и управлять им (см. раздел "О журналах выполнения задач" на стр. 261). Операция доступна для всех задач.
- **Сохранить задачу**. Сохранить и применить измененные параметры задачи (см. раздел "Сохранение задачи после изменения ее параметров" на стр. 61). Операция доступна для задач постоянной защиты файлов и задач проверки по требованию.

- **Удалить задачу**. Удалить пользовательскую задачу (см. раздел "Удаление задачи" на стр. 223). Операция доступна для задач проверки по требованию.
- **Статистика**. Перейти к просмотру статистики задачи. Операция доступна для задачи проверки целостности программы.
- **Шаблоны параметров**. Управлять шаблонами (см. раздел "Использование шаблонов параметров безопасности" на стр. 69). Операция доступна для задач постоянной защиты файлов и проверки по требованию.

Значок области уведомлений

Каждый раз, когда Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически запускается после перезагрузки защищаемого компьютера, в панели задач отображается значок области уведомлений  . Он отображается по умолчанию, если при установке программы вы установили компонент Значок области уведомлений.

Вид значка области уведомлений отражает текущий статус защиты компьютера. Возможны два статуса:

 активный (цветной значок), если работает минимум одна задача: Постоянная защита файлов, Контроль запуска программ, Контроль устройств;

 неактивный (черно-белый значок), если не работает ни одна из задач: Постоянная защита файлов, Контроль запуска приложений, Контроль устройств.

Вы можете открыть контекстное меню значка области уведомлений по правой клавише мыши.

Контекстное меню включает несколько команд, предназначенных для отображения окон программы (см. таблицу ниже).

Таблица 2. Команды контекстного меню, отображаемые с помощью значка области уведомлений

Команда	Описание
Открыть Консоль управления	Открывает Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 (если она установлена).
Открыть Диагностическое окно	Открывает Диагностическое окно программы.
О программе	Открывает окно О программе с информацией о Kaspersky Industrial CyberSecurity for Nodes 2.5. Если вы зарегистрированы в качестве пользователя Kaspersky Industrial CyberSecurity for Nodes 2.5, окно О программе 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 программы,*

в меню **Пуск** Microsoft Windows выберите **Все Программы > Kaspersky Industrial CyberSecurity for Nodes 2.5 > Значок области уведомлений**.

Названия параметров могут отличаться в разных операционных системах Windows.

В параметрах программы вы можете включать и выключать отображение значка области уведомлений при автоматическом запуске программы после перезагрузки компьютера.

Диагностическое окно

В этом разделе описано, как использовать диагностическое окно для просмотра статуса или текущей активности компьютера и как настраивать запись файла дампа и файла трассировки.

В этом разделе

О диагностическом окне

Компонент Диагностическое окно устанавливается и удаляется вместе с компонентом Значок области уведомлений независимо от Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 и может быть использован, даже если Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 не установлена на защищаемом компьютере. Диагностическое окно запускается через значок области уведомлений или путем запуска файла kavfsmui.exe из папки программы на компьютере.

В диагностическом окне можно выполнять следующие действия:

- Просматривать информацию об общем статусе программы (см. раздел "Просмотр статуса Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью диагностического окна" на стр. 26).
- Просматривать произошедшие инциденты безопасности (см. раздел "Просмотр статистики событий безопасности" на стр. 27).
- Просматривать текущую активность (см. раздел "Просмотр текущей активности программы" на стр. 28) на защищаемом компьютере.
- Запускать и останавливать запись файлов дампа и трассировки (см. раздел "Настройка записи файлов дампа и трассировки" на стр. 29).
- Открывать Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.

- Открывать окно **О программе** со списком установленных обновлений и доступных исправлений.

Если доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 защищен паролем, диагностическое окно предложит вам ввести пароль.

Диагностическое окно нельзя настроить через Kaspersky Security Center.

Просмотр статуса Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью диагностического окна

► *Чтобы открыть диагностическое окно, выполните следующие действия:*

6. По правой клавише мыши откройте контекстное меню Значка области уведомлений панели задач.
7. Выберите пункт меню **Открыть Диагностическое окно**.

   Откроется **диагностическое окно**.
8. Вы можете просмотреть текущий статус лицензии, а также задач постоянной защита компьютера и обновления на закладке **Статус защиты**. Для отображения состояния защиты используется цветовая индикация (см. таблицу ниже).

Таблица 3. Статус защиты в диагностическом окне

Блок	Статус

Постоянная защита компьютера	*Зеленый цвет* панели отображается в следующих ситуациях (при выполнении любого количества условий):
	• Рекомендуемая конфигурация:
	  • Задача Постоянная защита файлов запущена с параметрами по умолчанию.
	  • Задача Контроль запуска программ запущена в режиме **Активный** с параметрами по умолчанию.
	• Приемлемая конфигурация:
	  • Задача Постоянная защита файлов настроена пользователем.
	  • Параметры задачи Контроль запуска программ изменены.

	Желтый цвет панели отображается в следующих случаях (выполнено одно или несколько условий): • Задача Постоянная защита файлов приостановлена (пользователем или согласно расписанию). • Задача Контроль запуска программ запущена в режиме **Только статистика**. • Задачи Защита от эксплойтов и Контроль запуска программ запущены в режиме **Только статистика**.

Блок	Статус
	Красный цвет панели отображается в следующем случае (выполнены оба условия): • Компонент Постоянная защита файлов не установлен или задача остановлена / приостановлена. • Компонент Контроль запуска программ не установлен или задача запущена в режиме **Только статистика**.
Лицензирование	*Зеленый цвет* панели отображается, если текущая лицензия действительна.
	Желтый цвет панели отображается, если возникло одно из следующих событий: • **Выполняется проверка статуса ключа**. • **До истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ или код активации**. • **Добавленный ключ помещен в черный список и скоро будет заблокирован**. • **Подписка приостановлена**.
	Красный цвет отображается, если возникло одно из следующих событий: • **Программа не активирована.** • **Срок действия лицензии истек.** • **Нарушено Лицензионное соглашение.** • **Ключ помещен в черный список.**
Обновление	*Зеленый цвет* панели отображается в следующем случае: • Базы программы обновлены.
	Желтый цвет панели отображается в следующем случае: • Базы программы устарели.
	Красный цвет панели отображается в следующем случае: • Базы программы сильно устарели.

Просмотр статистики событий безопасности

На закладке **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, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню Значка области уведомлений панели задач.
2. Выберите пункт меню **Открыть Диагностическое окно**.

   Откроется **диагностическое окно**.
3. Откройте закладку **Статистика**.
4. Просмотрите инциденты безопасности для задач защиты.

Просмотр текущей активности программы

На этой закладке вы можете просматривать статус текущих задач и процессов программы, а также получать динамические сообщения о происходящих критических событиях.

Для отображения статуса активности программы используется цветовая индикация:

- В блоке **Задачи**:
  - *Зеленый цвет*. Не выполнены условия для желтого или красного цветов.
  - *Желтый цвет*. Проверка важных областей давно не выполнялась.
  - *Красный цвет*. Выполнено какое-либо 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 блоке **Kaspersky Security Network**:
  - *Зеленый цвет*. Задача Использование KSN запущена.
  - *Желтый цвет*. Положение о KSN принято, но задача не запущена.

► *Чтобы просмотреть текущую активность программы на компьютере, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню Значка области уведомлений панели задач.
2. Выберите пункт меню **Открыть Диагностическое окно**.

   Откроется **диагностическое окно**.
3. Откройте закладку **Текущая активность программы**.
4. В блоке **Задачи** можно просмотреть следующую информацию:
   - **Проверка важных областей давно не выполнялась**

     Это поле отображается, только если программа возвращает соответствующее предупреждение о проверке важных областей.
   - **Выполняются сейчас**.
   - **Завершены с ошибкой**.
   - **Следующий запуск определен по расписанию**.
5. В блоке **Kaspersky Security Network** можно просмотреть следующую информацию:
   - **Включено. Включено с запросами файловой репутации**. **Не используется**.
   - **Статистика программы отправляется в KSN**.

     Программа отправляет данные об обнаружении вредоносных программ, в том числе мошеннических, в ходе выполнения задач постоянной защиты и проверки по требованию, а также отладочную информацию о сбоях при проверке.

     Поле отображается, если флажок **Разрешить отправку данных о проверяемых файлах** установлен в параметрах задачи Использование KSN.
6. В блоке **Интеграция с Kaspersky Security Center** можно просмотреть следующую информацию:

- Локальное управление разрешено.
- Применяется политика: <имя сервера Kaspersky Security Center>.

Настройка записи файлов дампов и файлов трассировки

В диагностическом окне можно настроить запись файлов дампов и файлов трассировки.

Вы также можете настроить запись диагностики сбоев (см. раздел "Параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5 в Консоли» на стр. 44) в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

► *Чтобы запустить запись файлов дампа и трассировки, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню Значка области уведомлений панели задач.
2. Выберите пункт меню **Открыть Диагностическое окно**.

   Откроется **диагностическое окно**.
3. Откройте закладку **Диагностика сбоев**.
4. Если требуется, настройте следующие параметры трассировки:
   g. Установите флажок **Записывать отладочную информацию в файл трассировки**.
   h. Нажмите кнопку **Обзор** и укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes 2.5 будет сохранять файлы трассировки.
5. Если требуется, настройте следующие параметры дампа:
   a. Установите флажок **Создавать во время сбоя файл дампа**.
   b. Нажмите кнопку **Обзор** и укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes 2.5 будет сохранять файл дампа.
6. Нажмите кнопку **Применить**.

   Новая конфигурация будет применена.

О предоставлении данных

Лицензионное соглашение для Kaspersky Industrial CyberSecurity for Nodes 2.5, в частности в разделе «Условия обработки данных», определяет условия, ответственность и порядок передачи и обработки данных, указанных в настоящем Руководстве. Внимательно ознакомьтесь с условиями Лицензионного соглашения, а также со всеми документами, ссылки на которые содержит Лицензионное соглашение, перед тем, как принять его.

Данные, которые «Лаборатория Касперского» получает от вас при использовании программы, защищаются и обрабатываются в соответствии с Политикой конфиденциальности, опубликованной по адресу: https://www.kaspersky.ru/Products-and-Services-Privacy-Policy.

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 использования возможности навигации по Базе знаний при возникновении ошибки программы (служба перенаправления) – данные о программе и тип ссылки, в частности: название, регион и номер полной версии программы, тип перенаправляющей ссылки и идентификатор ошибки;
- 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.

Локальная обработка данных

В процессе выполнения основных функций программы, описанных в настоящем Руководстве, Kaspersky Industrial CyberSecurity for Nodes 2.5 локально обрабатывает и хранит ряд данных на защищаемом компьютере:

- данные о проверенных файлах и обнаруженных объектах, например: имена и атрибуты обработанных файлов и полные пути к ним на проверенных носителях; действия, предпринятые в отношении проверенных файлов; учетные записи пользователей, выполнявших любые действия в защищаемой сети или на защищаемом компьютере; названия проверенных устройств и данные о них; данные о процессах, запущенных в системе;
- данные об активности и параметрах операционной системы, например: параметры брандмауэра Windows, журнал событий Windows, названия учетных записей пользователей, экземпляры запускаемых исполняемых файлов, а также типы, имена, контрольные суммы и атрибуты этих файлов;
- информацию о сетевой активности, в том числе IP-адреса заблокированных клиентских компьютеров;
- информацию о сетях Wi-Fi, к которым подключается защищаемый компьютер;
- информацию о проектах ПЛК, добавленных в область защиты, включая параметры подключения ПЛК и контрольные суммы микропрограммного обеспечения.

Kaspersky Industrial CyberSecurity for Nodes 2.5 обрабатывает и хранит данные в рамках базовых функций программы, в том числе регистрирует события программы и получает диагностические данные. Обработка и защита локально обрабатываемых данных выполняются в соответствии с настроенными и применяющимися параметрами программы.

Kaspersky Industrial CyberSecurity for Nodes 2.5 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.

Запуск и остановка Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию о запуске Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5, а также о запуске и остановке службы Kaspersky Security.

В этом разделе

Запуск Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

► *Чтобы запустить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 из меню Пуск, выполните следующие действия:*

в меню **Пуск** выберите **Программы → Kaspersky Industrial CyberSecurity for Nodes 2.5 → Средства администрирования → Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5**.

Чтобы добавить в Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 другую оснастку, запустите Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 в авторском режиме.

► *Чтобы запустить Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 в авторском режиме, выполните следующие действия:*

1. В меню **Пуск** выберите **Программы → Kaspersky Industrial CyberSecurity for Nodes 2.5 → Средства администрирования**.
2. В контекстном меню программы Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите команду **Автор**.

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 будет запущена в авторском режиме.

Если вы запустили Консоль на защищаемом компьютере, откроется окно Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. раздел "Интерфейс окна Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 19).

Если вы запустили Консоль не на защищаемом компьютере, а на другом устройстве, подключитесь к защищаемому компьютеру.

► *Чтобы подключиться к защищаемому компьютеру, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите команду **Подключиться к другому компьютеру**.

   Откроется окно **Выбор компьютера**.
3. В открывшемся окне выберите **Другой компьютер**.
4. В поле ввода справа укажите сетевое имя защищаемого компьютера.
5. Нажмите на кнопку **OK**.

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 будет подключена к защищаемому компьютеру.

Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management на компьютере, установите флажок **Установить соединение с правами учетной записи** и укажите другую учетную запись, которая обладает такими правами.

Запуск и остановка службы Kaspersky Security

По умолчанию служба Kaspersky Security запускается автоматически при старте операционной системы. Служба Kaspersky Security управляет рабочими процессами, в которых выполняются задачи постоянной защиты компьютера, контроля компьютера, проверки по требованию и обновления.

По умолчанию при запуске Kaspersky Industrial CyberSecurity for Nodes 2.5 запускаются задачи Постоянная защита файлов и Проверка при запуске операционной системы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

Если вы остановите службу Kaspersky Security, все выполняющиеся задачи будут остановлены. После того как вы снова запустите службу Kaspersky Security, программа автоматически запустит только задачи, в расписании которых указана частота запуска **При запуске программы**, остальные задачи требуется запустить вручную.

Вы можете запускать и останавливать службу Kaspersky Security с помощью контекстного меню узла **Kaspersky Industrial CyberSecurity for Nodes** или с помощью оснастки Службы Microsoft Windows.

Вы можете запускать и останавливать Kaspersky Industrial CyberSecurity for Nodes 2.5, если вы входите в группу "Администраторы" на защищаемом компьютере.

► *Чтобы остановить программу с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите одну из следующих команд:
   - **Остановка службы**.
   - **Запуск службы**.

Служба Kaspersky Security будет запущена или остановлена.

Просмотр состояния защиты и информации о Kaspersky Industrial CyberSecurity for Nodes 2.5

► *Чтобы просмотреть информацию о состоянии защиты компьютера и информацию о Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

Выберите узел **Kaspersky Industrial CyberSecurity for Nodes** в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

По умолчанию информация в панели результатов Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 обновляется автоматически:

- каждые 10 сек. при локальном подключении;
- каждые 15 сек. при удаленном подключении.

Вы можете обновлять информацию вручную.

► *Чтобы вручную обновить информацию в узле **Kaspersky Industrial CyberSecurity for Nodes**, выполните следующие действия:*

Выберите команду **Обновить** в контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes**.

В панели результатов Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 отображается следующая информация о программе:

- статус использования Kaspersky Security Network;
- состояние защиты компьютера;
- данные об обновлении баз и модулей программы;
- актуальные данные диагностики;
- данные о задачах контроля компьютера;
- данные о лицензии;
- статус защиты промышленной сети;
- статус интеграции с Kaspersky Security Center: данные компьютера с установленным 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 блоке **Использование Kaspersky Security Network** отображается текущий статус задачи, например, *Выполняется, Остановлена* или *Не выполнялась*. 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.

Закладка Защита компьютера

Блок **Защита компьютера** (см. таблицу ниже) отображает информацию о текущем состоянии защиты компьютера.

Таблица 4. Информация о состоянии защиты компьютера

Блок Защита	Информация
Индикатор статуса защиты компьютера	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. 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 задачи** – текущее состояние задачи, например, Выполняется или Остановлена. **Обнаружено** – количество объектов, которые обнаружила программа Kaspersky Industrial CyberSecurity for Nodes 2.5. Например, если программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаружила в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу. Если количество обнаруженных вредоносных программ превышает 0, значение выделяется красным цветом.
Проверка важных областей	**Дата последней проверки** – дата и время последней проверки важных областей на наличие вирусов и других угроз компьютерной безопасности. *Не выполнялась* – 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 шифрования	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы** – один из двух доступных режимов работы задачи Защита от шифрования. • Активна • Только статистика. **Компьютеров заблокировано** – количество узлов, проявивших потенциально опасную активность и заблокированных при попытке подключения к защищаемому компьютеру.
Резервные копии объектов	*Превышен порог доступного пространства в резервном хранилище* – событие, которое возникает, если порог доступного пространства в резервном хранилище достигает указанного значения. Kaspersky Industrial CyberSecurity for Nodes 2.5 при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется желтым цветом. *Превышен максимальный размер резервного хранилища* – событие, которое возникает, если размер резервного хранилища достигает указанного значения. Kaspersky Industrial CyberSecurity for Nodes 2.5 при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется красным цветом. **Объектов в резервном хранилище** – количество объектов, находящихся в резервном хранилище в текущий момент. **Используемое пространство** – объем используемого пространства в резервном хранилище.

Блок **Обновление** (см. таблицу ниже) отображает информацию об актуальности антивирусных баз и модулей программы.

Таблица 5. Информация о состоянии баз и модулей Kaspersky Industrial CyberSecurity for

Блок Обновление	Информация
Индикатор состояния баз и модулей программы	Цвет панели с названием блока является индикатором состояния баз и модулей программы. Индикатор может принимать следующие значения: • Зеленый цвет панели отображается по умолчанию и означает, что базы программы актуальны и последняя задача обновления баз программы завершена успешно. • Желтый цвет панели – означает, что базы устарели или последняя задача обновления баз программы завершена с ошибкой. • Красный цвет панели – возникло событие *Базы программы сильно устарели* или *Базы программы повреждены*.
Обновление баз программы и **Обновление модулей программы**	**Актуальность баз программы** – оценка статуса Обновления баз программы. Параметр может принимать следующие значения: • **Базы программы актуальны** – базы программы обновлены не более чем 7 дней назад (по умолчанию). • **Базы программы устарели** – базы программы обновлены 7–14 дней назад (по умолчанию). • **Базы программы сильно устарели** – базы программы обновлены более чем 14 дней назад (по умолчанию). Вы можете изменять пороги формирования событий Базы программы устарели и *Базы программы сильно устарели*. **Дата выпуска баз программы** – дата и время выпуска последнего установленного обновления баз программы. Дата и время указаны в UTC. **Статус последней запущенной задачи обновления баз программы** – дата и время последнего обновления базы программы. Дата и время указаны по местному времени защищаемого компьютера. Значение в поле окрашивается в красный цвет, если возникло событие *Завершена с ошибкой*. **Доступно обновлений модулей программы** – количество обновлений модулей Kaspersky Industrial CyberSecurity for Nodes 2.5, доступных для загрузки и установки. **Установлено обновлений модулей программы** – количество установленных обновлений модулей Kaspersky Industrial CyberSecurity for Nodes 2.5.

Блок **Контроль** (см. таблицу ниже) отображает информацию о состоянии задач Контроль запуска программ, Контроль устройств и Управление сетевым экраном.

Таблица 6. Информация о состоянии контроля компьютера

Блок Контроль	Информация

Индикатор статуса контроля компьютера	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. 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 работает.
	  • Задача Контроль запуска программ запущена в режиме Только статистика.
	  • 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 Только статистика.

Контроль запуска программ	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы –** один из двух доступных режимов работы задачи Контроль запуска программ: • Активна • Только статистика. **Заблокировано запусков программ** – количество попыток запуска программ, заблокированных Kaspersky Industrial CyberSecurity for Nodes 2.5 в ходе выполнения задачи Контроль запуска программ. Если количество заблокированных запусков программ превышает 0, значение поля окрашивается в красный цвет. **Среднее время обработки (мс)** – время, которое потребовалось Kaspersky Industrial CyberSecurity for Nodes 2.5 для обработки попытки запуска программ на защищаемом компьютере.
Защита от эксплойтов	**Статус задачи** – текущее состояние, например *Выполняется* или *Остановлена*. **Режим работы** – один из двух доступных режимов, выбранный при настройке защиты памяти процессов: • Завершать скомпрометированные процессы. • Только сообщать о компрометации процесса. **Процессов защищено** – общее количество процессов, которые находятся под защитой и обрабатываются в соответствие с выбранным режимом.

Блок Контроль	Информация
Контроль устройств	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы –** один из двух доступных режимов работы задачи Контроль устройств: **Заблокировано устройств** – количество подключений устройств с попыткой их использования в качестве запоминающих, заблокированных Kaspersky Industrial CyberSecurity for Nodes 2.5 в ходе выполнения задачи Контроль устройств. Если количество заблокированных устройств превышает 0, значение поля окрашивается в красный цвет.
Управление сетевым экраном	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Заблокировано попыток подключения** – количество подключений к защищаемому компьютеру, которые не были разрешены заданными правилами сетевого экрана.
Контроль Wi-Fi	Разрешенные сети Wi-Fi – количество сетей Wi-Fi, которым разрешено подключаться к защищаемому компьютеру. Заблокированные сети Wi-Fi – количество заблокированных сетей Wi-Fi.

Блок **Диагностика** (см. таблицу ниже) отображает информацию о состоянии задач Мониторинг файловых операций и Анализ журналов.

Таблица 7. Информация о состоянии диагностики системы

Блок Диагностика	**Информация**
Индикатор статуса диагностики	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. 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.
Мониторинг файловых операций	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Несанкционированные файловые операции** – количество изменений в файлах из области мониторинга. Эти изменения могут указывать на нарушение безопасности защищаемого устройства.
Анализ журналов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Возможных нарушений** – количество зафиксированных нарушений по данным журнала событий Windows, выявленных на основе заданных правил задачи или применения эвристического анализатора.

Закладка Защита промышленной сети

В блоке **Область защиты ПЛК** отображается информация о списке ПЛК, включенных в область защиты.

Таблица 8. Информация о получении данных о ПЛК

Блок Область защиты ПЛК	**Информация**
Индикатор статуса области защиты ПЛК	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. 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 ПЛК	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **ПЛК в списке** – количество ПЛК в области защиты.

В блоке **Целостность проектов ПЛК** отображается информация о количестве защищаемых ПЛК и событиях нарушения целостности.

Таблица 9. Информация о проверке целостности проектов ПЛК

Блок Целостность проектов ПЛК	Информация
Индикатор статуса проверки целостности проектов ПЛК	Цвет панели с названием блока является индикатором состояния задач, выполняемых в блоке. 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.
Получение данных о проектах ПЛК	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **ПЛК в области активной защиты** – количество ПЛК в области защиты. **Нарушения целостности** – количество обнаруженных нарушений.

Информация о лицензии Kaspersky Industrial CyberSecurity for Nodes 2.5 (см. раздел "Лицензирование" на стр. 52) отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes**.

Вы можете настроить свойства Kaspersky Industrial CyberSecurity for Nodes 2.5, перейдя по ссылке Свойства программы (см. раздел "Параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5 в Консоли " на стр. 44).

Вы можете выполнить подключение к другому компьютеру, перейдя по ссылке Подключиться к другому компьютеру (см. раздел "Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере" на стр. 51).

Работа с Консолью Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию о Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 и об управлении программой через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, установленную на защищаемом или другом компьютере.

В этом разделе

О Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять программой через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, установленную на защищаемом компьютере или на другом компьютере в сети организации. После того как вы установили Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере (см. раздел "Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 через Консоль на другом компьютере" на стр. 51), вам нужно выполнить дополнительную настройку.

Если Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 и программа установлены на разных компьютерах, принадлежащих к разным доменам, возможны ограничения в доставке информации от Kaspersky Industrial CyberSecurity for Nodes 2.5 в Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5.

При установке Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 утилита установки сохраняет файл kavfs.msc в папке установки и добавляет оснастку Kaspersky Industrial CyberSecurity for Nodes 2.5 в список изолированных оснасток Microsoft Windows.

Вы можете открыть Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 из меню **Пуск**. На защищаемом устройстве вы также можете открыть Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью значка области уведомлений в панели задач.

Вы можете запустить msc-файл оснастки Kaspersky Industrial CyberSecurity for Nodes 2.5 или добавить оснастку программы в Microsoft Management Console как новый элемент в дереве (см. раздел "Интерфейс Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 20).

В 64-разрядной версии Microsoft Windows вы можете добавить оснастку Kaspersky Industrial CyberSecurity for Nodes 2.5 только в Microsoft Management Console 32-разрядной версии. Для этого откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

Вы можете добавить несколько оснасток программы в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких компьютеров, на которых установлена программа Kaspersky Industrial CyberSecurity for Nodes 2.5.

Параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5 в Консоли

Общие параметры и параметры диагностики сбоев Kaspersky Industrial CyberSecurity for Nodes 2.5 определяют общие условия работы программы. Эти параметры позволяют регулировать количество рабочих процессов, используемых Kaspersky Industrial CyberSecurity for Nodes 2.5, включать восстановление задач Kaspersky Industrial CyberSecurity for Nodes 2.5 после их аварийного завершения, вести журнал трассировки, включать создание файла дампа процессов Kaspersky Industrial CyberSecurity for Nodes 2.5 при их аварийном завершении и настраивать другие общие параметры.

Настройка параметров работы программы в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 недоступна, если в активной политике Kaspersky Security Center установлен запрет на изменение данных параметров.

► *Чтобы настроить параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите узел **Kaspersky Industrial CyberSecurity for Nodes** и выполните одно из следующих действий:
   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.
2. В открывшемся окне настройте общие параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5 согласно вашим требованиям:
   - На закладке **Масштабируемость и интерфейс** вы можете настроить следующие параметры:
     - В блоке **Параметры масштабируемости**:
       - Максимальное количество активных процессов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 может запустить.

Таблица 10. Максимальное количество активных процессов.

Параметр	**Максимальное количество активных процессов**

<table>
<tr><td>Описание</td><td>Этот параметр относится к группе Параметры масштабируемости Kaspersky Industrial CyberSecurity for Nodes 2.5. Он устанавливает максимальное количество рабочих процессов, которые программа может запустить одновременно.
Увеличение количества параллельно работающих процессов повышает скорость проверки файлов и устойчивость Kaspersky Industrial CyberSecurity for Nodes к сбоям. Однако, высокое значение этого параметра может снизить общую производительность компьютера и повысить потребление оперативной памяти.
В Консоли администрирования программы Kaspersky Security Center вы можете устанавливать параметр Максимальное количество активных процессов только для Kaspersky Industrial CyberSecurity for Nodes 2.5 на отдельном компьютере (в диалоговом окне Параметры программы); вы не можете изменять этот параметр в свойствах политики для группы компьютеров.</td></tr>
<tr><td>Возможные значения</td><td>1 – 8</td></tr>
<tr><td>Значение по умолчанию</td><td>Kaspersky Industrial CyberSecurity for Nodes выполняет масштабирование автоматически в зависимости от количества процессоров на компьютере:
<table>
<tr><th>Количество процессоров</th><th>Максимальное количество активных процессов</th></tr>
<tr><td>1</td><td>1</td></tr>
<tr><td>1 < кол-во процессоров < 4</td><td>2</td></tr>
<tr><td>4 и более</td><td>4</td></tr>
</table></td></tr>
</table>

- Количество процессов для постоянной защиты компьютера.

Таблица 11. Количество процессов для постоянной защиты.

<table>
<tr><td>Параметр</td><td>Количество процессов для постоянной защиты</td></tr>
<tr><td>Описание</td><td>Этот параметр относится к группе Параметры масштабируемости Kaspersky Industrial CyberSecurity for Nodes 2.5.
С помощью этого параметра вы можете устанавливать фиксированное количество процессов, в которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет выполнять задачи постоянной защиты.
Более высокое значение этого параметра повысит скорость проверки объектов в задачах постоянной защиты. Однако чем больше рабочих процессов задействует Kaspersky Industrial CyberSecurity for Nodes 2.5, тем больше будет его влияние на общую производительность защищаемого компьютера и его потребление оперативной памяти.
В Консоли администрирования программы Kaspersky Security Center вы можете устанавливать параметр Количество процессов для постоянной защиты только для Kaspersky Industrial CyberSecurity for Nodes 2.5 на отдельном компьютере (в окне Параметры программы); вы не можете изменять этот параметр в свойствах политики для группы компьютеров.</td></tr>
<tr><td>Возможные значения</td><td>Возможные значения: 1-N, где N – значение, заданное параметром Максимальное количество активных процессов.
Если вы установите значение параметра Количество процессов для постоянной защиты равным максимальному числу активных процессов, вы снизите влияние Kaspersky Industrial CyberSecurity for Nodes 2.5 на скорость файлового обмена компьютеров с компьютером, еще повысив его быстродействие во время постоянной защиты. Однако задачи обновления и задачи проверки по требованию с базовым приоритетом Средний (Normal) будут выполняться в уже запущенных рабочих процессах Kaspersky Industrial CyberSecurity for Nodes 2.5. Задачи проверки по требованию будут выполняться медленнее. А если выполнение задачи вызовет аварийное завершение процесса, на его перезапуск потребуется больше времени.
Задачи проверки по требованию с базовым приоритетом Низкий (Low) всегда выполняются в отдельном процессе или процессах.</td></tr>
<tr><td>Значение по умолчанию</td><td>Kaspersky Industrial CyberSecurity for Nodes 2.5 выполняет масштабирование автоматически в зависимости от количества процессоров на компьютере:
<table>
<tr><th>Количество процессоров</th><th>Количество процессов для постоянной защиты.</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>>1</td><td>2</td></tr>
</table></td></tr>
</table>

- Количество рабочих процессов для фоновых задач проверки по требованию.

Таблица 12. Количество процессов для фоновых задач проверки по требованию.

Параметр	Количество процессов для фоновых задач проверки по требованию.
Описание	Этот параметр относится к группе **Параметры масштабируемости** Kaspersky Industrial CyberSecurity for Nodes 2.5. С помощью этого параметра вы можете указывать максимальное количество процессов, в которых Kaspersky Industrial CyberSecurity for Nodes будет выполнять задачи проверки по требованию в фоновом режиме. Количество процессов, которое вы устанавливаете этим параметром, не входит в общее количество рабочих процессов Kaspersky Industrial CyberSecurity for Nodes, заданное параметром **Максимальное количество активных процессов**. Например, если вы установите следующие значения параметров: • максимальное количество активных процессов – 3; • количество процессов для задач постоянной защиты – 3; • количество процессов для фоновых задач проверки по требованию – 1; а затем запустите задачи постоянной защиты и одну задачу проверки по требованию в фоновом режиме, общее количество рабочих процессов kavfswp.exe Kaspersky Industrial CyberSecurity for Nodes составит 4. В одном рабочем процессе с низким приоритетом может выполняться несколько задач проверки по требованию. Вы можете повысить количество рабочих процессов, например, если вы запускаете одновременно несколько задач в фоновом режиме, чтобы выделить отдельный процесс для каждой задачи. Выделение отдельных процессов для задач повышает надежность выполнения этих задач и их скорость.
Возможные значения	1-4
Значение по умолчанию	1

- В блоке **Взаимодействие с пользователем** настройте отображение Значка области уведомлений в панели задач (см. раздел "Значок области уведомлений в панели задач" на стр. 24) при каждом запуске программы.

- На закладке **Безопасность и надежность** вы можете настроить следующие параметры:
  - В блоке **Параметры надежности** укажите количество попыток восстановления задач проверки по требованию после их аварийного завершения.

Таблица 13. Восстановление задач

Параметр	Восстановление задач (**Выполнять восстановление задач**).
Описание	Этот параметр относится к группе **Параметры надежности** Kaspersky Industrial CyberSecurity for Nodes. Он включает восстановление задач, если они завершаются аварийно, и устанавливает количество попыток восстановления задач проверки по требованию. Когда задача завершается аварийно, процесс kavfs.exe Kaspersky Industrial CyberSecurity for Nodes пытается повторно запустить процесс, в котором эта задача выполнялась в момент завершения. Если восстановление задач выключено, Kaspersky Industrial CyberSecurity for Nodes не восстанавливает задачи постоянной защиты и проверки по требованию. Если восстановление задач включено, Kaspersky Industrial CyberSecurity for Nodes пытается восстановить задачи постоянной защиты, пока они не будут успешно запущены, и пытается восстановить задачи проверки по требованию столько раз, сколько указано этим параметром.
Возможные значения:	Включено / выключено. Количество попыток восстановления задач проверки по требованию: 1 – 10
Значение по умолчанию	Восстановление задач включено. Количество попыток восстановления задач проверки по требованию: 2.

- В блоке **Действия при переходе на источник бесперебойного питания** укажите действия Kaspersky Industrial CyberSecurity for Nodes 2.5 при работе от источника бесперебойного питания.

Таблица 14. Использование источника бесперебойного питания

Параметр	Действия при переходе на источник бесперебойного питания.
Описание	Этот параметр определяет действия, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 выполнит, когда компьютер перейдет на питание от источника бесперебойного питания.
Возможные значения:	Запускать или не запускать задачи проверки по требованию, которые должны быть запущены по расписанию. Выполнять или останавливать все выполняемые задачи проверки по требованию.
Значение по умолчанию	По умолчанию при работе компьютера от источника бесперебойного питания Kaspersky Industrial CyberSecurity for Nodes 2.5 работает в следующем режиме: • не запускает задачи проверки по требованию, которые должны быть запущены по расписанию; • автоматически останавливает все выполняемые задачи проверки по требованию.

- В блоке **Настройки пароля** настройте параметры защиты паролем функций программы (см. раздел "Защита доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью пароля" на стр. 17).

- На закладке **Параметры соединения**:
  - В блоке **Параметры прокси-сервера** укажите параметры использования прокси-сервера.
  - В блоке **Параметры аутентификации на прокси-сервере** укажите тип аутентификации и необходимые данные для аутентификации на прокси-сервере.

- В блоке **Лицензирование** укажите, будет ли Kaspersky Security Center использоваться в качестве прокси-сервера для активации программы.

- На закладке **Диагностика сбоев**:
  - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
    - В поле ниже укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes 2.5 будет сохранять файлы трассировки.
    - Настройте уровень детализации отладочной информации.

      В раскрывающемся списке вы можете выбрать уровень детализации отладочной информации, которую Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в файле трассировки.

      Вы можете выбрать один из следующих уровней детализации:

      - **Критические события** – Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в файле трассировки только информацию о критических событиях.
      - **Ошибки** – Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в файле трассировки информацию о критических событиях и ошибках.
      - **Важные события** – Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в файле трассировки информацию о критических событиях, ошибках и важных событиях.
      - **Информационные события** – Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в файле трассировки информацию о критических событиях, ошибках, важных событиях и информационных событиях.
      - **Вся отладочная информация** – Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в файле трассировки всю отладочную информацию.

      Уровень детализации, который требуется установить для решения возникшей проблемы, определяет специалист Службы технической поддержки.

      По умолчанию установлен уровень детализации **Вся отладочная информация**.

      Раскрывающийся список доступен, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

    - Укажите максимальный размер файлов трассировки.
    - Укажите отлаживаемые компоненты.

      Список кодов подсистем Kaspersky Industrial CyberSecurity for Nodes 2.5, о работе которых программа сохраняет отладочную информацию в файле трассировки. Коды компонентов требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Таблица 15. Коды подсистем Kaspersky Industrial CyberSecurity for Nodes 2.5

Код подси-стемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Industrial CyberSecurity for Nodes в Microsoft Management Console.
ak_conn	Подсистема интеграции с Агентом администрирования Kaspersky Security Center.

bl	Управляющий процесс, реализует задачи управления Kaspersky Industrial CyberSecurity for Nodes.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Industrial CyberSecurity for Nodes.
ods	Подсистема проверки по требованию.
oas	Подсистема постоянной защиты файлов.
qb	Подсистема карантина и резервного хранилища.
scandll	Вспомогательный модуль антивирусной проверки.
core	Подсистема базовой антивирусной функциональности.
avscan	Подсистема антивирусной обработки.
avserv	Подсистема управления антивирусным ядром.
prague	Подсистема базовой функциональности.
updater	Подсистема обновления баз и модулей программы.
snmp	Подсистема поддержки SNMP протокола.
perfcount	Подсистема счетчиков производительности.

Параметры трассировки оснастки Kaspersky Industrial CyberSecurity for Nodes 2.5 (gui) и плагина управления Kaspersky Industrial CyberSecurity for Nodes 2.5 для Kaspersky Security Center (ak_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcount) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Industrial CyberSecurity for Nodes 2.5 применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет отладочную информацию о работе всех подсистем Kaspersky Industrial CyberSecurity for Nodes 2.5 (рекомендуется).

Поле ввода доступно, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Если вы хотите создавать файл дампа, установите флажок **Создавать во время сбоя файл дампа**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не отправляет файлы трассировки и дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

- В поле ниже укажите папку, в которую Kaspersky Industrial CyberSecurity for Nodes 2.5 будет сохранять файл дампа.

Kaspersky Industrial CyberSecurity for Nodes 2.5 записывает информацию в файлы трассировки и дампа в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете настроить права доступа (см. раздел "Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 43) и разрешить доступ к журналам, файлам трассировки и дампа только для выбранных пользователей.

3. Нажмите на кнопку **OK**.

Параметры работы Kaspersky Industrial CyberSecurity for Nodes 2.5 будут сохранены.

Управление Kaspersky Industrial CyberSecurity for Nodes 2.5 через Консоль на другом компьютере

Вы можете управлять Kaspersky Industrial CyberSecurity for Nodes 2.5 через Консоль, которая установлена на удаленном компьютере.

Чтобы управление программой с помощью Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на удаленном компьютере было доступно, убедитесь, что выполняются следующие условия:

- Пользователи Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 на удаленном компьютере добавлены в группу KICS Administrators на защищаемом компьютере.
- Разрешены сетевые соединения для процесса службы Kaspersky Security Management kavfsgt.exe, если на защищаемом компьютере включен брандмауэр Windows.
- Во время установки Kaspersky Industrial CyberSecurity for Nodes 2.5 был установлен флажок **Разрешить удаленный доступ** в окне мастера установки.

Если управление Kaspersky Industrial CyberSecurity for Nodes 2.5 на удаленном компьютере защищено паролем, вам нужно ввести пароль для получения доступа к управлению программой через Консоль.

Лицензирование

Подробнее о типах лицензионных сертификатов, способах активации продуктов и Лицензионном соглашении см. в разделе "Лицензирование программы" *Руководства администратора Kaspersky Industrial CyberSecurity for Nodes 2.5*.

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

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите узел **Лицензирование**.
2. Чтобы активировать Kaspersky Industrial CyberSecurity for Nodes 2.5, перейдите по ссылке **Добавить ключ**.
3. В открывшемся окне **Добавление ключа** нажмите на кнопку **Обзор**.
4. Выберите файл ключа на своем компьютере и нажмите на кнопку **Открыть**.

   Также можно пометить ключ как дополнительный, установив флажок **Использовать дополнительный ключ**.
5. Нажмите на кнопку **ОК**, чтобы применить добавленный ключ.

Настройка доверенной зоны

Этот раздел содержит информацию о доверенной зоне Kaspersky Industrial CyberSecurity for Nodes 2.5, инструкции по добавлению объектов в доверенную зону и применению доверенной зоны в задачах Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

О доверенной зоне Kaspersky Industrial CyberSecurity for Nodes 2.5

Доверенная зона - это список исключений из области защиты или проверки, который вы можете сформировать и применять в задачах проверки по требованию и в задаче Постояння защита файлов.

Если при установке Kaspersky Industrial CyberSecurity for Nodes 2.5 вы установили флажки **Добавить к исключениям файлы, рекомендованные Microsoft** и **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**, Kaspersky Industrial CyberSecurity for Nodes 2.5 добавляет в доверенную зону файлы, рекомендованные Microsoft и "Лабораторией Касперского", для задач постоянной защиты компьютера.

Вы можете формировать доверенную зону Kaspersky Industrial CyberSecurity for Nodes 2.5 по следующим правилам:

- Доверенные процессы. В доверенную зону помещаются объекты, к которым обращаются процессы программ, чувствительных к файловым перехватам.
- Операции резервного копирования. В доверенную зону помещаются объекты, доступ к которым выполняется в операциях систем резервного копирования жестких дисков на внешние устройства.
- Исключения. В доверенную зону помещаются объекты, указанные по их местоположению и / или обнаруженному в них объекту.

Вы можете применить доверенную зону в задаче Постоянная защита файлов, в создаваемых пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

По умолчанию доверенная зона применяется в задачах постоянной защиты файлов и в задачах проверки по требованию.

Вы можете экспортировать список правил формирования доверенной зоны в конфигурационный файл в формате XML, чтобы затем импортировать его в Kaspersky Industrial CyberSecurity for Nodes 2.5 на другом компьютере.

Доверенные процессы

Применяется в задаче постоянной защиты файлов.

Некоторые программы на компьютере могут работать нестабильно, если файлы, к которым они обращаются, перехватываются Kaspersky Industrial CyberSecurity for Nodes 2.5. К таким программам относятся, например, системные программы домен-контроллеров.

Чтобы не нарушать работу таких программ, вы можете выключить функцию постоянной защиты объектов, к которым обращаются выполняющиеся процессы этих программ, сформировав в доверенной зоне список доверенных процессов.

Корпорация Microsoft рекомендует исключать из постоянной защиты некоторые файлы операционной системы Microsoft Windows и файлы программ корпорации Microsoft как неподверженные заражению. Имена некоторых из них приводятся на веб-сайте Microsoft (код статьи: KB822158).

Вы можете включать и выключать применение доверенных процессов в доверенной зоне.

Если исполняемый файл процесса изменяется, например обновляется, Kaspersky Industrial CyberSecurity for Nodes 2.5 исключает его из списка доверенных процессов.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не использует значение пути к файлу на локальном компьютере для идентификации процесса как доверенного. Путь к файлу на локальном компьютере применяется только для поиска файла и расчета его контрольной суммы, а также для информирования пользователя об источнике исполняемого файла.

Операции резервного копирования

Применяется в задачах постоянной защиты компьютера.

На время резервного копирования данных, хранящихся на жестких дисках, на внешние устройства вы можете выключить функцию постоянной защиты объектов, доступ к которым осуществляется в операциях резервного копирования. Kaspersky Industrial CyberSecurity for Nodes 2.5 не проверяет объекты, которые программа резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

Исключения

Применяется в задачах постоянной защиты файлов и проверки по требованию.

Вы можете выбрать задачи, в которых вы хотите применять каждое исключение, добавленное в доверенную зону. Также вы можете исключать объекты из проверки в параметрах уровня безопасности каждой задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 по отдельности.

Вы можете добавлять в доверенную зону объекты по их местоположению на компьютере, по имени или маске имени обнаруженного в них объекта или использовать оба параметра.

На основании исключения Kaspersky Industrial CyberSecurity for Nodes 2.5 может пропускать в указанных задачах объекты согласно следующим параметрам:

- указанные обнаруживаемые объекты по имени или маске имени в указанных областях компьютера;
- все обнаруживаемые объекты в указанных областях компьютера;
- указанные обнаруживаемые объекты по имени или маске имени во всей области защиты или проверки..

Включение и выключение применения доверенной зоны в задачах Kaspersky Industrial CyberSecurity for Nodes 2.5

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов, в создаваемых пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

После того как вы включите или выключите доверенную зону, заданные в ней исключения начнут или перестанут действовать в выполняющихся задачах немедленно.

► *Чтобы включить или выключить применение доверенной зоны в задачах Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню задачи, для которой хотите настроить применение доверенной зоны.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке Общие в соответствующем блоке выполните одно из следующих действий:
   - Если вы хотите применять доверенную зону в задаче, установите флажок **Применять доверенную зону**.
   - Если вы хотите выключить применение доверенной зоны в задаче, снимите флажок **Применять доверенную зону**.
4. Если вы хотите настроить параметры доверенной зоны, перейдите по ссылке, расположенной в названии флажка **Применять доверенную зону** (см. раздел "Добавление исключений в доверенную зону" на стр. 55).
5. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Добавление исключений в доверенную зону

Этот раздел содержит инструкции по добавлению единых исключений в доверенную зону Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

Доверенные процессы

Вы можете добавить процесс в список доверенных процессов одним из следующих способов:

- выбрать процесс из списка процессов, выполняемых на защищаемом компьютере;
- выбрать исполняемый файл процесса независимо от того, выполняется ли процесс в текущий момент.

> Если исполняемый файл процесса изменится, Kaspersky Industrial CyberSecurity for Nodes 2.5 исключит этот процесс из списка доверенных процессов.

► *Чтобы добавить один или несколько процессов в список доверенных, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. На закладке **Доверенные процессы** установите флажок **Не проверять файловую активность указанных процессов**.
4. Нажмите на кнопку **Добавить**.
5. Выберите один из вариантов из контекстного меню кнопки:
   - **Несколько процессов**.

     В открывшемся окне **Добавление процессов в список доверенных** настройте следующие параметры:

     a. **Использовать полный путь для определения доверенности процесса**.

        Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать полный путь к файлу для определения статуса доверенности процесса.

        Если флажок не установлен, путь к файлу не будет учитываться в качестве критерия для определения статуса доверенности процесса.

        По умолчанию флажок установлен.

     b. **Использовать хеш файла для определения доверенности процесса**.

        Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать хеш выбранного файла для определения статуса доверенности процесса.

        Если флажок не установлен, хеш файла не будет учитываться в качестве критерия для определения статуса доверенности процесса.

        По умолчанию флажок установлен.

     c. Чтобы добавить данные на основе исполняемых файлов, нажмите на кнопку **Обзор**.

     d. Выберите исполняемый файл в открывшемся окне.

        > Вы можете добавлять процессы только по одному. Повторите шаги c-d, чтобы добавить другие исполняемые файлы.

     e. Чтобы добавить данные на основе запущенных процессов, нажмите на кнопку **Процессы**.

     f. Выберите процессы в открывшемся окне. Чтобы выбрать несколько процессов, удерживайте клавишу **CTRL** при выборе.

g. Нажмите на кнопку **OK**.

> Требуется, чтобы учетная запись, с правами которой запускается задача Постоянная защита файлов, имела права администратора на компьютере с установленной программой Kaspersky Industrial CyberSecurity for Nodes 2.5, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, PID или пути к исполняемому файлу процесса на локальном компьютере. Обратите внимание, что вы можете выбрать процесс из списка запущенных процессов, нажав на кнопку **Процессы**, только при работе через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 на локальном компьютере или в параметрах узла в Kaspersky Security Center.

- **Один процесс на основе имени и пути.**

  В открывшемся окне **Добавление процессов в список доверенных вручную** настройте следующие параметры:

  a. Укажите путь к исполняемому файлу (включая имя файла)

  b. Нажмите на кнопку **OK**.

- **Один процесс на основе свойств объекта.**

  В открывшемся окне **Добавление процессов в список доверенных** настройте следующие параметры:

  a. Нажмите на кнопку **Обзор** и выберите процесс.

  b. **Использовать полный путь для определения доверенности процесса**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать полный путь к файлу для определения статуса доверенности процесса.

     Если флажок не установлен, путь к файлу не будет учитываться в качестве критерия для определения статуса доверенности процесса.

     По умолчанию флажок установлен.

  c. **Использовать хеш файла для определения доверенности процесса**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать хеш выбранного файла для определения статуса доверенности процесса.

     Если флажок не установлен, хеш файла не будет учитываться в качестве критерия для определения статуса доверенности процесса.

     По умолчанию флажок установлен.

  d. Нажмите на кнопку **OK**.

> Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран по крайней мере один критерий доверенности.

6. В окне **Добавление доверенного процесса** нажмите на кнопку **OK**.

Выбранный файл или процесс будет добавлен в список доверенных процессов в окне **Доверенная зона**.

Удаление процесса из списка доверенных

► *Чтобы выключить применение доверенного процесса в доверенной зоне, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. В окне **Доверенная зона** на закладке **Доверенные процессы** в списке доверенных процессов снимите флажок рядом с именем исполняемого файла процесса, который вы хотите временно не применять в доверенной зоне.
4. Нажмите на кнопку **OK**.

Окно **Доверенная зона** будет закрыто; выбранные процессы будут удалены из списка доверенных.

Выключение Постоянной защиты файлов на время резервного копирования

► *Чтобы выключить постоянную защиту файлов на время резервного копирования данных с жестких дисков, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. В окне **Доверенная зона**, на закладке **Доверенные процессы** установите флажок **Не проверять файловые операции резервного копирования**.
4. Нажмите на кнопку **OK**.

Окно **Доверенная зона** будет закрыто; постоянная защита файлов будет приостановлена на время резервного копирования.

Добавление исключения в доверенную зону

► *Чтобы добавить исключения в доверенную зону, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
2. Выберите пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. В окне **Доверенная зона** на закладке **Исключения** нажмите на кнопку **Добавить**.

   Откроется окно **Исключение**.

4. В блоке **Объект не будет проверяться при выполнении следующих условий** укажите объекты, которые вы хотите исключить из области защиты / проверки, и объекты, которые вы хотите исключить из числа обнаруживаемых (например, утилиты удаленного администрирования):

   - Если вы хотите исключить объект из области защиты / проверки, выполните следующие действия:

     a. Установите флажок **Проверяемый объект**.

     Добавление файла, папки, диска или файла скрипта в исключение.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает указанную предопределенную область, файл, папку, диск или файл скрипта при проверке с использованием компонента Kaspersky Industrial CyberSecurity for Nodes 2.5, выбранного в блоке **Область применения правила**.

     По умолчанию флажок установлен.

     b. Нажмите на кнопку **Изменить**.

     Откроется окно **Выбор объекта**.

     c. В открывшемся окне укажите объект, который хотите исключить из области проверки.

     Вы можете использовать специальные символы ? и * при указании объектов.

   - Если вы хотите указать имя обнаруживаемого объекта, выполните следующие действия:

     a. Установите флажок **Обнаруживаемые объекты**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта.Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии (http://www.securelist.ru).

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке указанные обнаруживаемые объекты.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.

     b. Нажмите на кнопку **Изменить**.

     Откроется окно **Список обнаруживаемых объектов**.

     c. В открывшемся окне укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии (http://www.securelist.ru).

   - В блоке **Область применения исключений** установите флажки рядом с названием задач, в которых применяется исключение.

5. Нажмите на кнопку **ОК**.

Добавленное исключение отобразится в списке на закладке **Исключения** окна **Доверенная зона**.

Управление задачами Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию о задачах Kaspersky Industrial CyberSecurity for Nodes, их создании, настройке параметров выполнения, запуске и остановке.

В этом разделе

Категории задач Kaspersky Industrial CyberSecurity for Nodes 2.5

Функции постоянной защиты компьютера, контроля компьютера, проверки по требованию и обновления Kaspersky Industrial CyberSecurity for Nodes 2.5 реализованы в виде задач.

Вы можете управлять задачей с помощью пунктов контекстного меню названия задачи в дереве Консоли, панели инструментов и панели быстрого доступа. 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 2.5: *локальные* и *групповые*.

Локальные задачи

Локальные задачи выполняются только на том защищаемом компьютере, для которого они созданы. В зависимости от способа запуска существуют следующие типы локальных задач:

- **Локальные системные задачи**. Создаются автоматически при установке Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете изменять параметры всех системных задач, кроме задач Проверка объектов на карантине и Откат обновления баз программы. Вы не можете переименовывать или удалять системные задачи. Вы можете запускать системные и пользовательские задачи проверки по требованию одновременно.
- **Локальные пользовательские задачи**. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете создавать задачи проверки по требованию. В Kaspersky Security Center вы можете создавать задачи проверки по требованию, обновления баз программы, отката обновления баз программы и копирования обновлений. Такие задачи называются пользовательскими. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

Групповые задачи

Групповые задачи и задачи для наборов компьютеров, созданные через Kaspersky Security Center, отображаются в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Такие задачи называются групповыми. Вы можете управлять групповыми задачами и настраивать их из программы Kaspersky Security Center. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете только просматривать состояние групповых задач.

Сохранение задачи после изменения ее параметров

Вы можете изменять параметры как выполняемой, так и остановленной (приостановленной) задачи. Новые значения параметров вступят в силу при следующих условиях:

- если вы изменили параметры выполняемой задачи: новые значения параметров применяются сразу после сохранения задачи;.
- если вы изменили параметры остановленной (приостановленной) задачи: новые значения параметров применяются при следующем запуске задачи.

► *Чтобы сохранить измененные параметры задачи,*

в контекстном меню названия задачи выберите пункт **Сохранить задачу**.

Если после изменения параметров задачи вы выберете другой узел дерева Консоли, не выбрав предварительно команду **Сохранить задачу**, появится окно сохранения параметров.

► *Чтобы сохранить измененные параметры при переходе к другому узлу Консоли,*

в окне сохранения параметров нажмите на кнопку **Да**.

Запуск / приостановка / возобновление / остановка задачи вручную

Вы можете приостанавливать и возобновлять только задачи постоянной защиты компьютера и проверки по требованию.

► *Чтобы запустить / приостановить / возобновить / остановить задачу, выполните следующие действия:*

1. Откройте контекстное меню названия задачи в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.
2. Выберите одну из следующих команд: **Запустить**, **Приостановить**, **Возобновить** или **Остановить**.

Операция будет выполнена и зарегистрирована в журнале системного аудита (на стр. 259).

После возобновления задачи проверки по требованию Kaspersky Industrial CyberSecurity for Nodes 2.5 продолжает проверку с того объекта, на котором выполнение задачи было приостановлено.

Работа с расписанием задач

Вы можете настраивать запуск задач Kaspersky Industrial CyberSecurity for Nodes 2.5 по расписанию, а также настраивать параметры запуска по расписанию.

В этом разделе

Настройка параметров расписания запуска задач

В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

► *Чтобы настроить параметры расписания запуска задачи, выполните следующие действия:*

1. Откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** включите запуск задачи по расписанию, установив флажок **Запускать задачу по расписанию**.
4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:
   a. В списке **Частота запуска** выберите одно из следующих значений:
      - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное вами количество часов, и укажите количество часов в поле **Раз в <количество> ч.**;
      - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное вами количество дней, и укажите количество дней в поле **Раз в <количество> сут.**;
      - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное вами количество недель, и укажите количество недель в поле **Раз в <количество> нед**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам);
      - **При запуске программы**, если хотите, чтобы задача запускалась при каждом запуске Kaspersky Industrial CyberSecurity for Nodes 2.5;
      - **После обновления баз программы**, если хотите, чтобы задача запускалась после каждого обновления баз программы.
   b. В поле **Время запуска** укажите время первого запуска задачи.
   c. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** появится информация о расчетном времени очередного запуска задачи. Обновленная информация о расчетном времени следующего запуска будет отображаться каждый раз, когда вы откроете окно **Параметры задачи** на закладке **Расписание**.
В поле **Следующий запуск** отображается значение **Запрещен политикой**, если запуск системных задач по расписанию определен параметрами действующей политики Kaspersky Security Center.

5. На закладке **Дополнительно** настройте в соответствии с вашими требованиями следующие параметры расписания.
   - В блоке **Параметры остановки задачи**:
     a. Установите флажок **Длительность** и введите нужное количество часов и минут в полях справа, чтобы указать максимальную длительность выполнения задачи.
     b. Установите флажок **Приостановить с** и введите начальное и конечное значение временного промежутка в полях справа, чтобы указать промежуток времени в пределах суток, в течение которого выполнение задачи будет приостановлено.
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
     c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.
6. Нажмите на кнопку **Применить**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

Включение и выключение запуска по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

► *Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню названия задачи, расписание запуска которой вы хотите настроить.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке Расписание выполните одно из следующих действий:
   - установите флажок **Запускать задачу по расписанию**, если хотите включить запуск задачи по расписанию;
   - снимите флажок **Запускать задачу по расписанию,** если хотите выключить запуск задачи по расписанию.

Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.

4. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Использование учетных записей для запуска задач

Вы можете запускать задачи, используя системную учетную запись пользователя или указать другую учетную запись.

В этом разделе

Об использовании учетных записей для запуска задач

Вы можете указать учетную запись, с правами которой вы хотите запускать выбранную задачу, для следующих функциональных компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5:

- задачи формирования правил контроля устройств и контроля запуска программ;
- задачи проверки по требованию;
- Задачи обновления

По умолчанию указанные задачи выполняются с правами системной учетной записи.

Рекомендуется указать другую учетную запись с достаточными правами доступа в следующих случаях:

- в задаче обновления, если в качестве источника обновления вы указали папку общего доступа на другом компьютере в сети;
- в задаче обновления, если для доступа к источнику обновлений используется прокси-сервер со встроенной проверкой подлинности Microsoft Windows (NTLM-authentication);
- в задачах проверки по требованию, если системная учетная запись не обладает правами доступа к каким-либо из проверяемых объектов (например, к файлам в общих сетевых папках компьютера);
- в задаче автоматического формирования правил, если после окончания выполнения задачи сформированные правила экспортируются в конфигурационный файл, недоступный для системной учетной записи (например, расположенный в одной из общих сетевых папок компьютера).

Вы можете запускать задачи обновления, проверки по требованию и автоматического формирования разрешающих правил контроля запуска программ с правами системной учетной записи. В ходе выполнения этих задач Kaspersky Industrial CyberSecurity for Nodes 2.5 обращается к папкам общего доступа на другом компьютере в сети, если этот компьютер зарегистрирован в одном домене с защищаемым компьютером. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Industrial CyberSecurity for Nodes 2.5 будет обращаться к компьютеру с правами учетной записи **<имя домена \ имя компьютера>**.

Указание учетной записи для запуска задачи

► *Чтобы указать учетную запись для запуска задачи, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню названия задачи, для которой вы хотите настроить запуск с правами учетной записи.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке Запуск с правами выполните следующие действия:
   a. Выберите пункт **Имя пользователя**.
   b. Укажите имя и пароль пользователя, учетную запись которого вы хотите использовать.

      Выбранный вами пользователь должен быть зарегистрирован на защищаемом компьютере или в одном домене с ним.

   c. Подтвердите введенный пароль.
4. Нажмите на кнопку **Применить**.

Измененные параметры запуска задачи с правами учетной записи будут сохранены.

Импорт и экспорт параметров

Этот раздел содержит информацию об экспорте параметров работы Kaspersky Industrial CyberSecurity for Nodes 2.5 или параметров работы отдельных компонентов программы в конфигурационный файл в формате XML и импорте этих параметров из конфигурационного файла в программу.

В этом разделе

Об импорте и экспорте параметров

Вы можете экспортировать параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Industrial CyberSecurity for Nodes 2.5 из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.

Когда вы экспортируете все параметры Kaspersky Industrial CyberSecurity for Nodes 2.5, в файл сохраняются общие параметры программы и параметры следующих компонентов и функций Kaspersky Industrial CyberSecurity for Nodes 2.5:

- Бизнес-логика.
- Права доступа.
- Параметры соединения.
- Постоянная защита файлов.
- Использование KSN.
- Контроль устройств.
- Контроль запуска программ.
- Формирование правил контроля устройств.
- Формирование правил контроля запуска программ.
- Проверка по требованию.
- Мониторинг файловых операций.
- Проверка целостности проектов ПЛК.
- Получение данных о проектах ПЛК.
- Контроль Wi-Fi.
- Анализ журналов.
- Защита то шифрования.
- Управление сетевым экраном.
- Обновление баз и модулей Kaspersky Industrial CyberSecurity for Nodes 2.5.
- Карантин.
- Резервное хранилище.
- Журналы.
- Уведомления администратора и пользователей.
- Доверенная зона.
- Защита от эксплойтов.
- Хранилище Заблокированных узлов.
- Защита паролем.

Также вы можете сохранять в файле общие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 и права учетных записей пользователей.

Вы не можете экспортировать параметры групповых задач.

Kaspersky Industrial CyberSecurity for Nodes 2.5 экспортирует все пароли, которые используются для работы программы, например учетные данные для запуска задач или соединения с прокси-сервером. Экспортированные пароли хранятся в конфигурационном файле в зашифрованном виде. Вы можете импортировать пароли только с помощью программы Kaspersky Industrial CyberSecurity for Nodes 2.5, установленной на этом же компьютере, если она не была переустановлен или обновлена.

Вы не можете импортировать ранее сохраненные пароли с помощью программы Kaspersky Industrial CyberSecurity for Nodes 2.5, установленной на другом компьютере. После импорта параметров на другом компьютере вам нужно ввести все пароли вручную.

Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует значения, применяемые политикой.

Вы можете импортировать параметры из конфигурационного файла, содержащего параметры только некоторых компонентов Kaspersky Industrial CyberSecurity for Nodes 2.5 (например, созданного в программе Kaspersky Industrial CyberSecurity for Nodes 2.5, установленной с неполным набором компонентов). После импорта параметров в Kaspersky Industrial CyberSecurity for Nodes 2.5 изменяются только те параметры, которые содержались в конфигурационном файле. Остальные параметры не изменяются.

Заблокированные параметры активной политики Kaspersky Security Center при импорте параметров не изменяются.

Экспорт параметров

► *Чтобы экспортировать параметры в конфигурационный файл, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выполните одно из следующих действий:
   - В контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes** выберите пункт **Экспортировать параметры**, чтобы экспортировать все параметры Kaspersky Industrial CyberSecurity for Nodes 2.5.
   - В контекстном меню названия задачи, параметры которой вы хотите экспортировать, и выберите пункт **Экспортировать параметры,** чтобы экспортировать параметры отдельного функционального компонента программы.
   - Чтобы экспортировать параметры компонента Доверенная зона:
     a. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
     b. Выберите пункт **Настроить параметры доверенной зоны**.

        Откроется окно **Доверенная зона**.
     c. Нажмите на кнопку **Экспорт**.

        Откроется окно приветствия мастера экспорта параметров.
2. Выполните инструкции в окнах **мастера**: задайте имя конфигурационного файла, в котором вы хотите сохранить параметры, и путь к файлу.

Указывая путь, вы можете использовать системные переменные окружения, но не можете использовать пользовательские переменные окружения.

Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует значения параметров в политике.

3. В окне **Экспорт параметров программы завершен** нажмите на кнопку **ОК**.

Мастер экспорта параметров будет закрыт; экспорт параметров будет завершен.

Импорт параметров

► *Чтобы импортировать параметры из конфигурационного файла, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выполните одно из следующих действий:
   - В контекстном меню узла **Kaspersky Industrial CyberSecurity for Nodes** выберите пункт **Импортировать параметры**, чтобы импортировать все параметры Kaspersky Industrial CyberSecurity for Nodes 2.5.
   - В контекстном меню названия задачи, параметры которой вы хотите импортировать, и выберите пункт **Импортировать параметры**, чтобы импортировать параметры отдельного функционального компонента.
   - Чтобы импортировать параметры компонента Доверенная зона:
     a. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes**.
     b. Выберите пункт **Настроить параметры доверенной зоны**.

        Откроется окно **Доверенная зона**.
     c. Нажмите на кнопку **Импорт**.

        Откроется окно приветствия мастера импорта параметров.
2. Выполните инструкции в окнах мастера: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

   После того как вы импортируете общие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5 или его функциональных компонентов на компьютере, вы не сможете вернуть их прежние значения.
3. В окне **Импорт параметров программы завершен** нажмите на кнопку **ОК**.

   Мастер импорта параметров будет закрыт; импортированные параметры будут сохранены.
4. В панели инструментов Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 нажмите на кнопку **Обновить**.

Импортированные параметры отобразятся в окне Консоли.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не импортирует пароли (данные учетных записей для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом компьютере или на том же компьютере, после того как на нем была переустановлена или обновлена программа Kaspersky Industrial CyberSecurity for Nodes 2.5. После завершения импорта вам нужно ввести пароли вручную.

Использование шаблонов параметров безопасности

Этот раздел содержит информацию о работе с шаблонами параметров безопасности в задачах защиты и проверки Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

О шаблонах параметров безопасности

Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов компьютера и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Industrial CyberSecurity for Nodes.

Использование шаблонов доступно при настройке параметров безопасности следующих задач Kaspersky Industrial CyberSecurity for Nodes 2.5:

- Постоянная защита файлов.
- Проверка при старте операционной системы;
- Проверка важных областей;
- пользовательские задачи проверки по требованию.

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов компьютера, устанавливаются на все вложенные узлы. Шаблон родительского узла не применяется к вложенным узлам в следующих случаях:

- Если параметры безопасности вложенных узлов настраивались отдельно (см. раздел "Применение шаблона параметров безопасности" на стр. 71).
- Если вложенные узлы виртуальные. Вам нужно применить шаблон для каждого виртуального узла отдельно.

Создание шаблона параметров безопасности

► *Чтобы сохранить параметры безопасности узла вручную и сохранить эти параметры в шаблон, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите задачу, параметры безопасности которой вы хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или в списке сетевых файловых ресурсов компьютера выберите шаблон, который вы хотите просмотреть.
4. На закладке **Уровень безопасности** нажмите на кнопку **Сохранить как шаблон**.

   Откроется окно **Свойства шаблона**.
5. В поле **Название шаблона** введите название шаблона.
6. В поле **Описание** введите любую дополнительную информацию о шаблоне.
7. Нажмите на кнопку **OK**.

Шаблон с набором значений параметров безопасности будет сохранен.

Вы также можете перейти к созданию шаблона параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.

Просмотр параметров безопасности в шаблоне

► *Чтобы просмотреть значения параметров безопасности в созданном шаблоне, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите задачу, шаблон безопасности для которой вы хотите просмотреть.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите просмотреть.
4. Нажмите на кнопку **Просмотреть**.

Откроется окно **<Имя шаблона>**. На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне; на закладке **Параметры** приводится список значений параметров безопасности, сохраненных в шаблоне.

Применение шаблона параметров безопасности

► *Чтобы применить параметры безопасности из шаблона для выбранного узла, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите задачу, параметры безопасности которой вы хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке сетевых файловых ресурсов компьютера откройте контекстное меню узла, для которого вы хотите применить шаблон.
4. Выберите **Применить шаблон** > **<Имя шаблона>**.
5. В дереве Консоли откройте контекстное меню настраиваемой задачи.
6. Выберите пункт **Сохранить задачу**.

Шаблон параметров безопасности будет применен к выбранному узлу в дереве файловых ресурсов компьютера. На закладке **Уровень безопасности выбранного узла будет установлено значение** Другой.

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов компьютера, устанавливаются на все вложенные узлы.

Если область защиты или область проверки вложенных узлов в дереве файловых ресурсов компьютера настраивалась отдельно, параметры безопасности из шаблона, примененного к родительскому узлу, не установятся автоматически для таких вложенных узлов.

► *Чтобы установить параметры безопасности из шаблона для всех вложенных узлов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите задачу, параметры безопасности которой вы хотите сохранить в шаблон.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке сетевых файловых ресурсов компьютера выберите родительский узел, чтобы применить шаблон к этому узлу и ко всем вложенным узлам.
4. Выберите **Применить шаблон** > **<Имя шаблона>**.
5. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню настраиваемой задачи.
6. Выберите пункт **Сохранить задачу**.

Шаблон параметров безопасности будет применен к родительскому и всем вложенным узлам в дереве файловых ресурсов компьютера. На закладке **Уровень безопасности выбранного узла** будет установлено значение **Другой**.

Удаление шаблона параметров безопасности

► *Чтобы удалить шаблон параметров безопасности, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите задачу, для настройки которой вы больше не хотите использовать шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Вы можете перейти к созданию шаблона параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.

   Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения операции удаления.
5. В открывшемся окне нажмите на кнопку **Да**.

Выбранный шаблон будет удален.

Если шаблон параметров безопасности применялся для защиты или проверки узлов файловых ресурсов компьютера, настроенные параметры безопасности для этих узлов сохраняются после удаления шаблона.

Постоянная защита компьютера

Этот раздел содержит информацию о компонентах постоянной защиты: Постоянная защита файлов, Использование KSN, Защита от шифрования и Защита от эксплойтов. Также этот раздел содержит инструкции по настройке параметров задач постоянной защиты и по настройке параметров безопасности защищаемого компьютера.

В этом разделе

Постоянная защита файлов

Этот раздел содержит информацию о задаче Постоянная защита файлов и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет следующие объекты защищаемого компьютера при доступе к ним:

- файлы;
- альтернативные потоки файловых систем (NTFS-streams);
- главную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств;
- файлы контейнеров Windows Server® 2016.

При записи или считывании записанного файла любой программой на компьютере Kaspersky Industrial CyberSecurity for Nodes 2.5 перехватывает этот файл, проверяет его на наличие угроз компьютерной безопасности и при обнаружении угрозы выполняет действия, указанные в параметрах задачи или заданные по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Kaspersky Industrial CyberSecurity for Nodes возвращает файл программе, если он не заражен или успешно вылечен.

Kaspersky Industrial CyberSecurity for Nodes 2.5 перехватывает файловые операции, исполняемые в контейнерах Windows Server 2016.

Контейнер – это изолированная среда, где программа может работать, не оказывая воздействия на операционную систему и не подвергаясь при этом воздействию с ее стороны. Если контейнер расположен в области защиты задачи, Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5 также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem для Linux®. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих настройках.

Статистика задачи Постоянная защита файлов

Пока выполняется задача Постоянная защита файлов, вы можете просматривать в реальном времени информацию о количестве объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обработала с момента запуска задачи до текущего момента.

► *Чтобы просмотреть статистику задачи Постоянная защита файлов, выполните следующие действия:*

1. В дереве Консоли разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть следующую информацию об объектах, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обработала с момента запуска задачи до текущего момента (см. таблицу ниже).

Таблица 16. Статистика задачи Постоянная защита файлов

Поле	Описание
Обнаружено	Количество объектов, которые обнаружила программа Kaspersky Industrial CyberSecurity for Nodes 2.5. Например, если программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаружила в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу.
Зараженных и других обнаруженных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 признала зараженными, или обнаруженных объектов, которые не были исключены из области действия задач постоянной защиты или проверки по требованию и были определены как легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 признала возможно зараженными.
Объектов не вылечено	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 не вылечила по следующим причинам: • тип обнаруженного объекта не предполагает лечения; • при лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 попыталась поместить на карантин, но безуспешно, например, из-за отсутствия доступного пространства на диске.
Объектов не удалено	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 не смогла проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes 2.5 попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые вылечила программа Kaspersky Industrial CyberSecurity for Nodes 2.5.
Помещено на карантин	Количество объектов, которые поместила на карантин программа Kaspersky Industrial CyberSecurity for Nodes 2.5.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes 2.5 сохранила в резервном хранилище.
Удалено объектов	Количество объектов, которые удалила программа Kaspersky Industrial CyberSecurity for Nodes 2.5.

Поле	Описание
Защищенных паролем объектов	Количество объектов (например, архивов), которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 пропустила, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 пропустила, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые обработала программа Kaspersky Industrial CyberSecurity for Nodes 2.5.

Вы также можете посмотреть статистику задачи Постоянная защита файлов в журнале выполнения задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

Если значение в поле **Всего событий** в окне журнала выполнения задачи Постоянная защита файлов больше 0, рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Настройка параметров задачи Постоянная защита файлов

По умолчанию системная задача Постоянная защита файлов имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 17. Параметры задачи Постоянная защита файлов по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Весь компьютер, исключая виртуальные диски.	Вы можете ограничить область защиты.
Уровень безопасности	Единый для всей области защиты; соответствует уровню безопасности **Рекомендуемый**.	Для выбранных узлов в дереве файловых ресурсов компьютера вы можете: • применить другой предустановленный уровень безопасности; • вручную изменить уровень безопасности; • сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.
Режим защиты объектов	При открытии и изменении.	Вы можете выбрать режим защиты объектов – указать, при каком типе доступа к объектам Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет их.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа.
Применять доверенную зону.	Применяется.	Единый список исключений, который вы можете применять в выбранных задачах.
Использование служб KSN	Применяется	Вы можете увеличить эффективность защиты компьютера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Расписание запуска задачи	При запуске программы	Вы можете настраивать параметры запуска задачи по расписанию.
Блокировать компьютеры, с которых ведется вредоносная активность	Не применяется	Вы можете включить добавление компьютеров, со стороны которых выявлена вредоносная активность, в список недоверенных узлов.

Чтобы настроить параметры задачи Постоянная защита файлов, выполните следующие действия:

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - **Использовать эвристический анализатор** (см. раздел "**Использование эвристического анализатора**" на стр. 80);

- **Режим защиты объектов** (см. раздел "**Выбор режима защиты объектов**" на стр. 79);
- **Интеграция с другими компонентами** (см. раздел "**Интеграция задачи с другими компонентами Kaspersky Industrial CyberSecurity for Nodes 2.5**" на стр. 81).

- На закладках **Расписание** и **Дополнительно**:
  - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 62)

5. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Изменения параметров задачи будут сохранены.

6. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.
7. Выполните следующие действия:
   - В дереве или списке файловых ресурсов компьютера выберите узлы, которые вы хотите включить в область защиты задачи (см. раздел "Об области защиты в задаче Постоянная защита файлов" на стр. 85).
   - Выберите один из предустановленных уровней безопасности (см. раздел "Выбор предустановленных уровней безопасности" на стр. 91) или настройте параметры защиты объектов вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 93).
8. В окне **Настройка области защиты**, нажмите на кнопку **Сохранить**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. Блок **Режим защиты объектов** позволяет определить, при каком типе доступа к объектам Kaspersky Industrial CyberSecurity for Nodes 2.5 их проверяет.

Параметр **Режим защиты объектов** имеет единое значение для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

► *Чтобы выбрать режим защиты объектов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне на закладке **Общие** выберите режим защиты объектов, который вы хотите установить:
   - **Интеллектуальный режим**

Kaspersky Industrial CyberSecurity for Nodes 2.5 выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс во время своей работы многократно обращается к объекту и изменяет его, Kaspersky Industrial CyberSecurity for Nodes 2.5 повторно проверяет объект только после его последнего сохранения этим процессом.

- **При открытии и изменении.**

  Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объект при открытии и проверяет его повторно при сохранении, если объект был изменен.

  Данный вариант выбран по умолчанию.

- **При открытии.**

  Kaspersky Industrial CyberSecurity for Nodes проверяет все объекты при их открытии как на чтение, так и на выполнение или изменение.

- **При выполнении.**

  Kaspersky Industrial CyberSecurity for Nodes проверяет файл только при открытии на выполнение.

5. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

Применение эвристического анализатора

Вы можете использовать эвристический анализатор и настроить уровень анализа для задач Проверка по требованию и Постоянная защита файлов.

► *Чтобы настроить применение эвристического анализатора, выполните следующие действия:*

1. В зависимости от задачи:
   - Для задачи Проверка по требованию:
     a. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
     b. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
     c. В панели результатов перейдите по ссылке **Свойства**.
   - Для задачи Постоянная защита файлов:
     a. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита файлов**.
     b. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
2. Снимите или установите флажок **Использовать эвристический анализатор**.
3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни детализации проверки:

- **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

  Этот уровень выбран по умолчанию.
- **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

4. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены. немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Интеграция задачи с другими компонентами Kaspersky Industrial CyberSecurity for Nodes 2.5

В задаче Постоянная защита файлов вы можете настроить параметры интеграции задачи с другими функциональными компонентами Kaspersky Industrial CyberSecurity for Nodes 2.5.

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network и запустить задачу.

► *Чтобы настроить взаимодействие задачи Постоянная защита файлов с другими компонентами программы, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Интеграция с другими компонентами** настройте следующие параметры:
   - Установите или снимите флажок **Применять доверенную зону**.

     Флажок включает или выключает применение доверенной зоны в работе задачи.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не учитывает файловые операции доверенных процессов при формировании области защиты в задаче Постоянная защита файлов.

По умолчанию флажок установлен.

- Установите или снимите флажок **Использовать KSN для защиты**.

  Этот флажок включает или выключает использование служб KSN.

  Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

  Если флажок снят, задача не использует службы KSN.

  По умолчанию флажок установлен.

  Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи Использование KSN.

5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

Список расширений файлов, проверяемых по умолчанию в задаче Постоянная защита файлов

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 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?*

Область защиты в задаче Постоянная защита файлов

Этот раздел содержит информацию о формировании и использовании области защиты в задаче Постоянная защита файлов и дальнейшей работе с ней.

В этом разделе

Об области защиты в задаче Постоянная защита файлов

По умолчанию под действие задачи Постоянная защита файлов подпадают все объекты файловой системы компьютера. 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 Kaspersky Industrial CyberSecurity for Nodes 2.5 область защиты представляет собой дерево или список файловых ресурсов компьютера, которые программа может контролировать. По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.

► *Чтобы включить отображение файловых ресурсов компьютера в виде дерева,*

в раскрывающемся списке, расположенном в левом верхнем углу окна **Настройка области защиты**, выберите пункт **Показывать в виде дерева**.

Узлы в дереве или списке файловых ресурсов компьютера отображаются следующим образом:

 Узел включен в область защиты.

 Узел исключен из области защиты.

 По крайней мере один из узлов, вложенных в этот узел, исключен из области защиты, или параметры безопасности вложенных узлов отличаются от параметров безопасности этого узла (только для режима отображения в виде дерева).

Значок  отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области защиты для выбранного вложенного узла.

Имена виртуальных узлов области защиты отображаются шрифтом синего цвета.

Предопределенные области защиты

Файловые ресурсы защищаемого компьютера отображается в панели результатов узла **Постоянная защита файлов** по ссылке **Настройка области защиты**. Вы можете настроить отображение файловых ресурсов в виде списка или дерева.

Дерево или список файловых ресурсов отображает узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Industrial CyberSecurity for Nodes 2.5 предусмотрены следующие предопределенные области защиты:

- **Локальные жесткие диски**. Kaspersky Industrial CyberSecurity for Nodes 2.5 защищает файлы на жестких дисках компьютера.
- **Съемные диски**. Kaspersky Industrial CyberSecurity for Nodes 2.5 защищает файлы на внешних устройствах, например, на компакт-дисках или флеш-накопителях. 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 2.5 защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на компьютере. Kaspersky Industrial CyberSecurity for Nodes 2.5 не защищает файлы в сетевых папках, когда к ним обращаются программы с других компьютеров.
- **Виртуальные диски**. Вы можете включать в область защиты динамические папки и файлы, а также диски, которые монтируются на компьютер временно, например, общие диски кластера.

Предопределенные области проверки по умолчанию отображаются в дереве файловых ресурсов компьютера и доступны для добавления в список файловых ресурсов при его формировании в параметрах области защиты.

По умолчанию в область защиты включены все предопределенные области, кроме виртуальных дисков.

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов компьютера в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Чтобы включить в область защиты объекты на псевдодиске, включите в область защиты папку на компьютере, с которой этот псевдодиск связан.
Подключенные сетевые диски также не отображаются в дереве файловых ресурсов компьютера. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Настройка параметров отображения сетевых файловых ресурсов

► *Чтобы выбрать способ отображения файловых ресурсов компьютера при настройке параметров области проверки, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В левом верхнем углу открывшегося окна разверните раскрывающийся список. Выполните одно из следующих действий:
   - Выберите пункт **Показывать в виде дерева**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде дерева.
   - Выберите пункт **Показывать в виде списка**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде списка.

   По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.
5. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут применены.

Формирование области защиты

Процедура формирования области защиты в задаче Постоянная защита файлов зависит от типа отображения файловых ресурсов защищаемого компьютера (см. раздел "Настройка параметров отображения файловых ресурсов области защиты" на стр. 204). Вы можете настроить отображение файловых ресурсов в виде списка (применяется по умолчанию) или в виде дерева.

Чтобы применить к задаче новые настройки области защиты, необходимо перезапустить задачу Постоянной защиты файлов.

► *Чтобы сформировать область защиты, работая с деревом файловых ресурсов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В правой части открывшегося окна разверните дерево файловых ресурсов компьютера, чтобы отобразить все узлы.
5. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
     - если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с именем нужного типа дисков (например, чтобы включить все съемные диски на компьютере, установите флажок **Съемные диски**);
     - если вы хотите включить в область защиты отдельный диск нужного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**.
     - если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
6. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

► *Чтобы сформировать область защиты, работая со списком файловых ресурсов, выполните следующие действия*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область защиты**.
   c. В открывшемся окне **Добавление области защиты** выберите тип объекта, который вы хотите добавить в область защиты:

- **Предопределенная область**, если вы хотите включить в область защиты одну из предопределенный областей на защищаемом компьютере. Затем в раскрывающемся списке выберите необходимую область.
- **Диск, папка или сетевой объект**, если вы хотите включить в область защиты отдельный диск, папку или сетевой объект нужного типа. Затем выберите необходимый файл по кнопке **Обзор**.
- **Файл**, если вы хотите включить в область защиты только отдельный файл на диске. Затем выберите необходимый файл по кнопке **Обзор**.

Вы не можете добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.

5. Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В открывшемся окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
6. Чтобы изменить добавленную область защиты или исключение, в контекстном меню области, которую хотите изменить, выберите пункт **Изменить область**.
7. Чтобы скрыть отображение ранее добавленной области защиты или исключения в списке файловых ресурсов, в контекстном меню области, которую хотите скрыть, выберите пункт **Удалить из списка**.

   Область защиты исключается из области действия задачи Постоянная защита файлов при ее удалении из списка файловых ресурсов.

8. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

Вы можете запустить задачу **Постоянная защита файлов,** если по крайней мере один узел файловых ресурсов компьютера включен в область защиты. Если вы укажете сложную область защиты, например, установите различные значения параметров безопасности для многих отдельных узлов в дереве файловых ресурсов компьютера, это может привести к замедлению проверки объектов при доступе.

О виртуальной области защиты

Kaspersky Industrial CyberSecurity for Nodes 2.5 может проверять не только существующие папки и файлы на жестких и съемных дисках, но и папки и файлы, которые динамически создаются на компьютере различными программами и службами.

Если вы включили в область защиты все объекты компьютера, эти динамические узлы автоматически войдут в область защиты. Однако если вы хотите задать специальные значения параметров безопасности для этих динамических узлов или вы выбрали для защиты не весь компьютер, а отдельные области, то,

чтобы включить в область защиты динамические диски, файлы или папки, вам нужно предварительно создать их в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5, то есть задать виртуальную область защиты. Созданные вами диски, файлы и папки существуют только в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5, но не в структуре файловой системы защищаемого компьютера.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, динамические папки или файлы, которые появятся в ней, не будут автоматически включены в область защиты. Вам нужно создать их виртуальные копии в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 и добавить их в область защиты.

Создание виртуальной области защиты

Вы можете добавить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка параметров отображения файловых ресурсов области защиты" на стр. 204).

► *Чтобы добавить в область защиты виртуальный диск, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. Откройте контекстное меню узла **Виртуальные диски** и в списке доступных имен выберите имя для создаваемого виртуального диска.

   Установите флажок рядом с добавленным диском, чтобы включить этот диск в область защиты.
6. В окне **Настройка области защиты**, нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

► *Чтобы добавить в область защиты виртуальную папку или виртуальный файл, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. Откройте контекстное меню виртуального диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, если хотите добавить виртуальную папку в область защиты.

- **Добавить виртуальный файл**, если хотите добавить виртуальный файл в область защиты.

6. В поле ввода задайте имя для папки или файла.
7. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область защиты.
8. В окне **Настройка области защиты**, нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Параметры безопасности выбранного узла в задаче Постоянная защита файлов

В задаче Постоянная защита файлов вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области защиты или проверки, так и различными для разных узлов в дереве или списке файловых ресурсов компьютера.

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 или проверки одним из следующих способов:

- выбрать один из трех предустановленных уровней безопасности (**Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**);
- вручную изменить параметры безопасности для выбранных узлов в дереве или списке файловых ресурсов компьютера (уровень безопасности примет значение **Другой**).

Вы можете сохранить набор параметров узла в шаблон, чтобы потом применять этот шаблон для других узлов.

Выбор предустановленных уровней безопасности

Для выбранных узлов в дереве или списке файловых ресурсов компьютера вы можете применить один из следующих предустановленных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**. Каждый из этих уровней имеет свой набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, кроме использования Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютерах и рабочих станциях, принимаются дополнительные меры компьютерной безопасности, например сетевые экраны и политики безопасности для пользователей сети.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых компьютеров. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты компьютеров в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если вы предъявляете повышенные требования к компьютерной безопасности в сети организации.

Таблица 18. Предустановленные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности		
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**
Защита объектов	По расширению	По формату	По формату
Проверка только новых и измененных файлов	Включена	Включена	Выключено
Действия над зараженными и другими обнаруженными объектами	Блокировать доступ и лечить. Удалить, если не удалось вылечить.	Блокировать доступ и выполнить рекомендуемое действие.	Блокировать доступ и лечить. Удалить, если не удалось вылечить.
Действия над возможно зараженными объектами	Блокировать доступ и поместить на карантин.	Блокировать доступ и выполнить рекомендуемое действие.	Блокировать доступ и поместить на карантин.
Исключать файлы	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.
Не проверять составные объекты размером более (МБ)	8 МБ	8 МБ	Не установлен
Альтернативные потоки NTFS	Да	Да	Да
Проверять загрузочные секторы дисков и MBR	Да	Да	Да
Защита составных объектов	• упакованные объекты* * Только новые и измененные	• SFX-архивы* • упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• SFX-архивы* • упакованные объекты* • Вложенные OLE-объекты* *Все объекты

Параметры **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** не входят в набор параметров предустановленных уровней безопасности. Если, выбрав один из предустановленных уровней безопасности, вы измените состояние параметров **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор**, выбранный вами предустановленный уровень безопасности не изменится.

► *Чтобы выбрать один из предустановленных уровней безопасности, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. Выберите узел, для которого вы хотите выбрать предустановленный уровень безопасности.
5. Убедитесь, что этот узел включен в область защиты.
6. В правой части окна на закладке **Уровень безопасности** в списке выберите уровень безопасности, который вы хотите применить.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному вами уровню безопасности.
7. В окне **Настройка области защиты**, нажмите на кнопку **Сохранить**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Настройка параметров безопасности вручную

По умолчанию в задачах постоянной защиты компьютера применяются единые параметры безопасности для всей области проверки. Эти параметры соответствуют значениям предустановленного уровня безопасности **Рекомендуемый**.

Вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области защиты, так и различными для разных узлов в дереве или списке файловых ресурсов компьютера.

При работе с деревом файловых ресурсов компьютера 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.

► *Чтобы настроить параметры безопасности вручную, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.
4. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.

   К выбранному узлу в области защиты можно применить предустановленный шаблон с параметрами безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 69).

5. Настройте нужные параметры безопасности выбранного узла в соответствии с вашими требованиями.
   - Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. 94)
   - Действия (см. раздел "Настройка действий" на стр. 96)
   - Производительность (см. раздел "Настройка производительности" на стр. 98)
6. Нажмите кнопку **Сохранить** в окне **Настройка области защиты**.

Новые параметры области защиты будут сохранены.

Настройка общих параметров задачи

► *Чтобы настроить общие параметры безопасности задачи Постоянная защита файлов, выполните следующие действия.*

1. Откройте окно **Настройка области защиты** (см. раздел "Настройка параметров безопасности вручную" на стр. 93).
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите объекты, которые вы хотите включить в область защиты:
   - **Все объекты.**

     Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет все объекты.
   - **Объекты, проверяемые по формату.**

     Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5.
   - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах.**

     Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет только потенциально заражаемые файлы на основании формата файла.

     Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes 2.5.
   - **Объекты, проверяемые по указанному списку расширений.**

     Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы на основании расширения файла. Список расширений файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.
   - **Проверять загрузочные секторы дисков и MBR.**

     Включение защиты загрузочных секторов дисков и главных загрузочных записей.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет загрузочные секторы и загрузочные надписи на жестких и съемных дисках компьютера.

     По умолчанию флажок установлен.
   - **Альтернативные потоки NTFS**

Проверка дополнительных потоков файлов и папок на дисках файловой системы NTFS.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет дополнительные потоки файлов и папок.

По умолчанию флажок установлен.

4. В блоке **Производительность** установите или снимите флажок **Защищать только новые и измененные файлы**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Industrial CyberSecurity for Nodes 2.5 новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок снят, вы можете указать, какие файлы вы хотите проверять и защищать.

   По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**. Если установлен уровень безопасности **Рекомендуемый** или **Максимальная защита**, то флажок снят.

> Для переключения между доступными вариантами при снятом флажке щелкните ссылку **Все** / **Только новые** для каждого типа составных объектов.

5. В блоке **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область защиты:

   - **Все / Только новые архивы.**

     Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет архивы.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

   - **Все / Только новые SFX-архивы.**

     Проверка самораспаковывающихся архивов.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет SFX-архивы.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает SFX-архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

     Параметр активен, если снят флажок **Архивы**.

   - **Все / Только новые почтовые базы.**

     Проверка файлов почтовых баз Microsoft Outlook® и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает файлы почтовых баз при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты.**

  Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые файлы почтовых форматов.**

  Проверка файлов почтовых форматов, например, сообщения форматов Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты.**

  Проверка встроенных в файл объектов (например, макрос Microsoft Word или вложение сообщения электронной почты).

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

► *Чтобы настроить действия, которые задача Постоянная защита файлов выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "Настройка параметров безопасности вручную" на стр. 93).
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

Когда выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется событие *Обнаруженный объект не вылечен согласно пользовательским параметрам задачи*. В событии указана вся доступная информация об обнаруженном объекте, а также тот факт, что объект не был вылечен.

Режим **Только сообщать** требуется отдельно настроить для каждой области защиты. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выберете этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически изменит уровень безопасности на **Пользовательский**.

- **Блокировать доступ**.

  Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes 2.5 блокирует доступ зараженным или другим обнаруженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

- **Выполнять дополнительное действие**.

  Выберите действие из раскрывающегося списка:

  - **Лечить.**
  - **Лечить. Удалить, если не удалось вылечить.**
  - **Удалить**.
  - **Рекомендуемое**.

4. Выберите действие над возможно зараженными объектами:

   - **Только сообщать**.

     Когда выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется событие *Обнаруженный объект не вылечен согласно пользовательским параметрам задачи*. В событии указана вся доступная информация об обнаруженном объекте, а также тот факт, что объект не был вылечен.

     Режим **Только сообщать** требуется отдельно настроить для каждой области защиты. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выберете этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически изменит уровень безопасности на **Пользовательский**.

   - **Блокировать доступ**.

     Если выбран этот вариант, Kaspersky Industrial CyberSecurity for Nodes 2.5 блокирует доступ зараженным или другим обнаруженным объектам. Вы можете выбрать дополнительное действие над заблокированными объектами из раскрывающегося списка.

   - **Выполнять дополнительное действие**.

     Выберите действие из раскрывающегося списка:

     - **Поместить на карантин**.
     - **Удалить**.

- **Рекомендуемое**.

5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, вы можете выбрать основное и дополнительное действие для каждого типа объектов, нажав на кнопку **Настройка**, расположенную рядом с флажком.

      Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет действия, которые выбраны в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** соответственно указанным типам объектов.

      По умолчанию флажок снят.

   a. Нажмите на кнопку **Настройка**.

   b. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.

   c. Нажмите на кнопку **OK**.

6. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

   Флажок включает или выключает форсированное удаление родительского составного файла при обнаружении вложенного вредоносного, возможно зараженного или другого обнаруживаемого объекта.

   Если флажок установлен и задача настроена на удаление зараженных или возможно зараженных объектов, Kaspersky Industrial CyberSecurity for Nodes 2.5 принудительно удаляет весь родительский составной файл при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление составного объекта со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если составной объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Industrial CyberSecurity for Nodes 2.5 не выполняет выбранное действие, если родительский объект неизменяем.

   По умолчанию установлен флажок для уровня безопасности **Максимальная защита** и сняты флажки **Рекомендуемый** и **Максимальное быстродействие**.

7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

► *Чтобы настроить производительность задачи Постоянная защита файлов, выполните следующие действия:*

1. Откройте окно **Настройка области защиты** (см. раздел "Настройка параметров безопасности вручную" на стр. 93).
2. Выберите закладку **Производительность**.

3. В блоке **Исключения**:

   - Снимите или установите флажок **Исключать файлы**.

     Исключение файлов из проверки по имени файла или маске имени файла.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет все объекты.

     По умолчанию флажок снят.

   - Снимите или установите флажок **Не обнаруживать**.

     Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает все объекты, указанные в программе по умолчанию.

     По умолчанию флажок снят.

   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

4. В блоке **Дополнительные параметры**:

   - **Останавливать проверку, если она длится более (сек.).**

     Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

     Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

     Если флажок снят, максимальная продолжительность проверки не ограничена.

     По умолчанию флажок установлен.

   - **Не проверять составные объекты размером более (МБ).**

     Исключение из проверки составных объектов больше указанного размера.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет составные объекты, не учитывая размер.

     По умолчанию флажок установлен для уровней безопасности **Рекомендуемый** и **Максимальное быстродействие**.

   - **Использовать технологию iSwift.**

     Проверка только новых или измененных с момента последней проверки объектов файловой системы NTFS.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты файловой системы NTFS, не учитывая дату создания и изменения.

По умолчанию флажок установлен.

- **Использовать технологию iChecker.**

  Проверка только новых или измененных с момента последней проверки файлов.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет только новые или изменившиеся с момента последней проверки файлы.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы, не учитывая дату создания и изменения.

  По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Использование KSN

Этот раздел содержит информацию о задаче Использование KSN и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Использование KSN

Использование Глобального KSN предполагает передачу данных, описанных в Положении о KSN, на серверы Лаборатории Касперского, и влечет к выходу программы из сертифицированного состояния.

Kaspersky Security Network (далее также "KSN") – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программ. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Industrial CyberSecurity for Nodes 2.5 на новые угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Kaspersky Industrial CyberSecurity for Nodes 2.5 получает от Kaspersky Security Network только информацию о репутации программ.

Участие пользователей в KSN позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний компонентов программы.

Более подробную информацию о передаче, обработке, хранении и уничтожении информации об использовании программы вы можете получить, прочитав Положение о KSN в окне Обработка данных задачи Использование KSN, а также ознакомившись с Политикой конфиденциальности на веб-сайте "Лаборатории Касперского".

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается после установки Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете изменить свое решение об участии в Kaspersky Security Network в любой момент.

Kaspersky Security Network может использоваться в следующих задачах Kaspersky Industrial CyberSecurity for Nodes 2.5:

- Постоянная защита файлов;
- Проверка по требованию;
- Контроль запуска программ.

Локальный Kaspersky Security Network

Подробнее о том, как настроить Kaspersky Private Security Network (далее "Локальный KSN"), см. в *Справочной системе Kaspersky Security Center*.

Если вы используете Локальный KSN на защищаемом компьютере, в окне **Обработка данных** задачи Использование KSN вы можете прочитать Положение о KPSN и включить использование компонента, установив флажок **Я принимаю условия участия в Kaspersky Private Security Network**. Принимая условия, вы соглашаетесь отправлять все типы данных, упомянутые в Положении о KPSN (запросы безопасности, статистические данные), в службы KSN.

После принятия условий Локального KSN флажки, регулирующие использование Глобального KSN, недоступны.

Если вы отключаете Локальный KSN во время работы задачи Использование KSN, происходит ошибка *Нарушение лицензии* и задача останавливается. Чтобы продолжить защищать компьютер, вам требуется принять Положение о Глобальном KSN в окне **Обработка данных** вручную и перезапустить задачу.

Отзыв согласия с Положением о KSN

Вы можете отозвать свое согласие и прекратить обмен данными с Kaspersky Security Network в любой момент. Следующие действия считаются полным или частичным отзывом согласия с Положением о KSN:

- Вы сняли флажок **Разрешить отправку данных о проверяемых файлах**: программа перестает отправлять контрольные суммы проверенных файлов в службы KSN для анализа.
- Вы сняли флажок **Разрешить отправку статистики Kaspersky Security Network**: программа прекращает обрабатывать данные с дополнительной статистикой KSN.
- Вы сняли флажок **Я принимаю условия участия в Kaspersky Security Network**: программа прекращает обрабатывать все связанные с KSN данные, задача Использование KSN останавливается.
- Вы удалили компонент Использование KSN: обработка всех связанных с KSN данных останавливается.
- Вы удалили Kaspersky Industrial CyberSecurity for Nodes 2.5: обработка всех связанных с KSN данных останавливается.

Настройка параметров задачи Использование KSN

Вы можете изменять параметры задачи Использование KSN, заданные по умолчанию (см. таблицу ниже).

Таблица 19. Параметры задачи Использование KSN по умолчанию

Параметр	Значение по умолчанию	Описание
Действия над объектами, недоверенными в KSN	Удалить	Вы можете указывать действия, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 будет выполнять над объектами, имеющими репутацию недоверенных в KSN.
Отправка данных	Контрольная сумма файла (MD5-хеш) рассчитывается для файлов, размер которых не превышает 2 МБ.	Вы можете указывать максимальный размер файлов, для которых рассчитывается контрольная сумма по алгоритму MD5 для отправки в KSN. Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 рассчитывает MD5-хеш для файлов любого размера.
Положение о KSN	Флажок **Я принимаю условия использования Kaspersky Security Network** снят.	Решите, хотите ли вы использовать KSN после установки. Вы можете изменять свое решение в любой момент.
Разрешить отправку статистики Kaspersky Security Network	Установлен (применяется, только если принято Положение о KSN)	Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимете флажок.
Разрешить отправку данных о проверяемых файлах	Установлен (применяется, только если принято Положение о KSN)	Если Положение о KSN принято, данные о файлах, которые были проверены и проанализированы с момента запуска задачи, отправляются. Снять флажок можно в любой момент.
Расписание запуска задачи	Первый запуск не определен.	Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.
Использовать Kaspersky Security Center как прокси-сервер KSN	Выбрано	По умолчанию все данные отправляются в KSN через Kaspersky Security Center.

► *Чтобы настроить параметры задачи Использование KSN, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Настройте параметры задачи:
   - В блоке **Действия над объектами, недоверенными в KSN** укажите действие, которое Kaspersky Industrial CyberSecurity for Nodes 2.5 необходимо совершить при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалить**

Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище.

Этот вариант выбран по умолчанию.

- **Фиксировать информацию в отчете**

  Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Industrial CyberSecurity for Nodes 2.5 не удаляет недоверенный объект.

- В блоке **Отправка данных**, выполните следующие действия:
  - Снимите или установите флажок **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)**.

    Флажок включает или выключает расчет контрольной суммы файлов установленного размера для отправки этой информации в службы KSN.

    Продолжительность расчета контрольной суммы зависит от размера файла.

    Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение.

    Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 рассчитывает контрольную сумму для файлов любого размера.

    По умолчанию флажок установлен.

  - Если требуется, в поле справа укажите максимальный размер файлов, для которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет рассчитывать контрольную сумму.

5. Если требуется, настройте расписание запуска задачи на закладке **Управление задачей**. Например, вы можете включить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если хотите, чтобы задача автоматически запускалась после перезагрузки компьютера.

   Программа будет запускать задачу Использование KSN по расписанию.

6. Настройте обработку данных (см. раздел "Настройка обработки данных" на стр. 104) перед запуском задачи.
7. Нажмите на кнопку **ОК**.

Изменения параметров задачи будут применены. Дата и время изменения параметров, а также информация о параметрах задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Настройка обработки данных

► *Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Обработка данных**.

Откроется окно **Обработка данных**.

4. Прочитайте Положение о Kaspersky Security Network (или Положение о Kaspersky Private Security Network, если вы используете Локальный KSN).
5. Если вы принимаете условия, упомянутые в Положении о KSN, установите флажок **Я принимаю условия использования Kaspersky Security Network**.

   Если флажок установлен, вы принимаете условия участия в Kaspersky Security Network.

   Если флажок снят, Положение о KSN не принято и задачу Использование KSN запустить нельзя. Данные в KSN не отправляются. Зависимые флажки **Разрешить отправку данных о проверяемых файлах** и **Разрешить отправку статистики Kaspersky Security Network** недоступны.

   По умолчанию флажок снят.

   Обратите внимание, что даже если вы уже приняли Положение о KSN, флажок будет автоматически снят в следующих случаях:

   - после обновления версии программы;
   - при переключении на Локальный KSN;
   - при переключении с Локального KSN на Глобальный KSN.

   Чтобы включить службы KSN, примите Положение о KSN снова.
6. Для повышения уровня защиты следующие флажки установлены по умолчанию:

   - **Разрешить отправку данных о проверяемых файлах**

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не отправляет контрольные суммы файлов в KSN.

     Обратите внимание, что запросы файловой репутации могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов KSN "Лаборатории Касперского" от DDoS-атак. В таком случае, параметры отправки запросов репутации в этом режиме определяются автоматически на основании правил и методов, разработанных экспертами "Лаборатории Касперского" и не могут быть изменены пользователем на защищаемых компьютерах. Обновления правил и методов осуществляются в ходе выполнения задачи обновления баз программы. Если ограниченный режим применяется, в статистике задачи Использование KSN отображается статус *Отправка запросов репутации в ограниченном режиме: применено "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS*.

     По умолчанию флажок установлен.

   - **Разрешить отправку статистики Kaspersky Security Network**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 отправляет дополнительную статистику, которая может содержать персональные данные. Список данных, отправляемых в качестве статистики KSN, указан в Положении о KSN. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не отправляет дополнительную статистику.

По умолчанию флажок установлен.

Если вы приняли Положение о KSN, вы не можете снять одновременно оба флажка **Разрешить отправку данных о проверяемых файлах** и **Разрешить отправку статистики Kaspersky Security Network**.

Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.

Флажки можно установить или снять, только если принято Положение о KSN.

7. Нажмите на кнопку **OK**.

Настройка передачи дополнительных данных

В Kaspersky Industrial CyberSecurity for Nodes 2.5 можно настроить отправку в "Лабораторию Касперского" следующих данных:

- контрольных сумм проверенных файлов (флажок **Разрешить отправку данных о проверяемых файлах**);
- дополнительной статистики, включая персональные данные (флажок **Разрешить отправку статистики Kaspersky Security Network**).

Подробнее о данных, отправляемых в "Лабораторию Касперского", см. в разделе "Локальная обработка данных" этого руководства.

Соответствующие флажки можно установить или снять (см. раздел "Настройка обработки данных" на стр. 104), только если установлен флажок **Я принимаю условия Kaspersky Security Network**.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 отправляет контрольные суммы файлов и дополнительную статистику после принятия Положения о KSN.

Таблица 20. Возможные состояния флажков и соответствующие условия

Состояние флажка	Условия для состояния флажка Разрешить отправку данных о проверяемых файлах	Условия для состояния флажка Разрешить отправку статистики Kaspersky Security Network
	• отправляются запросы репутации • действия с флажком доступны	• отправляется дополнительная статистика • действия с флажком доступны
	• не отправляются запросы репутации • действия с флажком недоступны	• не отправляется дополнительная статистика • действия с флажком недоступны
	• не отправляются запросы репутации • действия с флажком доступны	• не отправляется дополнительная статистика • действия с флажком доступны
	• не отправляются запросы репутации • действия с флажком недоступны	• не отправляется дополнительная статистика • действия с флажком недоступны

Статистика задачи Использование KSN

Пока выполняется задача Использование KSN, вы можете просматривать в реальном времени информацию о количестве объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обработала с момента ее запуска до текущего момента. Информация обо всех событиях, произошедших во время выполнения задачи, регистрируется в журнале выполнения задачи (см. раздел "О журналах выполнения задач" на стр. 261).

► *Чтобы просмотреть статистику задачи Использование KSN, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обработала за время работы задачи (см. таблицу ниже).

Таблица 21. Статистика задачи Использование KSN

Поле	Описание
Отправлено файловых запросов	Количество запросов о репутации файлов, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 отправил для проверки в службы KSN.
Недоверенных заключений по файлам	Количество объектов, признанных недоверенными службами KSN.

Поле	Описание
Ошибки отправки запросов	Количество запросов в KSN, во время обработки которых возникла ошибка задачи.
Пакетов статистики сформировано	Количество пакетов с данными, которые были отправлены на обработку в KSN.
Удалено объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 удалила в результате работы задачи Использование KSN.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes 2.5 сохранила в резервном хранилище.
Объектов не удалено	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой. Информация о таких объектах записывается в журнал выполнения задачи.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes 2.5 попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске. Программа не лечит и не удаляет файлы, которые не удалось поместить в резервное хранилище. Информация о таких объектах записывается в журнал выполнения задачи.
Ограниченный режим	Статус отправки запросов файловой репутации в ограниченном режиме.

Защита от эксплойтов

Этот раздел содержит инструкции по настройке параметров защиты памяти процессов от эксплуатации уязвимостей.

В этом разделе

О Защите от эксплойтов

Kaspersky Industrial CyberSecurity for Nodes 2.5 предоставляет возможность защитить память процессов от эксплойтов. Эта возможность реализована в компоненте Защита от эксплойтов. Вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

Компонент выполняет защиту памяти процессов от эксплойтов с помощью внедрения внешнего Агента защиты процессов (далее Агент) в защищаемый процесс.

Внешний Агент защиты – это динамически загружаемый модуль Kaspersky Industrial CyberSecurity for Nodes 2.5, 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, необходимо завершить данный процесс. Может потребоваться перезагрузка компьютера (например, если защищается системный процесс).

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Industrial CyberSecurity for Nodes 2.5 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.

Служба Kaspersky Security Exploit Prevention

Для максимальной эффективности компоненту Защита от эксплойтов требуется наличие службы Kaspersky Security Exploit Prevention на защищаемом компьютере. Эта служба входит в состав рекомендуемой установки совместно с компонентом Защита от эксплойтов. Во время установки службы на защищаемый компьютер создается и запускается процесс kavfswh. Он передает информацию о защищаемых процессах от компонентов Агенту защиты.

После остановки службы Kaspersky Security Exploit Prevention программа продолжает защищать процессы, которые были добавлены в список защищаемых, а также загружается в новые добавленные процессы и применяет все доступные техники защиты от эксплойтов для защиты памяти процессов.

В случае остановки службы Kaspersky Security Exploit Prevention программа не будет получать данные о событиях, происходящих с защищаемыми процессами (в том числе данные об атаках эксплойтов и о завершении процессов). Также Агент не сможет получать данные о новых параметрах защиты и о добавлении новых процессов в список защищаемых процессов.

Режимы защиты от эксплойтов

Вы можете настраивать действия по снижению рисков эксплуатации уязвимостей в защищаемых процессах, выбрав один из двух режимов:

- **Завершать скомпрометированные процессы**: применяйте данный режим, чтобы завершать процесс при попытке эксплуатации уязвимости.

При обнаружении попытки эксплуатации уязвимости в защищаемом процессе, которому присвоен уровень "критический" в операционной системе, Kaspersky Industrial CyberSecurity for Nodes 2.5 не выполняет завершение такого процесса независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

- **Только сообщать о компрометации процесса**: применяйте данный режим, чтобы получать данные о фактах эксплуатации уязвимостей в защищаемых процессах с помощью событий в журнале нарушений безопасности.

  Если выбран данный режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 регистрирует все попытки эксплуатации уязвимостей посредством создания событий.

Настройка параметров защиты памяти процессов

► *Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите узел **Kaspersky Industrial CyberSecurity for Nodes**.
2. Откройте контекстное меню и выберите пункт **Защита от эксплойтов: общие параметры защиты**.

   Откроется окно **Параметры защиты от эксплуатации уязвимостей**.
3. В блоке **Защита памяти процессов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 снижает риски эксплуатации уязвимостей процессов, находящихся в списке защищаемых процессов.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не защищает процессы на компьютере от эксплуатации уязвимостей.

     По умолчанию флажок снят.

     - **Завершать скомпрометированные процессы**

       Если выбран данный режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 завершает защищаемый процесс при обнаружении попытки эксплуатации уязвимости, к которой была применена активная техника снижения рисков.

     - **Только сообщать о компрометации процесса**

       Если выбран данный режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 сообщает о факте эксплуатации уязвимости посредством вывода терминального окна на экран. Скомпрометированный процесс продолжает выполняться.

       Если во время работы программы в режиме **Завершать скомпрометированные процессы** Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает факт эксплуатации уязвимости критического процесса, компонент принудительно переходит в режим **Только сообщать о компрометации процесса**.
4. В блоке **Профилактические действия** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов.**

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 выводит на экран терминальное окно с описанием причины срабатывания защиты и указанием на процесс, где была обнаружена попытка эксплуатации уязвимости.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет выводить на экран терминальное окно при обнаружении факта попытки эксплуатации уязвимости или завершения скомпрометированного процесса. Терминальное окно отображается независимо от статуса работы службы Kaspersky Security Exploit Prevention. По умолчанию флажок установлен.

- **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет снижать риски эксплуатации уязвимостей уже запущенных процессов независимо от статуса выполнения службы Kaspersky Security. Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет защищать процессы, которые были добавлены после остановки службы Kaspersky Security. После того как служба будет запущена, снижение рисков эксплуатации уязвимостей всех процессов будет остановлено.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не защищает процессы от эксплуатации уязвимостей при остановке службы Kaspersky Security.

  По умолчанию флажок установлен.

5. В окне **Параметры защиты от эксплойтов** нажмите на кнопку **ОК**.

   Kaspersky Industrial CyberSecurity for Nodes 2.5 сохранит и применит настроенные параметры защиты памяти процессов.

Добавление защищаемого процесса

Компонент Защита от эксплойтов защищает несколько процессов по умолчанию. Вы можете исключить какой-либо процесс из защиты, сняв флажок в соответствующей строке процесса.

► *Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:*

1. В дереве Консоли выберите узел **Kaspersky Industrial CyberSecurity for Nodes**.
2. Откройте контекстное меню и выберите пункт **Защита от эксплойтов: параметры защиты процессов**.

   Откроется окно **Параметры защиты процессов**.
3. Добавьте процесс в список защищаемых процессов, выполнив следующие действия:
   a. Нажмите на кнопку **Обзор**.

      Откроется стандартное окно Microsoft Windows **Открыть**.
   b. В открывшемся окне выберите процесс, который вы хотите добавить в список.
   c. Нажмите на кнопку **Открыть**.
   d. Нажмите на кнопку **Добавить**.

      Указанный процесс добавится в список защищаемых процессов.
4. Выберите добавленный процесс в списке.
5. На странице **Параметры защиты процесса** отображается текущая конфигурация:

- **Имя процесса**.
- **Выполняется сейчас**.
- **Применяемые техники защиты**.
- **Снижение области действия процесса (параметры техники Attack Surface Reduction)**.

6. Чтобы отредактировать применяемые к данному процессу техники защиты от эксплойтов, выберите закладку **Техники защиты**.
7. Выберите один из вариантов применения техник снижения рисков:
   - **Применять все доступные техники защиты от эксплойта**

     Если выбран этот вариант, редактирование списка недоступно, все техники применяются по умолчанию.
   - **Применять указанные техники защиты от эксплойта**

     Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.
8. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):
   - Внесите названия модулей, которые будут запрещены к запуску из защищаемого процесса в поле **Запрещать загрузку модулей**.
   - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, запуск модулей в которых вы хотите разрешить:
     - Интернет
     - Интранет
     - Доверенные сайты
     - Сайты с ограниченным доступом
     - Компьютер

     Данные параметры применимы только для Internet Explorer®.
9. Нажмите на кнопку **OK**.

Процесс будет добавлен в область защиты задачи.

Техники защиты от эксплойта

Таблица 22. Техники защиты от эксплойта

Техника защиты от эксплойтов	Описание
Data Execution Prevention (DEP)	Предотвращение выполнения данных - запрет исполнения произвольного кода в защищенной области памяти.
Address Space Layout Randomization (ASLR)	Изменение расположения структур данных в адресном пространстве процесса.
Structured Exeption Handler Overwrite Protection (SEHOP)	Подмена записи в структуре исключений или подмена обработчика исключений.
Null Page Allocation	Предотвращение переориентации нулевого указателя.
LoadLibrary Network Call Check (Anti ROP)	Защита от загрузки динамических библиотек с сетевых путей.
Executable Stack (Anti ROP)	Запрет на несанкционированное исполнение областей стека.
Anti RET Check (Anti ROP)	Проверка безопасного вызова функции через CALL инструкцию.
Anti Stack Pivoting (Anti ROP)	Защита от перемещения указателя стека ESP на эксплуатируемый адрес.
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Защита доступа на чтение таблицы экспорта адресов (Export Address Table) для модулей kernel32.dll, kernelbase.dll, ntdll.dll
Heap Spray Allocation (Heapspray)	Защита от выделения памяти под исполнение вредоносного кода.
Execution Flow Simulation (Anti Return Oriented Programming)	Обнаружение подозрительных цепочек инструкций (возможный ROP гаджет) в компоненте Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Защита от эскалации привилегий через уязвимость в драйвере AFD (выполнение произвольного кода на нулевом кольце через вызов QueryIntervalProfile.
Attack Surface Reduction (ASR)	Блокирование запуска уязвимых модулей через защищаемый процесс.
Anti Process Hollowing (Hollowing)	Защита от создания и запуска вредоносных копий доверенных процессов.
Anti AtomBombing (APC)	Защита от эксплуатации глобальных атомных таблиц через асинхронные вызовы процедур (APC)
Anti CreateLocalThread (RThreadRemote)	Сторонний процесс создал поток в защищаемом процессе
Anti CreateRemoteThread (RThreadRemote)	Защита внедрения потока защищаемого процесса в другой процесс.

Защита от шифрования

Этот раздел содержит информацию о задаче Защита от шифрования и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Защита от шифрования

Задача Защита от шифрования позволяет обнаруживать активность вредоносного шифрования сетевых файловых ресурсов защищаемого компьютера со стороны удаленных компьютеров сети.

В ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет обращения удаленных компьютеров сети к файлам, расположенным в общих сетевых папках защищаемого компьютера. Если программа расценивает действия удаленного компьютера над сетевыми файловыми ресурсами как активность вредоносного шифрования, такой компьютер вносится в список недоверенных и теряет доступ к общим сетевым папкам.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не расценивает активность шифрования как вредоносную, если обнаруженная активность шифрования ведется в каталогах, исключенных из области действия задачи Защита от шифрования.

По умолчанию программа блокирует доступ недоверенных компьютеров к сетевым файловым ресурсам на 30 минут.

Задача Защита от шифрования не позволяет блокировать доступ удаленного компьютера к сетевым файловым ресурсам до тех пор, пока активность этого компьютера не признана вредоносной. Это может занять некоторое время, в течение которого программа-шифровальщик может вести вредоносную активность.

Если задача Защита от шифрования запущена в режиме Только статистика, Kaspersky Industrial CyberSecurity for Nodes 2.5 только фиксирует попытки вредоносного шифрования с удаленных компьютеров в журнале выполнения задачи.

Статистика задачи Защита от шифрования

Если задача Защита от шифрования выполняется, вы можете просматривать в реальном времени информацию о количестве объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes обработала с момента запуска этой задачи до текущего момента, то есть статистику задачи.

► *Чтобы просмотреть статистику задачи Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обработала за время работы задачи (см. таблицу ниже).

Таблица 23. Статистика задачи Защита от шифрования

Поле	Описание
Обнаружено попыток шифрования	Количество попыток обращения к сетевому хранилищу, в которых Kaspersky Industrial CyberSecurity for Nodes 2.5 распознал активность шифрования.
Ошибок обработки	Количество обращений программ к сетевому хранилищу, во время обработки которых возникла ошибка задачи.
Обработано объектов	Общее количество обращений, которые обработала программа Kaspersky Industrial CyberSecurity for Nodes 2.5.

Настройка параметров задачи Защита от шифрования

Задача Защита от шифрования имеет следующие параметры по умолчанию:

- **Режим работы задачи**. Задача Защита от шифрования может быть запущена в режиме **Активный** или **Только статистика**. **Активный** режим применяется по умолчанию.
- **Область защиты**. По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет задачу Защита от шифрования ко всем общим сетевым папкам компьютера. Вы можете изменить область защиты, указав папки общего доступа, к которым должна применяться задача.
- **Исключения**. Укажите области, которые вы хотите исключить из области защиты задачи.
- **Эвристический анализатор**. По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет уровень детализации проверки **Средний**. Вы можете включать и выключать применение эвристического анализатора, а также регулировать уровень детализации проверки.
- **Параметры расписания**. По умолчанию первый запуск задачи не определен. Задача Защита от шифрования не запускается автоматически при старте Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. В открывшемся окне настройте следующие параметры:
   - Режим работы и использование эвристического анализатора (см. раздел "Общие параметры задачи" на стр. 116) на закладке **Общие**.
   - Область защиты (см. раздел "Формирование области защиты" на стр. 117) на закладке **Область защиты**.
   - Исключения (см.раздел "Добавление исключений" на стр. 118) на закладке **Исключения**.
   - Запуск задачи по расписанию (см. раздел "Настройка запуска задачи по расписанию" на стр. 62) на закладках **Расписание** и **Дополнительно**.
5. Нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

Общие параметры задачи

► *Чтобы настроить общие параметры задачи, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В блоке **Режим работы** укажите режим работы задачи:
   - **Только статистика**.

     Если выбран этот режим, все попытки вредоносного шифрования записываются в журнал событий задачи Защита от шифрования, и никакие действия не исключаются. Этот режим выбран по умолчанию.
   - **Активный**.

     Если выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 блокирует доступ к папкам общего доступа для скомпрометированных компьютеров при обнаружении попытки вредоносного шифрования.
5. Снимите или установите флажок **Использовать эвристический анализатор**.

   Флажок включает или выключает использование эвристического анализатора при проверке объектов.

   Если флажок установлен, эвристический анализатор включен.

   Если флажок снят, эвристический анализатор выключен.

   По умолчанию флажок установлен.
6. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни детализации проверки:

- **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
- **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

  Этот уровень выбран по умолчанию.
- **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний.

  Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

7. Нажмите на кнопку **ОК**, чтобы применить новые параметры.

Формирование области защиты

- В задаче Защита от шифрования применяются следующие типы области защиты:
- **Предустановленная**. Вы можете использовать область защиты, установленную по умолчанию и включающую в проверку все общие сетевые папки компьютера. Применяется, если выбран параметр **Все общие сетевые папки компьютера**.
- **Пользовательская**. Вы можете самостоятельно настроить область защиты, выбрав папки, которые требуется включить в область защиты от шифрования, вручную. Применяется, если выбран параметр **Только указанные папки общего доступа**.

Для настройки области защиты задачи Защита от шифрования можно использовать только локальный путь.

При использовании как предустановленной, так и пользовательской области защиты вы можете исключить выбранные папки из области защиты, например, если данные в этих папках шифруются программами, установленными на удаленных устройствах.

► *Чтобы настроить область защиты для задачи Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В блоке **Область защиты** выберите папки, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 будет проверять в ходе выполнения задачи Защита от шифрования:
   - **Все сетевые папки общего доступа на компьютере**

Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет все общие сетевые папки компьютера.

Этот вариант выбран по умолчанию.

- **Только указанные папки общего доступа**.

  Если выбран этот вариант, то в ходе выполнения задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет только те общие сетевые папки компьютера, которые вы указали вручную.

5. Чтобы указать общую папку компьютера, которую вы хотите включить в область защиты, используйте один из следующих способов:
   - Вручную:
     a. Введите имя папки общего доступа на защищаемом компьютере.
     b. Нажмите кнопку **Добавить**.

        Путь к папке будет добавлен в список.
   - Используя поиск:
     a. Нажмите на кнопку **Выбрать**.

        Откроется стандартное окно Microsoft Windows.
     b. Выберите папку, которую вы хотите добавить в область защиты задачи.
     c. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Добавление исключений

► *Чтобы настроить область защиты для задачи Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов узла **Защита от шифрования** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Исключения** установите флажок **Учитывать исключенные области защиты**.

   Если флажок установлен, то во время работы задачи Защита от шифрования Kaspersky Industrial CyberSecurity for Nodes 2.5 не обнаруживает вредоносное шифрование, осуществляющееся в указанных областях.

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает попытки шифрования на всех сетевых папках компьютера.

   По умолчанию флажок снят, список исключений пуст.
5. Укажите имя папки или маску.

6. Нажмите кнопку **Добавить**.
7. Если требуется, повторите шаги 5 и 6 для добавления дополнительных исключений.
8. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Исключения из области защиты будут добавлены и применены.

Защита промышленной сети

Этот раздел включает информацию о мониторинге проекта программируемого логического контроллера (далее "Проект ПЛК") и проверке целостности его прошивки.

В этом разделе

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 доступ по сети компьютера с установленной программой Kaspersky Industrial CyberSecurity for Nodes 2.5 к ПЛК.

► *Перед началом использования функции требуется выполнить следующие подготовительные действия:*

1. Получить информацию о проектах ПЛК с помощью локальной задачи Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 **Получение данных о проектах ПЛК**.
2. В параметрах локальной задачи Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 **Проверка целостности проектов ПЛК** указать эталонные проекты ПЛК из списка проектов, полученных на предыдущем шаге.

После запуска локальной задачи Проверка целостности проекта ПЛК программа 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 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, выполните следующие действия:*

Откройте закладку **Отчеты** и выберите **Отчет о проверке целостности программируемого логического контроллера (ПЛК)**.

Подробнее о создании отчетов см. в *Справке Kaspersky Security Center*.

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.

► *Чтобы настроить Получение данных о проектах ПЛК, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Защита промышленной сети**.
2. Выберите вложенный узел **Получение данных о проектах ПЛК**.
3. Перейдите по ссылке **Свойства** на панели результатов узла **Получение данных о проектах ПЛК**.

   Откроется окно Параметры задачи.
4. Чтобы получить информацию о проекте ПЛК, настройте следующие параметры:
   - В блоке **Общие параметры**:
     - **Тип ПЛК.**

       Раскрывающийся список доступных типов ПЛК, данные о проектах которых можно получить. Тип ПЛК представляет собой модель и серию конкретного изготовителя ПЛК.
     - **Описание.**

       Поле для ввода описания для каждого выбранного типа ПЛК. Программа привязывает заданное описание к каждой новой версии прошивки ПЛК, полученной в ходе выполнения задачи Получение данных о проектах ПЛК.
     - **Читать блоки данных.**

       Флажок включает или выключает считывание блоков данных проекта ПЛК.

       Если флажок установлен, программа 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, программа 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.

- В блоке **Параметры соединения**:
  a. Укажите **IP-адрес**, **Порт**, **Номер стойки** и **Номер слота** ПЛК.
  b. Для защиты соединения с ПЛК установите флажок **Использовать пароль** и введите пароль в поле ниже.

     Флажок включает или выключает применение пароля при подключении к ПЛК.

     Если флажок установлен, программа использует указанный пароль при подключении к ПЛК для его опроса.

     Если флажок снят, программа 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.
  c. Установите время ожидания соединения с указанным ПЛК в поле **Ожидать соединение**.

5. В окне **Конфигурация проекта ПЛК** нажмите кнопку **ОК**.
6. Повторите ввод параметров для каждого из остальных ПЛК.

   Введенные параметры отображаются в таблице **Сформированные конфигурации ПЛК**.
7. Нажмите **Удалить**, чтобы удалить выбранную конфигурацию ПЛК из списка задачи.

   Конфигурация ПЛК не удаляется из Реестра ПЛК, и ее можно добавить снова в любой момент. Подробная информация о Реестре конфигураци ПЛК содержится в *Руководстве администратора Kaspersky Industrial CyberSecurity for Nodes 2.5.*
8. В окне **Параметры задачи** нажмите кнопку **ОК**, чтобы сохранить 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

► *Чтобы настроить Проверку целостности проектов ПЛК, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Защита промышленной сети**.
2. Выберите вложенный узел **Проверка целостности проектов ПЛК**.
3. Перейдите по ссылке **Свойства** на панели результатов узла **Проверка целостности проектов ПЛК**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне настройте следующие параметры:

- На закладках **Расписание** и **Дополнительно**:
  - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 62)
- На закладке **Запуск с правами**:
  - Параметры запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 65)

5. На панели результатов узла **Проверка целостности проектов ПЛК** перейдите по ссылке **Настроить область защиты**.

   Откроется окно **Настройка области защиты**.

6. 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 ПЛК** в окне **Данные для проверки целостности проектов ПЛК** выберите тип ПЛК, целостность проекта которого вы хотите проверить.

   Раскрывающийся список доступных типов ПЛК, данные о проектах которых можно получить. Тип ПЛК представляет собой модель и серию конкретного изготовителя ПЛК.

   В списке отображаются доступные конфигурации для выбранного типа ПЛК и эталонные версии выбранного проекта ПЛК.

8. Установите значение параметра **Интервал опроса**, чтобы указать временной интервал, с которым программа должна проверять целостность проектов ПЛК.

9. В окне **Проверка целостности проектов ПЛК** нажмите кнопку **ОК**, чтобы сохранить внесенные изменения.

10. Выберите добавленную конфигурацию ПЛК из списка в окне **Параметры области защиты**.

    На закладке **Конфигурация ПЛК** отображаются параметры подключения ПЛК, указанные в параметрах задачи Получение данных о проектах ПЛК.

11. На закладке **Конфигурация ПЛК** установите или снимите флажок **Проверять текущий статус проекта ПЛК**.

    Флажок включает ПЛК в область задачи или исключает из нее.

    Если флажок снят, задача не проверяет проект ПЛК.

    Если флажок установлен, задача сравнивает текущие параметры проекта ПЛК с параметрами эталонного проекта ПЛК.

12. Выберите закладку **Настройка проверки целостности проектов ПЛК**.

    - В раскрывающемся списке содержится информация о хеше проекта ПЛК и дате, когда он был получен. Выполните следующие действия:

      a. Выберите **эталонный проект ПЛК** из списка. По результатам сравнения с параметрами эталонного проекта ПЛК программа делает вывод о целостности проекта ПЛК.

Если при добавлении конфигурации ПЛК был указан эталонный проект ПЛК, такой проект ПЛК отображается первым в списке. Остальные проекты ПЛК сортируются по дате их получения от старых к недавним.

b. Установите значение параметра **Интервал опроса ПЛК**, чтобы указать интервал времени, через который программа запрашивает информацию о параметрах проектов ПЛК.

13. Нажмите на кнопку **ОК** в окне **Настройка области защиты**.

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.

► *Чтобы включить или выключить Проверку целостности проектов ПЛК, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Защита промышленной сети**.
2. Выберите вложенный узел **Получение данных о проектах ПЛК**.
3. В блоке **Управление** на панели результатов узла **Получение данных о проектах ПЛК** перейдите по ссылке **Запустить**.
4. Выберите вложенный узел **Проверка целостности проектов ПЛК**.
5. В блоке **Управление** на 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.

Контроль компьютера

Этот раздел содержит информацию о функциональности Kaspersky Industrial CyberSecurity for Nodes 2.5, которая позволяет контролировать запуски программ, подключения флеш-накопителей и других внешних устройств по USB, а также контролировать работу брандмауэра Windows.

В этом разделе

Контроль запуска программ

Этот раздел содержит информацию о задаче Контроль запуска программ и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Контроль запуска программ

В ходе выполнения задачи Контроль запуска программ Kaspersky Industrial CyberSecurity for Nodes 2.5 отслеживает попытки запуска программ пользователями и разрешает или запрещает их запуск. Основой работы задачи Контроль запуска программ является принцип блокировки по умолчанию, который предполагает автоматическое блокирование запуска любых программ, неразрешенных в параметрах задачи.

Вы можете разрешить запуск программ одним из следующих способов:

- задать разрешающие правила для доверенных программ;
- учитывать репутацию доверенных программ в KSN при их запуске.

Запрет запуска программы имеет абсолютный приоритет: если запуск программы заблокирован одним компонентом задачи Контроль запуска программ, то запуск такой программы будет запрещен вне зависимости от заключений других компонентов задачи. Например, если программа признана недоверенной службами KSN, но подпадает под область действия разрешающего правила, запуск такой программы будет запрещен.

Все попытки запуска программ фиксируются в журнале выполнения задач (см. раздел "О журналах выполнения задач" на стр. 261).

Задача Контроль запуска программ может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует с помощью заданных правил запуск программ, которые подпадают под применение правил задачи Контроль запуска программ. Область применения правил задачи Контроль запуска программ указывается в параметрах этой задачи. Если программа подпадает под область применения правил задачи Контроль запуска программ, и ее параметры не удовлетворяют ни одному из правил контроля запуска программ, то запуск такой программы запрещен.

  Запуск программ, которые не подпадают под область применения правил, указанную в параметрах задачи Контроль запуска программ, разрешен вне зависимости от параметров правил контроля запуска программ.

  Запуск задачи **Контроль запуска программ** в режиме Активный невозможен, если не создано ни одно правило или количество созданных правил для одного компьютера превышает порог в 65 535 правил.

- **Только статистика**. Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует запуск программ с помощью правил, а только фиксирует в журнале выполнения задачи информацию о запусках программ и правилах контроля запуска программ, которым удовлетворяют запущенные программы, а также действия, которые были бы предприняты в режиме **Активный**. Запуск всех программ разрешен. Этот режим установлен по умолчанию.

  Вы можете использовать этот режим для формирования списка правил контроля запуска программ (см. раздел "Формирование списка правил по событиям задачи Контроль запуска программ" на стр. 146) на основе информации, зафиксированной в журнале выполнения задач.

Вы можете построить работу задачи Контроль запуска программ в соответствии с одним из следующих сценариев:

- Дополнительная настройка правил (см. раздел "О правилах Контроля запуска программ" на стр. 137) и их применение для контроля запуска программ.
- Базовая настройка правил и использование KSN (см. раздел "Использование KSN в задаче Контроль запуска программ" на стр. 131) для контроля запуска программ.

Если системные файлы подпадают под область применения задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что запуск таких программ разрешен созданными правилами. В противном случае операционная система может не запуститься.

Kaspersky Industrial CyberSecurity for Nodes 2.5 также перехватывает процессы, запущенные в рамках Windows Subsystem для Linux (за исключением скриптов, запущенных из оболочки UNIX® или командных интерпретаторов). Для данных целей задача Контроль запуска программ применяет действия, указанные в текущих настройках. Задача Формирование правил контроля запуска программ распознает запуск программы и создает соответствующие правила для программ, работающих в рамках Windows Subsystem для Linux.

Настройка параметров задачи Контроль запуска программ

По умолчанию задача Контроль запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 24. Параметры задачи Контроль запуска программ по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	**Только статистика**. Задача фиксирует события блокировки и запуска программ в соответствии с заданными правилами в журнале выполнения. Фактическая блокировка запуска программ не выполняется.	Вы можете выбрать режим **Активный** для защиты компьютера после того, как будет сформирован окончательный список правил.
Область применения правил	Задача контролирует запуск исполняемых файлов, скриптов и MSI-пакетов.	Вы можете указывать типы файлов, запуск которых будет контролироваться правилами.
Использование KSN	Данные о репутации программ в KSN не используются.	Вы можете использовать данные о репутации программ в KSN при работе задачи Контроль запуска программ.
Автоматически разрешать распространение для программ и пакетов из списка	Не применяется.	Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию разрешено только распространение программ с помощью службы Windows Installer.
Разрешение распространения программ через Windows Installer	Применяется.	Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются через Windows Installer.
Запретить запуск командных интерпретаторов без команд к исполнению	Не применяется.	Вы можете запрещать запуск командных интерпретаторов без исполняемых команд.
Запуск задачи	Первый запуск не определен.	Задача Контроль запуска программ не запускается автоматически при старте Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - Режим работы задачи Контроль запуска программ (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. 128).
     - Область применения правил в задаче (см. раздел "Формирование области применения задачи Контроль запуска программ" на стр. 130).
     - Использование KSN (см. раздел "Использование KSN в задаче Контроль запуска программ" на стр. 131).
   - На закладке **Контроль пакетов установки**:
     - Параметры контроля пакетов установки (см. раздел "Контроль пакетов установки" на стр. 135).
   - На закладках **Расписание** и **Дополнительно**:
     - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 62)
5. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Изменения параметров задачи будут сохранены.
6. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.
7. При необходимости измените список правил контроля запуска программ (см. раздел "О правилах контроля запуска программ" на стр. 137).

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Выбор режима работы задачи Контроль запуска программ

► *Чтобы настроить режим работы задачи Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. В раскрывающемся списке **Режим работы** выберите режим работы задачи.

   В раскрывающемся списке вы можете выбрать один из режимов работы задачи Контроль запуска программ:

   - **Активный**. Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует запуск программ с помощью заданных правил.
   - **Только статистика**. Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует запуск программ с помощью заданных правил, а только фиксирует в журнале выполнения задач информацию о запусках программ. Запуск всех программ разрешен. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации, зафиксированной в журнале выполнения задач.

   По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.

5. Снимите или установите флажок **Повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках**.

   Флажок включает или выключает контроль повторного запуска программ на основе записей кеша о прецедентах.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 запрещает или разрешает выполнение повторно запущенной программы на основе решения, которое было принято при первом запуске программы задачей контроля запуска программ. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом событии сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки на наличие разрешающих правил.

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет программу при каждом ее последующем запуске заново.

   По умолчанию флажок установлен.

   Kaspersky Industrial CyberSecurity for Nodes 2.5 заводит новый список прецедентов в кеше при каждом изменении параметров задачи Контроль запуска программ. Таким образом запуск программ контролируется в соответствии с актуальными настройками безопасности.

6. Снимите или установите флажок **Запретить запуск интерпретаторов команд при отсутствии команд**.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 запрещает запуск интерпретатора командной строки, даже если запуск интерпретатора разрешен. Запуск командной строки без команд разрешается только при выполнении обоих условий:

   - Запуск интерпретатора командной строки разрешен.
   - Выполняемая команда разрешена.

   Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает только разрешающие правила для запуска командной строки. Запуск блокируется, если не применено разрешающее правило, или выполняемый процесс не имеет статуса доверенного в KSN. Если разрешающее правило применено, или у процесса есть статус доверенного в KSN, запуск командной строки разрешается как с командой, так и без нее.

Kaspersky Industrial CyberSecurity for Nodes 2.5 работает со следующими интерпретаторами:

- cmd.exe;
- powershell.exe;
- python.exe;
- perl.exe.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Все попытки запуска программ фиксируются в журнале выполнения задач.

Формирование области применения задачи Контроль запуска программ

► *Чтобы сформировать область применения задачи Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Область применения правил** задайте следующие параметры:
   - **Использовать правила для исполняемых файлов**

     Флажок включает / выключает контроль запуска исполняемых файлов программ.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes разрешает или запрещает запуск исполняемых файлов программ с помощью заданных правил, в параметрах которых указана область применения Исполняемые файлы.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не контролирует запуск исполняемых файлов программ с помощью заданных правил. Запуск исполняемых файлов программ разрешен.

     По умолчанию флажок установлен.
   - **Контролировать загрузку DLL-модулей**

     Флажок включает/выключает контроль загрузки DLL-модулей.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает или запрещает загрузку DLL-модулей с помощью заданных правил, в параметрах которых указана область применения "Исполняемые файлы".

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена.

     Флажок доступен, если установлен флажок Использовать правила для исполняемых файлов.

     По умолчанию флажок снят.

Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**

  Флажок включает или выключает контроль запуска скриптов и пакетов MSI.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в параметрах которых указана область применения Скрипты и пакеты MSI.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен.

  По умолчанию флажок установлен.

5. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Использование KSN в задаче Контроль запуска программ

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

При использовании данных KSN о репутации программ в задаче Контроль запуска программ репутация программы в KSN является критерием разрешения или блокировки запуска этой программы. Если при попытке запуска программы Kaspersky Industrial CyberSecurity for Nodes 2.5 получает недоверенное заключение KSN, запуск такой программы запрещен. Если при попытке запуска программы Kaspersky Industrial CyberSecurity for Nodes 2.5 получает доверенное заключение KSN, запуск такой программы разрешен. Вы можете применять KSN совместно с правилами контроля запуска программ или в качестве самостоятельного критерия блокировки запуска программ.

Применение заключений KSN в качестве самостоятельного критерия блокировки запуска программ

Этот сценарий позволяет безопасно контролировать запуски программ на защищаемом компьютере без расширенной настройки списка правил.

Вы можете применить заключения KSN к Kaspersky Industrial CyberSecurity for Nodes 2.5 вместе с единственным указанным правилом. Будет разрешен запуск только тех программ, которые имеют статус доверенных в KSN, или запускать которые разрешает указанное правило.

При использовании этого сценария рекомендуется задать правило, разрешающее запуск программ по цифровому сертификату.

Все остальные программы будут блокироваться в соответствии с принципом блокировки по умолчанию. Применение KSN, при отсутствии правил, позволяет защитить компьютер от программ, которые по данным KSN представляют угрозу.

Применение заключений KSN совместно с правилами контроля запуска программ

При использовании KSN совместно с правилами контроля запуска программ действуют следующие сценарии:

- Kaspersky Industrial CyberSecurity for Nodes 2.5 всегда блокирует запуск программы, если программа подпадает под действие хотя бы одного запрещающего правила. Если такая программа признана доверенной службами KSN, это заключение имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет вам вручную расширять список нежелательных программ.
- Kaspersky Industrial CyberSecurity for Nodes 2.5 всегда блокирует запуск программы, если установлен запрет запуска программ, недоверенных в KSN, и данная программа признана недоверенной службами KSN. Если для такой программы задано разрешающее правило, оно имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет защитить компьютер от программ, которые по данным KSN представляют угрозу, но не были учтены при предварительной настройке правил.

► *Чтобы настроить использование служб KSN в задаче Контроль запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Использование KSN** задайте параметры использования служб KSN:
   - Если требуется, установите флажок **Запрещать запуск программ, недоверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 запрещает запуск программ, имеющих статус недоверенных в KSN. При этом разрешающие правила контроля запуска программ, под которые подпадают недоверенные в KSN программы, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не учитывает репутацию недоверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые подпадают программы.

     По умолчанию флажок снят.
   - Если требуется, установите флажок **Разрешать запуск программ, доверенных в KSN**.

     Флажок включает или выключает контроль запуска программ согласно их репутации в KSN.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает запуск программ, имеющих статус доверенных в KSN. При этом запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не учитывает репутацию доверенных в KSN программ и разрешает или запрещает их запуск в соответствии с правилами, под которые подпадают программы.

По умолчанию флажок снят.

- Если флажок **Разрешать запуск программ, доверенных в KSN** установлен, укажите пользователей и / или группы пользователей, которым разрешен запуск доверенных в KSN программ. Для этого выполните следующие действия:

  a. Нажмите на кнопку **Изменить**.

  Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

  b. Задайте список пользователей и / или групп пользователей.

  c. Нажмите на кнопку **ОК**.

5. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

О Контроле пакетов установки

Формирование правил контроля запуска программ может значительно усложняться, если вам требуется учитывать распространение программного обеспечения на защищаемом компьютере: например, для компьютеров, на которых выполняется периодическое автоматическое обновление установленных программ. В этом случае требуется обновлять списки разрешающих правил при каждом обновлении программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались запуски новых файлов, созданных в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения вы можете использовать соответствующую подсистему задачи Контроль запуска программ.

Подсистема Контроль пакетов установки реализована в виде дополнительного списка исключений. Вы можете добавлять в этот список *пакеты установки* (далее "доверенные пакеты") – программа будет разрешать распаковку доверенных пакетов и автоматический запуск программного обеспечения, установленного и измененного доверенным пакетом.

Учитывайте, что Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует только полный цикл распространения программного обеспечения. Программа не сможет корректно обработать запуски файлов, измененных доверенным дистрибутивом, если при первом запуске такого пакета установки контроль распространения программного обеспечения отключен, или не уставновлен компонент Контроль запуска программ.

Контроль пакетов установки невозможен, если в настройках задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

Кеш контроля пакетов установки

Kaspersky Industrial CyberSecurity for Nodes 2.5 определяет связь между файлами, созданными при распространении программного обеспечения, и доверенными пакетами с помощью динамического формирования *кеша контроля пакетов установки* (далее – "кеш распространения"). При первом запуске доверенного пакета, Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает все файлы, созданные при распространении программного обеспечения с помощью данного пакета, и сохраняет их контрольные суммы и полные пути в кеше распространения. В дальнейшем запуски всех файлов, сохраненных в кеше распространения, разрешаются автоматически.

Вы не можете просматривать, очищать, а также вручную изменять кеш распространения через пользовательский интерфейс. Kaspersky Industrial CyberSecurity for Nodes 2.5 самостоятельно наполняет его, а также контролирует его актуальность.

Вы можете экспортировать кеш распространения в конфигурационный файл (в формате XML), а также полностью очищать кеш распространения с помощью команд командной строки.

Чтобы экспортировать кеш распространения в конфигурационный файл, выполните команду:

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

Чтобы полностью очистить кеш распространения, выполните команду:

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Industrial CyberSecurity for Nodes 2.5 обновляет кеш распространения раз в сутки. Если значение полного пути или контрольной суммы ранее разрешенного файла изменены, программа удаляет запись о таком файле из кеша распространения. При активном режиме работы задачи Контроль запуска программ, дальнейшие запуски такого файла будут заблокированы.

Взаимодействие с основным списком правил контроля запуска программ

Список доверенных пакетов подсистемы 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 для таких пакетов и файлов отсутствуют правила в основном списке правил контроля запуска программ.

Использование KSN-заключений

Недоверенные KSN-заключения имеют больший приоритет, чем исключение Контроля пакетов установки: распаковка доверенного пакета установки или запуск созданных и измененных им файлов будут заблокированы, если для таких файлов получено недоверенное заключение от KSN.

Формирование списка доверенных пакетов установки

► *Чтобы добавить доверенный пакет установки, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла Контроль запуска программ перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На выбранной закладке установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью указанных в списке программ и пакетов установки.

   Если флажок установлен, программа автоматически разрешает запуск файлов, запущенных с помощью доверенных пакетов установки. Список программ и пакетов для установки, разрешенных к запуску, доступен для редактирования.

   Если флажок снят, программа не применяет указанные в списке исключения.

   По умолчанию флажок снят.

   Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если установлен флажок **Использовать правила для исполняемых файлов** в параметрах задачи **Контроль запуска программ**.
5. Если требуется, снимите флажок **Всегда разрешать распространение программ с помощью Windows Installer**.

   Флажок включает или выключает возможность автоматического создания исключений для всех файлов, запущенных с помощью подсистемы Windows Installer.

   Если флажок установлен, программа всегда разрешает запуск файлов, установленных с помощью Windows Installer.

   Если флажок снят, использование Windows Installer для запуска программы не является критерием для разрешения такой программы.

   По умолчанию флажок установлен.

   Флажок недоступен для редактирования, если снят флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Флажок **Всегда разрешать распространение программ с помощью Windows Installer** рекомендуется снимать только в случае крайней необходимости. Снятие флажка может привести к проблемам при обновлении файлов операционной системы, а также блокированию запуска файлов, дочерних по отношению к доверенным пакетам установки.
6. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

Флажок включает или выключает автоматическое разрешение распространения программного обеспечения с помощью решения System Center Configuration Manager.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически разрешает развертывание Microsoft Windows с использованием System Center Configuration Manager. Программа разрешает распространение программного обеспечения только с помощью службы фоновой интеллектуальной передачи данных (Background Intelligent Transfer Service).

Система контролирует запуск объектов со следующими расширениями:

- .exe
- .msi

По умолчанию флажок снят.

Программа контролирует цикл распространения программного обеспечения от доставки пакета на компьютер до факта установки/обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки системы на компьютере.

7. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в раскрывшемся меню выберите один из доступных способов:

- **Добавить один вручную**.

  a. Нажмите на кнопку **Обзор** и выберете файл запуска программы или пакет установки.

     Блок **Критерии доверенности** автоматически заполнится данными о выбранном файле.

  b. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

     - **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. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

     - **Использовать хеш SHA256**

       Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанным значением контрольной суммы.

       Этот вариант рекомендован для случаев, когда формирование правил обязательно для обеспечения соответствия максимальному уровню безопасности: в качестве уникального идентификатора файла может использоваться контрольная сумма SHA256. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

       Данный вариант выбран по умолчанию.

- **Добавить несколько по хешу**

Вы можете выбрать неограниченное число файлов запуска и пакетов установки и добавить их в список одновременно. Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

- **Изменить выбранный**

  Используйте этот вариант, чтобы выбрать другой файл запуска или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**.

  Вы можете импортировать список доверенных пакетов установки из сохраненного конфигурационного файла. Для распознавания в Kaspersky Industrial CyberSecurity for Nodes 2.5 файл должен удовлетворять следующим параметрам:

  - иметь текстовое расширение;
  - содержать информацию в виде списка строк, каждая из которых – данные для одного доверенного файла;
  - содержать список, соответствующий одному из двух форматов:
    - <имя файла>:<хеш SHA256>;
    - <хеш SHA256>*<имя файла>.

  В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

8. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск вложенных файлов будет разрешен.

   Чтобы запретить запуск вложенных файлов, полностью удалите программу с защищаемого компьютера или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

9. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

О правилах контроля запуска программ

По умолчанию компонент Контроль запуска программ устанавливается с двумя разрешающими правилами:

- Разрешающие правила для скриптов и MSI, имеющих доверенный сертификат в операционной системе.
- Разрешающие правила исполняемых файлов, имеющих доверенный сертификат в операционной системе.

Принцип работы правил контроля запуска программ

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.

  Правила контроля запуска программ могут разрешать или запрещать запуск программ и называются *разрешающими* или *запрещающими*, соответственно. Для создания списков разрешающих правил контроля запуска программ вы можете использовать задачу для создания разрешающих правил или режим **Только статистика** в задаче Контроль запуска программ. Вы также можете добавлять разрешающие правила вручную (см. раздел "Добавление одного правила контроля запуска программ" на стр. 143).

  > Подробнее о работе с правилами контроля запуска программ можно прочитать в разделе "О формировании правил для задачи Контроль запуск программ" в *Руководстве администратора Kaspersky Industrial CyberSecurity for Nodes 2.5*.

- Пользователь и / или группа пользователей.

  Правила контроля запуска программ контролируют запуски программ указанными в правиле пользователем и / или группой пользователей.

- Область применения правила.

  Правила контроля запуска программ могут быть применены к запускам *исполняемых файлов программ* или к запускам *скриптов* и *пакетов MSI*.

- Критерий срабатывания правила.

  Правила контроля запуска программ контролируют запуск тех файлов, которые удовлетворяют указанному в параметрах правила критерию: подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256* или расположены по указанному *пути*.

  Если в качестве критерия срабатывания правила установлен параметр **Цифровой сертификат**, созданное правило контролирует запуск любых программ, доверенных в операционной системе. Вы можете задать более строгие условия для этого критерия, установив флажки:

  - **Использовать заголовок**

    Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

    Если флажок установлен, указанный заголовок цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

    Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

    Заголовок цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

    По умолчанию флажок снят.

- **Использовать отпечаток**

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, указанный отпечаток цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

  Заголовок цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком Критерий срабатывания правила.

  По умолчанию флажок снят.

Использование отпечатка наиболее строго ограничивает срабатывания правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан, в отличие от заголовка цифрового сертификата.

Вы можете задать исключения для правила контроля запуска программ. Исключения из правила контроля запуска программ основываются на тех же критериях, по которым срабатывают правила: цифровой сертификат, хеш SHA256 или путь к файлу. Исключения из правил контроля запуска программ могут понадобиться для уточнения разрешающих правил: например, если вы хотите разрешить пользователям запуск программ по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

Если системные файлы подпадают под область применения задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что запуск таких программ разрешен созданными правилами. В противном случае операционная система может не запуститься.

Управление правилами контроля запуска программ

Вы можете выполнять следующие действия с правилами контроля запуска программ:

- Добавлять правила вручную.
- Формировать и добавлять правила автоматически.
- Удалять правила.
- Экспортировать правила в файл.
- Проверять выбранные файлы на наличие правил, разрешающих запуск этих файлов.
- Фильтровать список правил по заданному критерию.

Удаление правил контроля запуска программ

► *Чтобы удалить правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. В списке правил выберите одно или несколько правил, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить выбранные**.
6. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля запуска программ будут удалены.

Экспорт правил контроля запуска программ

► *Чтобы экспортировать правила контроля запуска программ в конфигурационный файл, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
5. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, его содержимое будет перезаписано после окончания экспорта правил.
6. Нажмите на кнопку **Сохранить**.

Параметры правила будут экспортированы в указанный файл.

Проверка запуска программ

Перед применением заданных правил контроля запуска программ вы можете проверить любую программу на срабатывание правил, чтобы определить, какие правила контролируют запуск выбранной программы.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 блокирует программы, запуск которых не контролируется ни одним правилом. Чтобы избежать блокировки запуска важных программ, вам нужно создать разрешающие правила для таких программ.

Если запуск программы контролируется несколькими правилами разных типов, приоритетными при запуске программы считаются запрещающие правила: запуск программы блокируется, если она подпадает под действие хотя бы одного запрещающего правила.

► *Чтобы протестировать правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.
4. Откроется окно **Правила контроля запуска программ**.
5. В открывшемся окне нажмите на кнопку **Показать правила для файла**.

   Откроется стандартное окно Microsoft Windows.
6. Выберите файл, контроль запуска которого хотите протестировать.

В строке поиска отобразится путь к указанному файлу. В списке правил отобразятся все найденные правила, которые будут срабатывать при запуске указанного файла.

Переход в режим разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и имеют доверенный статус в KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить режим только для скриптов или для всех исполняемых файлов.

► *Чтобы добавить правило, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите на кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
6. В поле **Название** введите название правила.
7. В раскрывающемся списке **Тип** выберите вариант **Разрешающее**.
8. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов программ.
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
9. В блоке **Критерий срабатывания правила** выберите **Путь к файлу**.
10. Введите следующую маску: **?:**

11. В окне **Параметры правила** нажмите на кнопку **OK**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет режим разрешения по умолчанию.

О наполнении списка правил контроля запуска программ

Вы можете импортировать списки правил контроля запуска программ из XML-файлов, сформированных автоматически в ходе выполнения задачи Контроль запуска программ или задачи Формирование правил контроля запуска программ. Списки, содержащиеся в таких XML-файлах, могут использоваться для создания только разрешающих правил контроля запуска программ.

Запрещающие правила контроля запуска программ создаются вручную. Также запрещаются запуски программ, для которых не найдено никаких правил.

Использование задачи Формирование правил контроля запуска программ

XML-файл, сформированный по завершении задачи Формирование правил контроля запуска программ, содержит разрешающие правила для запуска программ, указанных при настройке параметров задачи во время ее запуска. Для программ, запуск которых не разрешен в заданных параметрах задачи, не будет создано ни одного правила и их запуск будет заблокирован по умолчанию.

Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль запуска программ.

Использование отчета задачи Контроль запуска программ в режиме Только статистика

XML-файл, полученный по завершении задачи Контроль запуска программ в режиме **Только статистика**, формируется на основе журнала выполнения задачи.

В ходе выполнения задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует все запуски программ на защищаемом компьютере в журнале выполнения задачи. Вы можете сформировать разрешающие правила по событиям задачи и экспортировать их в XML-файл. Перед запуском задачи в режиме **Только статистика** вам нужно настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все возможные сценарии работы защищаемого компьютера и хотя бы одна его перезагрузка.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа запускаемых задач на защищаемом компьютере. Запуск задач автоматического формирования разрешающих правил и контроля запуска программ в режиме **Только статистика** для формирования списков правил рекомендуется выполнять на эталонной машине организации, чтобы учесть все используемые программы в сети.

Перед формированием списка разрешающих правил по программам, запущенным на эталонной машине организации, убедитесь, что на эталонной машине нет вредоносных программ.

Вы можете использовать списки правил, полученные по результатам анализа запуска программ на эталонной машине, при настройке политики в Kaspersky Security Center и применении созданных разрешающих правил для всей сети.

Добавление одного правила контроля запуска программ

► *Чтобы добавить правило контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В нижней части панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите на кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется контекстное окно **Параметры правила**.
6. Укажите следующие параметры:
   a. В поле **Название** введите название правила.
   b. В раскрывающемся списке **Тип** выберите тип правила:
      - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
      - **Запрещающее**, если вы хотите, чтобы правило запрещало запуск программ в соответствии с критериями, указанными в параметрах правила.
   c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:
      - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов программ.
      - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
   d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:
      i. Нажмите на кнопку **Выбрать**.
      ii. Откроется стандартное окно Microsoft Windows **Выбор пользователя или групп**.
      iii. Задайте список пользователей и / или групп пользователей.
      iv. Нажмите на кнопку **OK**.
   e. Выполните следующие действия, если вы хотите взять значения для критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла:
      i. Нажмите на кнопку **Задать критерий срабатывания файла из свойств файла**.

         Откроется стандартное окно Microsoft Windows **Открыть**.
      ii. Выберите файл и нажмите на кнопку **OK**.

         Значения критериев из файла отобразятся в полях блока Критерий срабатывания правила. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.

f. В блоке **Критерий срабатывания правила** выберите один из следующих вариантов:

- **Цифровой сертификат**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, подписанных цифровым сертификатом:
  - Установите флажок **Использовать заголовок**, если хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
  - Установите флажок **Использовать отпечаток**, если хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным отпечатком.
- **Хеш SHA256**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если хотите, чтобы правило контролировало запуск программ, запускаемых с помощью файлов, расположенных по указанному пути.

> Kaspersky Industrial CyberSecurity for Nodes 2.5 не распознает путь, включающий наклонную черту "/". Используйте обратную наклонную черту "\", чтобы правильно ввести путь.

g. Выполните следующие действия, если хотите добавить исключения из правила:

i. В блоке **Исключения из правила** нажмите на кнопку **Добавить**.

Откроется окно **Исключение из правила**.

ii. В поле **Название** введите название исключения из правила.

iii. Укажите параметры исключения файлов запуска программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

- **Цифровой сертификат**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается наличие цифрового сертификата. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

  - **Использовать заголовок**

    Флажок включает или выключает использование заголовка цифрового сертификата в качестве критерия срабатывания правила.

    Если флажок установлен, указанный заголовок цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ только для указанного в заголовке поставщика.

    Если флажок снят, программа не использует заголовок цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

Заголовок цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком **Критерий срабатывания правила**.

По умолчанию флажок снят.

- **Использовать отпечаток**

  Флажок включает или выключает использование отпечатка цифрового сертификата в качестве критерия срабатывания правила.

  Если флажок установлен, указанный отпечаток цифрового сертификата используется в качестве критерия срабатывания правила. Созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с указанным отпечатком.

  Если флажок снят, программа не использует отпечаток цифрового сертификата в качестве критерия срабатывания правила. Если выбран критерий **Цифровой сертификат**, созданное правило будет контролировать запуск программ, подписанных цифровым сертификатом с любым заголовком.

  Заголовок цифрового сертификата, которым подписан файл, вы можете указать только из свойств выбранного файла с помощью кнопки **Задать критерий срабатывания правила из свойств файла**, расположенной над блоком Критерий срабатывания правила.

  По умолчанию флажок снят.

- **Хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанным значением контрольной суммы.

  Этот вариант рекомендован для случаев, когда формирование правил обязательно для обеспечения соответствия максимальному уровню безопасности: в качестве уникального идентификатора файла может использоваться контрольная сумма SHA256. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

  Данный вариант выбран по умолчанию.

- **Путь к файлу**

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет использовать полный путь к файлу для определения статуса доверенности процесса.

  Если флажок не установлен, путь к файлу не будет учитываться в качестве критерия для определения статуса доверенности процесса.

  По умолчанию флажок установлен.

iv. Нажмите на кнопку **OK**.

v. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

7. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Формирование списка правил по событиям задачи Контроль запуска программ

► *Чтобы создать конфигурационный файл со списком правил контроля запуска программ, сформированным по событиям задачи Контроль запуска программ, выполните следующие действия:*

1. Запустите задачу Контроль запуска программ в режиме **Только статистика** (см. раздел "Выбор режима работы задачи Контроль запуска программ" на стр. 128), чтобы зафиксировать в журнале выполнения задачи все срабатывания правил на запуски программ на защищаемом компьютере.
2. По завершении выполнения задачи в режиме **Только статистика**, откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** панели результатов узла **Контроль запуска программ**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 создаст конфигурационный файл в формате XML со списком правил, сформированных по работе задачи Контроль запуска программ в режиме **Только статистика**. Вы можете применить этот список правил (см. раздел "Импорт правил контроля запуска программ из XML-файла" на стр. 146) в задаче Контроль запуска программ.

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть, а затем вручную обработать список правил, чтобы убедиться, что запуск критичных для работы компьютера программ (например, файлов операционной системы) разрешен заданными правилами.

Все события работы задачи фиксируются в журнале в ходе выполнения задачи в любом из двух режимов. Вы можете создать конфигурационный файл со списком правил по событиям задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется формировать списки правил до запуска задачи в режиме применения правил контроля запуска программ.

Импорт правил контроля запуска программ из файла формата XML

► *Чтобы импортировать правила контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Нажмите на кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Импортировать правила из файла формата XML**.
6. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла формата XML**:
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

- **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
- **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

Откроется стандартное окно Microsoft Windows **Открыть**.

7. В окне Microsoft Windows **Открыть** выберите XML-файл, который содержит параметры правил контроля запуска программ.
8. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля запуска программ**.

О задаче Формирование правил контроля запуска программ

Задача Формирование правил контроля запуска программ позволяет автоматически формировать список разрешающих правил контроля запуска программ на основе указанных типов файлов из указанных папок. Например, если вы укажете в качестве параметров задачи исполняемые файлы из папки C:\Program Files (x86), программа будет автоматически формировать правила, по которым разрешается запуск этих файлов. В дальнейшем программа будет разрешать запуск программ, для которых были автоматически сформированы разрешающие правила.

Сформированные правила отображаются по ссылке **Правила контроля запуска программ** в узле **Контроль запуска программ**.

Настройка параметров задачи Формирование правил контроля запуска программ

По умолчанию задача Формирование правил контроля запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 25. Параметры задачи Формирование правил контроля запуска программ

по умолчанию

Параметр	Значение по умолчанию	Описание
Префикс для названий разрешающих правил	Совпадает с именем компьютера, на котором установлена программа Kaspersky Industrial CyberSecurity for Nodes 2.5.	Вы можете изменить префикс для названий разрешающих правил.
Область применения разрешающих правил	Под область применения разрешающих правил по умолчанию подпадают следующие категории файлов: • файлы с расширением EXE, расположенные в папках C:\Windows, C:\Program Files (x86) и C:\Program Files; • пакеты MSI, расположенные в папке C:\Windows; • скрипты, расположенные в папке C:\Windows. Также задача создает правила для всех уже запущенных программ независимо от их расположения и формата.	Вы можете изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых разрешен автоматически сформированными правилами. Также при создании разрешающих правил вы можете не учитывать запущенные программы.
Критерии формирования разрешающих правил	Используется заголовок и отпечаток цифрового сертификата; правила формируются для всех пользователей и групп пользователей.	Вы можете использовать хеш SHA256 при формировании разрешающих правил. Вы можете выбрать пользователя и группу пользователей, для которых необходимо автоматически формировать разрешающие правила.
Действия по завершении задачи	Разрешающие правила добавляются в список правил задачи Контроль запуска программ; новые правила объединяются с существующими правилами; дублирующие правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующих правил или заменять существующие правила новыми разрешающими правилами, а также настроить параметры экспорта разрешающих правил в файл.
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете разрешить запуск задачи автоматического формирования разрешающих правил с правами системной учетной записи или с правами указанного пользователя.
Расписание запуска задачи	Первый запуск не определен.	Задача Формирование правил контроля запуска программ не запускается автоматически сразу после Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне настройте следующие параметры:
   - На закладке **Общие**:
     - Укажите префикс для названий правил.

       Первая часть названия правила. Вторая часть названия правила формируется из названия объекта, запуск которого разрешен.

       По умолчанию в качестве префикса указано имя компьютера, на котором установлен Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете изменить префикс для названий разрешающих правил.
     - Настройте область применения разрешающих правил (см. раздел "Ограничение области действия задачи" на стр. 150).
   - На закладке **Действия** укажите действия, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 должна выполнять:
     - При формировании правил (см. раздел "Действия при автоматическом формировании правил контроля запуска программ" на стр. 151).
     - По завершении задачи (см. раздел "Действия по завершении автоматического формирования правил контроля запуска программ" на стр. 152).
   - На закладках **Расписание** и **Дополнительно**:
     - Запуск задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 62).
   - На закладке **Запуск с правами**:
     - Параметры запуска задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 65)
5. Нажмите на кнопку **OK**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

В этом разделе

Ограничение области действия задачи

► *Чтобы ограничить область применения задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Настройте следующие параметры задачи:
   - **Создавать разрешающие правила на основе запущенных программ**

     Флажок включает или выключает автоматическое формирование разрешающих правил контроля запуска программ для уже запущенных программ. Этот вариант рекомендуется, если на компьютере запущен эталонный набор программ, по которому вы хотите построить разрешающие правила.

     Если флажок установлен, разрешающие правила контроля запуска программ формируются в соответствии с запущенными программами.

     Если флажок снят, запущенные программы не учитываются при формировании разрешающих правил.

     По умолчанию флажок установлен.

     Флажок не может быть снят, если не выбрана ни одна папка в таблице Создавать разрешающие правила для программ из папок.
   - **Создавать разрешающие правила для программ из папок**

     В таблице вы можете выбрать или указать области сканирования задачи и типы исполняемых файлов, которые будут учитываются при формировании правил контроля запуска программ. Задача будут формировать разрешающие правила для файлов выбранных типов, расположенных в указанных папках.
5. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил контроля запуска программ

► *Чтобы настроить действия, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 должна выполнять во время работы задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Откройте закладку **Действия**.
5. В блоке **При формировании разрешающих правил** настройте следующие параметры:

   - **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. В дальнейшем программа будет разрешать запуск программ с помощью файлов, у которых есть цифровой сертификат. Этот вариант рекомендуется, если вы хотите разрешать запуск любых программ, доверенных в операционной системе.

   - **Использовать заголовок и отпечаток цифрового сертификата**

     Флажок включает или выключает использование заголовка и отпечатка цифрового сертификата файла в качестве критерия срабатывания разрешающих правил контроля запуска программ. Включение этого флажка позволяет задать более строгие условия проверки цифрового сертификата.

     Если флажок установлен, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливаются значения заголовка и отпечатка цифрового сертификата файлов, для которых формируются правила. В дальнейшем программа будет разрешать запуск программ, которые запускаются с помощью файлов с указанными в правиле заголовком и отпечатком цифрового сертификата.

     Использование этого флажка наиболее строго ограничивает срабатывание разрешающих правил запуска программ по цифровому сертификату, так как отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан.

     Если флажок снят, то в качестве критерия срабатывания разрешающих правил контроля запуска программ устанавливается наличие любого цифрового сертификата, доверенного в операционной системе.

     Флажок доступен, если выбран вариант **Использовать цифровой сертификат**.

     По умолчанию флажок установлен.

   - **Если сертификат отсутствует**

Раскрывающийся список, позволяющий выбрать критерий срабатывания разрешающих правил контроля запуска программ для случая, если файл, на основе которого формируется правило, не имеет цифрового сертификата.

- **Хеш SHA256**. В качестве критерия разрешающего правила контроля запуска программ устанавливается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
- **Путь к файлу**. В качестве критерия разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице Создавать разрешающие правила для программ из папок.

- **Использовать хеш SHA256**

  Если выбран этот вариант, то в параметрах формируемых разрешающих правил контроля запуска программ в качестве критерия срабатывания правила указывается значение контрольной суммы файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанным значением контрольной суммы.

  Этот вариант рекомендован для случаев, когда формирование правил обязательно для обеспечения соответствия максимальному уровню безопасности: в качестве уникального идентификатора файла может использоваться контрольная сумма SHA256. Использование полученного значения хеша в качестве критерия срабатывания правила сужает область применения правила до одного файла.

  Данный вариант выбран по умолчанию.

- **Создавать правила для пользователя или группы пользователей**

  Поле, в котором отображаются пользователь и / или группа пользователей. Программа будет контролировать запуски программ указанным пользователем и / или группой.

  По умолчанию выбрана группа **Все**.

6. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил контроля запуска программ

► *Чтобы настроить действия, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 должна выполнять по завершении задачи Формирование правил контроля запуска программ, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. Откройте закладку **Действия**.
5. В блоке **По завершении задачи** настройте следующие параметры:

- **Добавлять разрешающие правила в список правил контроля запуска программ**.

  Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается по ссылке Правила контроля запуска программ в панели результатов узла Контроль запуска программ.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно установленному принципу добавления.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не добавляет сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

  По умолчанию флажок установлен.

  Флажок не может быть снят, если не установлен флажок **Экспортировать разрешающие правила в файл**.

- **Принцип добавления**.

  Раскрывающийся список, позволяющий указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

  - **Добавлять к существующим правилам**. Правила дополняют список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
  - **Объединять с существующими правилами**. Правила дополняют список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию установлен способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.

  Флажок включает или выключает экспорт сформированных разрешающих правил контроля запуска программ в файл.

  Если флажок установлен, по завершении задачи автоматического формирования разрешающих правил Kaspersky Industrial CyberSecurity for Nodes экспортирует сформированные правила в файл, указанный в поле ниже.

  Если флажок снят, по завершении задачи автоматического формирования разрешающих правил Kaspersky Industrial CyberSecurity for Nodes не экспортирует сформированные правила в файл, а только добавляет их в список правил контроля запуска программ.

  По умолчанию флажок снят.

  Флажок не может быть снят, если не установлен флажок **Добавлять разрешающие правила в список правил контроля запуска программ.**

- **Добавлять информацию о компьютере в имя файла**.

Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются сформированные правила контроля запуска программ.

Если флажок установлен, программа добавляет имя защищаемого компьютера, дату и время формирования файла в имя файла экспорта.

Если флажок снят, программа не добавляет информацию о защищаемом компьютере в имя файла экспорта.

Флажок доступен, если установлен флажок **Экспортировать разрешающие правила в файл**.

По умолчанию флажок установлен.

6. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Контроль устройств

Этот раздел содержит информацию о задаче Контроль устройств и инструкции по настройке ее параметров.

В этом разделе

О задаче Контроль устройств

Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует регистрацию и использование запоминающих устройств и устройств чтения CD/DVD-дисков в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемым флеш-накопителем или внешним устройством другого типа. Запоминающее устройство - это внешнее устройство, предназначенное для записи и хранения данных.

Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует подключение следующих типов внешних устройств:

- USB-подключаемые флеш-накопители;
- устройства чтения компакт-дисков;

- USB-подключаемые устройства чтения гибких дисков;
- USB-подключаемые мобильные устройства MTP.

Kaspersky Industrial CyberSecurity for Nodes 2.5 сообщает обо всех устройствах, подключенных по USB, с помощью соответствующего события в журнале событий и в журнале выполнения задачи. Описание события включает тип устройства и путь подключения При запуске задачи Контроль устройств Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет и перечисляет все устройства, подключенные по USB. Уведомления можно настроить в блоке параметров уведомлений Kaspersky Security Center.

Задача Контроль устройств отслеживает попытки подключения внешних устройств к защищаемому компьютеру и блокирует их подключение, если не находит разрешающих правил для этих устройств. После блокировки соединения устройство становится недоступно.

Программа присваивает каждому подключаемому внешнему устройству один из двух статусов:

- *Доверенное*. Устройство, обмен данными с которым разрешен. Путь к экземпляру такого устройства подпадает под область применения хотя бы одного разрешающего правила.
- *Недоверенное*. Устройство, обмен данными с которым запрещен. Путь к экземпляру такого устройства не подпадает под область определения разрешающих правил.

Вы можете создать разрешающие правила для внешних устройств, обмен данными с которыми вы хотите разрешить, с помощью задачи Формирование правил контроля устройств. Вы также можете расширять область применения уже созданных разрешающих правил. Вы не можете создавать разрешающие правила вручную.

Kaspersky Industrial CyberSecurity for Nodes 2.5 идентифицирует регистрируемое в системе внешнее устройство по значению *пути к экземпляру устройства*. Путь к экземпляру устройства является уникальным признаком для каждого устройства. Информация о пути к экземпляру устройства содержится в свойствах внешнего устройства в операционной системе Windows и определяется Kaspersky Industrial CyberSecurity for Nodes 2.5 в момент создания разрешающих правил автоматически.

Задача Контроль устройств может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом блокировки по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

  Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому компьютеру в момент запуска задачи Контроль устройств в режиме **Активный**, то такое устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить компьютер. В ином случае принцип блокирования по умолчанию не будет применен к устройству.

- **Только статистика**. Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом компьютере, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

Вы можете использовать этот режим для формирования списка правил контроля устройств на основе информации, зафиксированной в журнале выполнения задачи (см. раздел "Формирование списка правил по событиям задачи Контроль устройств" на стр. 164).

Настройка параметров задачи Контроль устройств

По умолчанию задача Контроль устройств имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 26. Параметры задачи Контроль устройств по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	**Только статистика**	Задача фиксирует в журнале выполнения события запрета и разрешения подключения внешних устройств в соответствии с заданными правилами. Фактическая блокировка использования внешних устройств не выполняется. Вы можете выбрать режим **Активный** для защиты компьютера, чтобы применять фактическую блокировку использования внешних устройств.
Разрешать использование всех накопителей, если задача Контроль устройств не выполняется	Не применяется	Kaspersky Industrial CyberSecurity for Nodes 2.5 запрещает использование внешних устройств вне зависимости от статуса выполнения задачи Контроль устройств. Это обеспечивает максимальную защиту от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами. Вы можете настраивать параметр таким образом, чтобы Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешал использование всех внешних устройств, если задача Контроль устройств не выполняется.
Расписание запуска задачи	При запуске программы	Задача Контроль устройств запускается автоматически сразу после Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** укажите режим работы задачи:
     - **Активный**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом блокировки по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому компьютеру в момент запуска задачи Контроль устройств в режиме Активный, то такое устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить компьютер. В ином случае принцип блокирования по умолчанию не будет применен к устройству.

- **Только статистика**.

  Kaspersky Industrial CyberSecurity for Nodes 2.5 не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом компьютере, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

- Снимите или установите флажок **Разрешать использование всех внешних устройств, если задача Контроль устройств не выполняется**.

  Флажок разрешает или запрещает использование запоминающих устройств при остановленной задаче Контроль устройств.

  Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает использовать любые запоминающие устройства на защищаемом компьютере.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes запрещает использовать недоверенные запоминающие устройства на защищаемом компьютере, если задача Контроль устройств не выполняется или если служба Kaspersky Security остановлена. Рекомендуется применять этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами.

  По умолчанию флажок снят.

5. Если требуется, на закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 62).
6. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Изменения параметров задачи будут сохранены.
7. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.
8. При необходимости измените список правил контроля устройств (см. раздел "О формировании списка правил контроля устройств" на стр. 162).

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

О правилах контроля устройств

Правила создаются индивидуально для каждого устройства, подключенного в данный момент или подключавшегося ранее к защищаемому компьютеру, если данные об этом устройстве сохранились в системе.

Для создания разрешающих правил контроля устройств вы можете:

- использовать задачу Формирование правил контроля устройств (см. раздел "О задаче Формирование правил контроля устройств" на стр. 165);
- использовать режим Только статистика в задаче Контроль устройств (см. раздел "Формирование списка правил по событиям задачи Контроль устройств" на стр. 164);
- использовать данные системы о подключавшихся устройствах (см. раздел "Добавление разрешающего правила для одного или нескольких внешних устройств" на стр. 163);
- расширять область применения уже созданных правил (см. раздел "Расширение области применения правил контроля устройств" на стр. 161).

Максимальное количество правил контроля устройств, которое поддерживает Kaspersky Industrial CyberSecurity for Nodes 2.5, составляет - 3072.

Правила контроля устройств содержат следующие параметры:

- Тип правила
- область применения правила;
- Данные исходного устройства
- Описание

Тип правила

Тип правила - всегда *разрешающее*. Задача контроля устройств по умолчанию блокирует подключение всех флеш-накопителей и других внешних устройств, если они не подпадают под область действия ни одного разрешающего правила.

Критерий срабатывания и область применения правила

Правила контроля устройств идентифицируют подключаемые флеш-накопители и другие внешние устройства по значению *пути к экземпляру устройства (Device Instance Path)*. Путь к экземпляру устройства является уникальным идентификатором, который присваивается устройству системой в момент его подключения и регистрации в качестве запоминающего устройства (Mass Storage) или устройства чтения CD/DVD дисков (например, IDE или SCSI).

Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует подключение внешних устройств чтения CD/DVD дисков вне зависимости от шины подключения. При монтировании таких устройств по USB, операционная система регистрирует два значения пути к экземпляру устройства: для запоминающего устройства (Mass Storage), а также для устройства CD/DVD (например, IDE или SCSI). Для корректного подключения таких устройств требуется наличие разрешающих правил для каждого значения пути к экземпляру устройства.

Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически определяет путь к экземпляру устройства и разбивает найденное значение на следующие составляющие:

- производитель устройства (VID);
- тип контроллера устройства (PID);
- серийный номер устройства.

Вы не можете задавать путь к экземпляру устройства вручную. Заданные в свойствах разрешающего правила критерии срабатывания правила определяют область применения этого правила. По умолчанию в область применения только что созданного разрешающего правила включено одно устройство, на основе свойств которого Kaspersky Industrial CyberSecurity for Nodes 2.5 сформировал разрешающее правило. Вы можете изменять указанные значения с помощью маски в свойствах созданного правила, чтобы расширить область применения правила (см. раздел "Расширение области применения правил контроля устройств" на стр. 161).

Данные исходного устройства

Данные устройства, на основе которых программа Kaspersky Industrial CyberSecurity for Nodes 2.5 сформировала разрешающее правило, отображаются в свойствах каждого правила.

Данные исходного устройства содержат следующую информацию:

- **Пусть к экземпляру устройства**. На основании этого свойства Kaspersky Industrial CyberSecurity for Nodes 2.5 определяет критерий срабатывания правила и заполняет следующие поля: **Производитель (VID)**, **Тип контроллера (PID)**, **Серийный номер** в блоке **Область применения правила** окна **Параметры правила**.
- **Адаптированное имя**. Имя, которое задается в свойствах устройства производителем.

При создании правила Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически определяет исходные значения для устройства. В дальнейшем вы можете использовать эти значения, чтобы определить, на основе данных какого устройства было создано правило. Данные исходного устройства недоступны для редактирования.

Описание

Вы можете добавить дополнительную информацию для каждого созданного разрешающего правила контроля устройств в поле **Комментарий**, например, название подключаемого флеш-накопителя или имя его владельца. Комментарий отображается в соответствующей графе таблицы в окне **Правила контроля устройств**.

Комментарий и данные исходного устройства не учитываются при работе правила и служат только для упрощения идентификации устройств и правил пользователем.

Удаление правил контроля устройств

► *Чтобы удалить правила контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.

3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.

4. В списке правил выберите одно или несколько правил, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить выбранные**.
6. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля устройств будут удалены.

Экспорт правил контроля устройств

► *Чтобы экспортировать правила контроля устройств в конфигурационный файл, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.

4. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.

5. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, его содержимое будет перезаписано после окончания экспорта правил.
6. Нажмите на кнопку **Сохранить**.

Правила и их параметры будут экспортированы в указанный файл.

Активация и выключение правила контроля устройств

Вы можете включать и выключать применение созданных разрешающих правил контроля устройств, не удаляя их.

► *Чтобы активировать или выключить созданное правило контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.

4. В списке заданных правил откройте окно **Параметры правила** двойным щелчком мыши на правиле, параметры которого хотите настроить.
5. В открывшемся окне снимите или установите флажок **Применять правило**.

   Флажок включает или выключает применение конкретного правила контроля устройств.

Если флажок установлен в параметрах правила, такое правило будет применяться. Подключение внешних устройств, подпадающих под область применения этого правила, будет разрешено.

Если флажок снят в параметрах правила, такое правило не будет применяться. Подключение внешних устройств, подпадающих под область применения этого правила, будет запрещено.

По умолчанию флажок установлен в параметрах каждого созданного правила.

6. Нажмите на кнопку **OK**.

Статус применения правила будет сохранен и отобразится для указанного правила.

Расширение области применения правил контроля устройств

Каждое автоматически созданное правило контроля устройств разрешает подключение только одного внешнего устройства. Вы можете вручную расширить область применения правила, применив маску пути к экземпляру устройства в свойствах любого заданного правила контроля устройств.

Применение маски пути к экземпляру устройства уменьшает количество разрешающих правил контроля устройств и упрощает процесс их обработки вручную. Однако расширение области применения правил может снижать эффективность контроля запоминающих устройств.

► *Чтобы применить маску пути к экземпляру устройства в свойствах разрешающего правила контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.
4. В открывшемся окне выберите правило, на основе свойств которого вы хотите применить маску пути к экземпляру устройства.
5. Откройте окно **Параметры правила** двойным щелчком мыши на выбранном правиле контроля устройств.
6. В открывшемся окне выполните следующие действия:
   - Установите флажок **Использовать маску** рядом с полем **Тип контроллера (PID)**, если хотите, чтобы редактируемое правило разрешало подключение всех устройств по указанным данным о производителе и типе устройства.
   - Установите флажок **Использовать маску** рядом с полем **Серийный номер**, если хотите, чтобы редактируемое правило разрешало подключение всех устройств по указанным данным о производителе и серийном номере устройства.
   - Установите флажки **Использовать маску** рядом с полями **Тип контроллера (PID)** и **Серийный номер**, если хотите, чтобы редактируемое правило разрешало подключение всех устройств по указанным данным о производителе устройства.

Если хотя бы в одном поле установлен флажок **Использовать маску**, данные в полях, в которых этот флажок не установлен, заменяются символом * и не будут учитываться при срабатывании правила.

7. Если требуется, введите дополнительную информацию о правиле в поле **Комментарий**. Например, уточните, на какие устройства должно распространяться правило.
8. Нажмите на кнопку **OK**.

Настроенные параметры правила будут сохранены. Область применения правила будет расширена в соответствии с указанной маской пути к экземпляру устройства.

О наполнении списка правил контроля устройств

Вы можете импортировать списки разрешающихправил контроля устройств из XML-файлов, сформированных автоматически в ходе выполнения задачи Контроль устройств или задачи Формирование правил контроля устройств.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 запрещает подключение любых флеш-накопителей и других внешних устройств, которые не подпадают под действие указанных разрешающих правил контроля устройств.

Таблица 27. Цели и сценарии формирования списков правил контроля устройств

Сценарий формирования списка правил	Решаемая задача
Задача Формирование правил контроля устройств	• Нужно создать разрешающие правила для уже использовавшихся доверенных устройств перед первым запуском задачи Контроль устройств. • Нужно сформировать список правил для доверенных устройств в сети защищаемых компьютеров.
Сформировать правила на основе данных системы	Нужно добавить разрешающие правила для одного или нескольких новых подключенных устройств.
Режим **Только статистика** задачи Контроль устройств	Добавить разрешающие правила для большого количества новых доверенных устройств.

Использование задачи Формирование правил контроля устройств

XML-файл, сформированный по завершении задачи Формирование правил контроля устройств, содержит разрешающие правила для флеш-накопителей и других внешних устройств, данные о подключении которых сохранились в системе.

В ходе выполнения задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 получает данные системы обо всех внешних устройствах, подключавшихся ранее и подключенных к защищаемому компьютеру в данный момент, и создает на основе этих данных список разрешающих правил для обнаруженных устройств. По завершении задачи программа формирует XML-файл в папке по пути, указанному в параметрах задачи. Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль устройств.

Рекомендуется использовать этот сценарий для формирования списка разрешающих правил перед первым запуском задачи Контроль устройств, чтобы созданные разрешающие правила учитывали все внешние устройства, используемые на защищаемом компьютере.

Использование данных системы обо всех подключаемых устройствах

В ходе выполнения задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 получает данные системы обо всех внешних устройствах, подключавшихся ранее и подключенных к защищаемому компьютеру в данный момент, и отображает найденные устройства в списке обнаруженных устройств в окне **Сформировать правила на основе данных системы**.

Для каждого обнаруженного устройства Kaspersky Industrial CyberSecurity for Nodes 2.5 определяет производителя (VID), тип контроллера (PID), адаптированное имя, серийный номер и путь к экземпляру устройства. Вы можете сформировать разрешающие правила для любого устройства, данные о котором были найдены, и сразу добавить новые правила в список заданных правил контроля устройств.

Рекомендуется использовать этот сценарий для обновления списка правил, если нужно разрешить использование небольшого количества новых запоминающих устройств.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать запрещающие правила для MTP-подключаемых мобильных устройств.

Использование отчета задачи Контроль устройств в режиме Только статистика

XML-файл, полученный по завершении задачи Контроль устройств в режиме **Только статистика**, формируется на основе журнала выполнения задачи.

В ходе выполнения задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует все подключения флеш-накопителей и других запоминающих устройств к защищаемому компьютеру в журнале выполнения задачи. Вы можете сформировать разрешающие правила по событиям задачи и экспортировать их в XML-файл. Перед запуском задачи в режиме **Только статистика** рекомендуется настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все возможные подключения внешних устройств к защищаемому компьютеру.

Рекомендуется использовать этот сценарий для обновления существующего списка правил, если нужно разрешить использование большого количества новых внешних устройств.

Если формирование списка правил по этому сценарию выполняется на эталонной машине, вы можете применить сформированный список разрешающих правил при настройке политики Контроль устройств в Kaspersky Security Center. Таким образом вы сможете разрешать использование внешних устройств, подключенных к эталонной машине, на всех компьютерах защищаемой сети.

Добавление разрешающего правила для одного или нескольких внешних устройств

В задаче контроля устройств не предусмотрена функция добавления одного правила вручную. Однако в случае, если вам необходимо добавить разрешающие правила для одного или нескольких новых внешних устройств, вы можете использовать опцию **Сформировать правила на основе данных системы**. При использовании этого сценария наполнения списка правил программа использует данные Windows о всех подключениях внешних устройств, когда-либо регистрировавшихся в системе, а также учитывает внешние устройства, подключенные в текущий момент.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать запрещающие правила для MTP-подключаемых мобильных устройств.

► *Чтобы добавить разрешающее правило для одного или нескольких внешних устройств, подключенных в данный момент, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.
4. Нажмите на кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Сформировать правила на основе данных системы**.
6. В открывшемся окне в списке обнаруженных устройств выберите устройство или несколько устройств, использование которых вы хотите разрешить на защищаемом компьютере.
7. Нажмите на кнопку **Добавить правила для выбранных устройств**.

Новые правила будут добавлены в список правил контроля устройств.

Формирование списка правил по событиям задачи Контроль устройств

► *Чтобы создать конфигурационный файл со списком правил контроля устройств, сформированным по событиям задачи Контроль устройств, выполните следующие действия:*

1. Запустите задачу Контроль устройств в режиме **Только статистика (см. раздел "Настройка параметров задачи Контроль устройств" на стр.** 156**),** чтобы зафиксировать в журнале выполнения задачи все события, сформированные по подключениям флеш-накопителей и других внешних устройств к защищаемому компьютеру.
2. По завершении выполнения задачи в режиме **Только статистика** откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке Управление панели результатов узла **Контроль устройств**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 создаст конфигурационный файл в формате XML со списком правил, сформированных по результатам работы задачи Контроль устройств в режиме **Только статистика**. Вы можете применить этот список в задаче Контроль устройств (см. раздел "Импорт правил контроля устройств из файла формата XML" на стр. 165).

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть, а затем вручную обработать список правил, чтобы убедиться, что подключение недоверенных устройств не разрешено заданными правилами.

При конвертации XML-файла с событиями выполнения задачи в список правил контроля устройств, программа создает разрешающие правила для всех зафиксированных событий, в том числе для событий блокирования устройств.

Все события работы задачи фиксируются в журнале в ходе выполнения задачи в любом из двух режимов. Вы можете создать конфигурационный файл со списком правил по результатам работы задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется формировать списки правил до запуска задачи в режиме активного контроля подключения внешних устройств.

Импорт правил контроля устройств из файла формата XML

► *Чтобы импортировать правила контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В нижней части панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.
4. Нажмите на кнопку **Добавить**.
5. В контекстном меню кнопки выберите пункт **Импортировать правила из файла формата XML**.
6. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла формата XML**:

   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.
7. В окне Microsoft Windows **Открыть** выберите XML-файл, который содержит параметры **правил контроля устройств**.
8. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля устройств**.

О задаче Формирование правил контроля устройств

Задача Формирование правил контроля устройств позволяет автоматически формировать список разрешающих правил для подключения флеш-накопителей и других запоминающих устройств на основе данных операционной системы об устройствах, которые ранее подключались к защищаемому компьютеру.

> Kaspersky Industrial CyberSecurity for Nodes 2.5 не получает доступ к данным системы о мобильных устройствах, подключаемых по протоколу MTP. Вы не можете создавать запрещающие правила для MTP-подключаемых мобильных устройств.

По завершении выполнения задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 создает конфигурационный файл в формате XML со списком разрешающих правил для обнаруженных внешних устройств или сразу добавляет сформированные правила в задачу Контроль устройств в зависимости от настроенных параметров задачи. В дальнейшем программа будет разрешать подключение устройств, для которых были автоматически сформированы разрешающие правила.

Сформированные и добавленные в задачу правила отображаются по ссылке **Правила контроля устройств** в узле **Контроль устройств**.

Настройка задачи Формирование правил контроля устройств

По умолчанию задача Фомирование правил контроля устройств имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Таблица 28. Параметры задачи Формирование правил контроля устройств по умолчанию

Параметр	Значение по умолчанию	Описание
Действия по завершении задачи	Разрешающие правила добавляются в список правил задачи Контроль устройств; новые правила объединяются с существующими правилами; дублирующие правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующих правил или заменять существующие правила новыми разрешающими правилами, а также настроить параметры экспорта разрешающих правил в файл.
Расписание запуска задачи	Первый запуск не определен.	Задача Формирование правил контроля устройств не запускается автоматически чразу после Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

► *Чтобы настроить параметры задачи Формирование правил контроля устройств, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Формирование правил контроля устройств**.
3. В панели результатов узла **Формирование правил контроля устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** укажите действия, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 должна выполнять по завершении задачи:
   - **Добавлять разрешающие правила в список правил контроля запуска программ**.

     Флажок включает или выключает добавление сформированных разрешающих правил в список правил контроля запуска программ. Список правил контроля запуска программ отображается по ссылке Правила контроля запуска программ в панели результатов узла Контроль запуска программ.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 добавляет правила, сформированные в ходе выполнения задачи Формирование правил контроля запуска программ, в список правил контроля запуска программ согласно установленному принципу добавления.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не добавляет сформированные разрешающие правила в список правил контроля запуска программ. Сформированные правила только экспортируются в файл.

По умолчанию флажок установлен.

Флажок не может быть снят, если не установлен флажок **Экспортировать разрешающие правила в файл**.

- **Принцип добавления**.

  Раскрывающийся список, позволяющий указать способ добавления сформированных разрешающих правил в список правил контроля запуска программ.

  - **Добавлять к существующим правилам**. Правила дополняют список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
  - **Заменять существующие правила**. Правила добавляются вместо существующих правил.
  - **Объединять с существующими правилами**. Правила дополняют список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

  По умолчанию установлен способ **Объединять с существующими правилами**.

- **Экспортировать разрешающие правила в файл**.

  Флажок включает или выключает экспорт сформированных разрешающих правил контроля запуска программ в файл.

  Если флажок установлен, по завершении задачи автоматического формирования разрешающих правил Kaspersky Industrial CyberSecurity for Nodes экспортирует сформированные правила в файл, указанный в поле ниже.

  Если флажок снят, по завершении задачи автоматического формирования разрешающих правил Kaspersky Industrial CyberSecurity for Nodes не экспортирует сформированные правила в файл, а только добавляет их в список правил контроля запуска программ.

  По умолчанию флажок снят.

  Флажок не может быть снят, если не установлен флажок **Добавлять разрешающие правила в список правил контроля запуска программ.**

- **Добавлять информацию о компьютере в имя файла**.

  Флажок включает или выключает добавление информации о защищаемом компьютере в имя файла, в который экспортируются сформированные правила контроля запуска программ.

  Если флажок установлен, программа добавляет имя защищаемого компьютера, дату и время формирования файла в имя файла экспорта.

  Если флажок снят, программа не добавляет информацию о защищаемом компьютере в имя файла экспорта.

Флажок доступен, если установлен флажок **Экспортировать разрешающие правила в файл**.

По умолчанию флажок установлен.

5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 62).
6. Нажмите на кнопку **OK**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Контроль Wi-Fi

Этот раздел содержит описание задачи "Контроль Wi-Fi" и инструкции по ее настройке.

В этом разделе

О задаче Контроль Wi-Fi

В ходе выполнения задачи Контроль Wi-Fi Kaspersky Industrial CyberSecurity for Nodes 2.5 отслеживает попытки подключения защищаемого компьютера к сетям Wi-Fi и блокирует или разрешает подключения к обнаруженным сетям Wi-Fi. Задача Контроль Wi-Fi работает на основе принципа блокировки по умолчанию (Default Deny), который означает автоматическое блокирование подключений к любым сетям Wi-Fi, если такие сети не разрешены в параметрах задачи.

Задача Контроль Wi-Fi может выполняться в одном из двух режимов:

- **Активный**. Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует подключения к сетям Wi-Fi в соответствии с настроенными параметрами задачи. Если в задаче применяется список доверенных сетей Wi-Fi, программа блокирует подключения к любым сетям Wi-Fi, кроме указанных в списке. Если в задаче не применяется список доверенных сетей Wi-Fi, программа блокирует подключения к любым сетям Wi-Fi.

При запуске задачи в режиме Контролировать подключения к сетям Wi-Fi Kaspersky Industrial CyberSecurity for Nodes 2.5 заблокирует все текущие подключения к сетям Wi-Fi, если используемые сети Wi-Fi не добавлены в список доверенных.

- **Только сообщать**. Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет блокировать подключения к сетям Wi-Fi. Вместо этого он только фиксирует в журнале выполнения задачи информацию о подключениях к доступным сетям Wi-Fi и возможный ответ программы на попытки подключения. Подключение ко всем сетям Wi-Fi разрешено.

  Этот режим установлен по умолчанию.

Вы можете использовать этот режим для последующего формирования списка доверенных сетей Wi-Fi на основе информации, зафиксированной в журнале выполнения задачи.

Задача Контроль Wi-Fi доступна для запуска на серверах под управлением операционных систем, в которых установлен и запущен сервис wlansvc. Задача Контроль Wi-Fi недоступна без донастройки параметров в операционных системах, не поддерживающих сервис wlansvc в качестве предустановленного:

- Microsoft Windows Server 2003 R2 – сервис wlansvc отсутствует и не может быть установлен.
- Microsoft Windows Server 2008 – сервис wlansvc отсутствует и должен быть установлен и запущен до запуска задачи Контроль Wi-Fi.
- Microsoft Windows Server 2008 R2 – сервис wlansvc отсутствует и должен быть установлен и запущен до запуска задачи Контроль Wi-Fi.
- Microsoft Windows Server 2012 R2 – сервис wlansvc отсутствует и должен быть установлен и запущен до запуска задачи Контроль Wi-Fi.

  Для установки сервиса wlansvc на компьютере под управлением Microsoft Windows Server 2012 R2 требуется перезагрузка защищаемого компьютера.

- Microsoft Windows Server 2016 – сервис wlansvc отсутствует и должен быть установлен до запуска задачи Контроль Wi-Fi.

Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически проверяет наличие сервиса wlansvc в операционной системе при установке и исключает компонент Контроль Wi-Fi из списка рекомендуемой установки, если не обнаруживает сервис wlansvc. В этом случае вы все равно можете выбрать Компонент Wi-Fi в списке выборочной установки: задача Контроль Wi-Fi будет недоступна для запуска до установки и запуска сервиса wlansvc.

Настройка задачи Контроль Wi-Fi

Задача Контроль Wi-Fi имеет ряд параметров, настроенных по умолчанию, которые вы можете изменять в соответствии с требованиями безопасности (см. таблицу ниже).

Таблица 29. Параметры задачи Контроль Wi-Fi по умолчанию

Параметр	Значение по умолчанию	Описание
Режим работы задачи	**Только сообщать**	По умолчанию задача только уведомляет пользователя о блокировке и разрешении подключений к сетям Wi-Fi с помощью записей в журнале выполнения задачи. Фактическая блокировка подключений не выполняется. Вы можете выбрать режим **Активный** для защиты компьютера после того, как будет сформирован список доверенных сетей Wi-Fi.
Разрешение подключений к доверенным Wi-Fi сетям	Список доверенных сетей Wi-Fi учитывается. Список доверенных сетей Wi-Fi пуст.	Вы можете не учитывать список исключений для доверенных сетей Wi-Fi, чтобы блокировать подключения к любым сетям Wi-Fi.

Параметр	Значение по умолчанию	Описание
Расписание запуска задачи	При запуске программы	Задача Контроль Wi-Fi запускается автоматически при запуске программы. Вы можете настроить расписание запуска задачи.

► *Чтобы настроить параметры задачи Контроль Wi-Fi, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль Wi-Fi**.
3. **Перейдите по ссылке** Свойства на панели результатов узла Контроль Wi-Fi.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие**:
   - **В блоке** Режим работы укажите режим работы задачи Контроль Wi-Fi:
     - **Активный**.

       Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует подключения к сетям Wi-Fi в соответствии с настроенными параметрами задачи. Если в задаче применяется список исключений для доверенных сетей Wi-Fi, программа блокирует подключения к любым сетям Wi-Fi, кроме указанных в списке. Если в задаче не применяется список исключений, программа блокирует подключения к любым сетям Wi-Fi.
     - **Только сообщать**.

       Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет контролировать подключения к сетям Wi-Fi. Вместо этого он только фиксирует в журнале выполнения задачи информацию о подключениях к доступным сетям Wi-Fi и возможный ответ программы на попытки подключения. Подключение ко всем сетям Wi-Fi разрешено.

       Этот режим установлен по умолчанию.
   - Снимите или установите флажок **Разрешать подключение к указанным сетям Wi-Fi**.

     Флажок включает или выключает применение списка исключений для доверенных сетей Wi-Fi.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает сети Wi-Fi, добавленные в список, в качестве исключений. В случае, если вы задавали список исключений ранее и устанавливаете флажок повторно, программа автоматически применяет последнюю версию списка.

     Если флажок снят, программа блокирует подключения к любым сетям Wi-Fi. Редактирование списка исключений недоступно. Заданный список исключений не учитывается, но сохраняется в параметрах задачи.

     По умолчанию флажок установлен.
   - Если требуется, отредактируйте **список доверенных сетей Wi-Fi** (см. раздел "**О списке доверенных сетей Wi-Fi**" на стр. 171).
5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 62).
6. Нажмите на кнопку **ОК**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров задачи. Данные о времени изменения параметров, а также значения параметров задачи до и после их изменения будут сохранены в журнале выполнения задачи.

О списке доверенных сетей Wi-Fi

Вы можете задавать список доверенных сетей Wi-Fi, чтобы не учитывать такие сети при блокировании подключений. Для создания исключения для доверенной сети Wi-Fi вы можете:

- добавить доверенные сети Wi-Fi вручную (см. раздел "Добавление доверенной сети Wi-Fi вручную" на стр. 171);
- выбрать доверенные сети Wi-Fi из списка доступных сетей (см. раздел "Добавление доверенной сети Wi-Fi с помощью списка доверенных сетей Wi-Fi" на стр. 172);
- использовать режим **Только сообщать** в задаче Контроль Wi-Fi.

Вы можете добавлять и удалять заданные исключения. Вы не можете редактировать заданные исключения.

Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает подключение к доверенным сетям Wi-Fi на основе следующих критериев:

- **Идентификатор беспроводной сети SSID** (далее "SSID"). SSID (Service Set Identifier) – это имя сети Wi-Fi, которое вы можете найти в списке операционной системы, содержащем данные о доступных для подключения сетях Wi-Fi. Значение SSID не является уникальным признаком сети Wi-Fi.
- **Наличие шифрования сети Wi-Fi**. Вы можете узнать, защищено ли подключение к сети Wi-Fi паролем, в списке операционной системы, содержащем данные о доступных для подключения сетях Wi-Fi.

Значения этих критериев отображаются в соответствующих графах списка доверенных сетей Wi-Fi в параметрах задачи Контроль Wi-Fi.

В ходе выполнения задачи Контроль Wi-Fi программа также блокирует подключение к сетям Wi-Fi со скрытым SSID, если сети Wi-Fi с таким SSID не добавлены в список доверенных. Вы можете добавить исключение для доверенной сети Wi-Fi со скрытым SSID только вручную.

Добавление доверенной сети Wi-Fi вручную

При добавлении доверенной сети Wi-Fi вручную вам нужно самостоятельно задать критерии, на основе которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет разрешать подключение к доверенной сети Wi-Fi.

► *Чтобы добавить сети Wi-Fi в список доверенных вручную, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль Wi-Fi**.
3. Перейдите по ссылке **Свойства** на панели результатов узла Контроль Wi-Fi.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. Если требуется, установите флажок **Разрешать подключения к указанным сетям Wi-Fi**, чтобы разрешить редактирование списка доверенных сетей Wi-Fi.

   Флажок включает или выключает применение списка исключений для доверенных сетей Wi-Fi.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает сети Wi-Fi, добавленные в список, в качестве исключений. В случае, если вы задавали список исключений ранее и устанавливаете флажок повторно, программа автоматически применяет последнюю версию списка.

   Если флажок снят, программа блокирует подключения к любым сетям Wi-Fi. Редактирование списка исключений недоступно. Заданный список исключений не учитывается, но сохраняется в параметрах задачи.

   По умолчанию флажок установлен.

5. Нажмите на кнопку **Добавить доверенную сеть Wi-Fi**.
6. В контекстном меню кнопки выберите пункт **Добавить сеть Wi-Fi вручную**.

   Откроется окно **Доступные сети Wi-Fi**.

7. Укажите параметры сети Wi-Fi, на основе которых Kaspersky Industrial CyberSecurity for Nodes 2.5 будет разрешать подключение к доверенной сети Wi-Fi:

   - В поле **Идентификатор сети Wi-Fi (SSID)** укажите имя сети Wi-Fi.

     Вы не можете задать пустое значение SSID.

   - Снимите или установите флажок **Разрешать только безопасные сети Wi-Fi**.

     Флажок включает или выключает учет наличия шифрования при исключении сети Wi-Fi с заданным SSID.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 разрешает подключение к сетям Wi-Fi с заданным SSID, только если такое подключение зашифровано и защищено паролем.

     Если флажок снят, программа разрешает подключение к любым сетям Wi-Fi с заданным SSID.

     По умолчанию флажок установлен.

8. В окне **Доступные сети Wi-Fi**, нажмите на кнопку **ОК**.

Указанная сеть Wi-Fi будет добавлена в список доверенных сетей Wi-Fi в параметрах задачи Контроль Wi-Fi. При выполнении задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 будет разрешать подключение к сетям Wi-Fi, которые подпадают под действие заданного исключения.

Добавление доверенной сети Wi-Fi с помощью списка доступных сетей Wi-Fi

При добавлении исключения для доверенной сети Wi-Fi Kaspersky Industrial CyberSecurity for Nodes 2.5 получает данные обо всех доступных сетях Wi-Fi от операционной системы.

Вы не можете добавить сеть Wi-Fi в список доверенных с помощью списка доступных сетей Wi-Fi: если SSID сети Wi-Fi скрыт, она не будет отображаться в списке доступных сетей Wi-Fi.

► *Чтобы добавить доверенную сеть Wi-Fi с помощью списка доступных сетей Wi-Fi, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль Wi-Fi**.
3. Перейдите по ссылке Свойства на панели результатов узла **Контроль Wi-Fi**.

   Откроется окно **Параметры задачи** на закладке Общие.
4. Если требуется, установите флажок **Разрешать подключения к указанным сетям Wi-Fi**, чтобы разрешить редактирование списка доверенных сетей Wi-Fi.

   Флажок включает или выключает применение списка исключений для доверенных сетей Wi-Fi.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает сети Wi-Fi, добавленные в список, в качестве исключений. В случае, если вы задавали список исключений ранее и устанавливаете флажок повторно, программа автоматически применяет последнюю версию списка.

   Если флажок снят, программа блокирует подключения к любым сетям Wi-Fi. Редактирование списка исключений недоступно. Заданный список исключений не учитывается, но сохраняется в параметрах задачи.

   По умолчанию флажок установлен.
5. Нажмите кнопку **Добавить доверенную сеть Wi-Fi**.
6. В контекстном меню кнопки выберите пункт **Выбрать из списка доступных сетей Wi-Fi**.

   Откроется окно **Доступные сети Wi-Fi**.
7. Если требуется, нажмите кнопку **Обновить список**, чтобы получить актуальный список доступных сетей Wi-Fi.
8. В списке доступных сетей Wi-Fi выберите одну или несколько сетей Wi-Fi для добавления в список доверенных.
9. Нажмите на кнопку **Добавить выбранные**.
10. Нажмите на кнопку **ОК**.

Указанные сети Wi-Fi будут добавлены в список доверенных сетей Wi-Fi в параметрах задачи Контроль Wi-Fi. При выполнении задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 будет разрешать подключение к указанным сетям Wi-Fi.

Удаление исключения для сети Wi-Fi

► *Чтобы удалить сеть Wi-Fi из списка доверенных, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль Wi-Fi**.
3. Перейдите по ссылке **Свойства** на панели результатов узла Контроль Wi-Fi.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. Если требуется, установите флажок **Разрешать подключения к указанным сетям Wi-Fi**, чтобы разрешить редактирование списка доверенных сетей Wi-Fi.
5. В списке доверенных сетей Wi-Fi выделите сети Wi-Fi, которые вы хотите удалить.
6. Нажмите на кнопку **Удалить сеть Wi-Fi**.
7. Нажмите на кнопку **ОК**.

Выбранные сети Wi-Fi будут удалены из списка доверенных сетей Wi-Fi. Kaspersky Industrial CyberSecurity for Nodes 2.5 будет блокировать подключение к таким сетям Wi-Fi.

Управление сетевым экраном

Этот раздел содержит информацию о задаче Управление сетевым экраном и инструкции о том, как настроить параметры этой задачи.

В этом разделе

О задаче Управление сетевым экраном

Kaspersky Industrial CyberSecurity for Nodes 2.5 обеспечивает надежное и эргономичное решение для защиты сетевых подключений с помощью задачи Управление сетевым экраном.

Задача Управление сетевым экраном не выполняет самостоятельную фильтрацию сетевого трафика, но предоставляет возможность управления сетевым экраном Windows через графический интерфейс Kaspersky Industrial CyberSecurity for Nodes 2.5. В ходе выполнения задачи Управление сетевым экраном Kaspersky Industrial CyberSecurity for Nodes 2.5 полностью принимает на себя управление параметрами и правилами сетевого экрана операционной системы и блокирует любую возможность настройки сетевого экрана другими способами.

В ходе установки программы компонент Управление сетевым экраном считывает и копирует состояние сетевого экрана Windows, а также все заданные правила. В дальнейшем изменение набора правил или их параметров, а также остановка или запуск сетевого экрана возможны только через Kaspersky Industrial CyberSecurity for Nodes 2.5.

Если при установке Kaspersky Industrial CyberSecurity for Nodes 2.5 сетевой экран Windows отключен, задача Управление сетевым экраном не выполняется по завершении установки. Если при установке программы сетевой экран Windows включен, задача Управление сетевым экраном выполняется по завершении установки и блокирует все сетевые подключения, на разрешенные заданными правилами.

Компонент Управление сетевым экраном не входит в набор компонентов Рекомендуемой установки и не устанавливается по умолчанию.

Задача Управление сетевым экраном форсирует блокирование всех входящих и исходящих подключений, если они не разрешены заданными правилами задачи.

Задача регулярно опрашивает сетевой экран Windows и контролирует его состояние. По умолчанию интервал опроса составляет 1 минуту и не может быть изменен. Если при совершении опроса Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает несовпадение параметров сетевого экрана Windows и параметров задачи Управление сетевым экраном, программа форсированно передает параметры задачи сетевому экрану операционной системы.

При ежеминутном опросе сетевого экрана Windows Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует следующие статусы:

- статус работы сетевого экрана Windows;
- статус правил, добавленных после установки Kaspersky Industrial CyberSecurity for Nodes 2.5 другими программами или инструментами (например, добавление нового правила программы для порта или программы с помощью wf.msc).

После передачи правил сетевому экрану Kaspersky Industrial CyberSecurity for Nodes 2.5 создает группу правил Kaspersky Security Group в оснастке **Брандмауэр Windows**. Эта группа объединяет все правила, созданные на стороне Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью задачи Управление сетевым экраном. Правила, входящие в группу Kaspersky Security Group, не контролируются программой при ежеминутном опросе и не синхронизируются автоматически со списком правил, заданным в параметрах задачи Управление сетевым экраном.При необходимости вы можете выполнить обновление правил Kaspersky Security Group вручную.

► *Чтобы обновить список правил Kaspersky Security Group вручную,*

перезапустите задачу Управление сетевым экраном Kaspersky Industrial CyberSecurity for Nodes 2.5.

Вы также можете изменять правила Kaspersky Security Group вручную через оснастку **Брандмауэр Windows**.

Запуск задачи Управление сетевым экраном невозможен, если сетевой экран Windows находится под управлением групповой политики Kaspersky Security Center.

О правилах сетевого экрана

Задача Управление сетевым экраном контролирует фильтрацию входящего и исходящего трафика с помощью разрешающих правил, которые форсировано сообщаются сетевому экрану Windows при выполнении задачи.

При первом запуске задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 считывает и копирует все разрешающие правила для входящего трафика, заданные в параметрах сетевого экрана Windows, в параметры задачи Управление сетевым экраном. При дальнейшей работе программа действует в соответствии со следующими алгоритмами:

- если в параметрах сетевого экрана Windows создается новое правило (вручную или автоматически при установке новой программы), Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет такое правило;
- если в параметрах сетевого экрана Windows удаляется существующее правило, Kaspersky Industrial CyberSecurity for Nodes 2.5 восстанавливает такое правило;
- если в параметрах сетевого экрана Windows изменяются параметры существующего правила, Kaspersky Industrial CyberSecurity for Nodes 2.5 отменяет изменения;
- если в параметрах задачи Управление сетевым экраном создается новое правило, Kaspersky Industrial CyberSecurity for Nodes 2.5 форсированно передает это правило сетевому крану Windows;
- если в параметрах задачи Управление сетевым экраном удаляется существующее правило, Kaspersky Industrial CyberSecurity for Nodes 2.5 форсированно удаляет такое правило в параметрах сетевого экрана Windows.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не работает с запрещающими правилами, а также с правилами, контролирующими исходящий трафик. В момент запуска задачи Управление сетевым экраном Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет все правила этих типов в параметрах сетевого экрана Windows.

Вы можете задавать, удалять и редактировать правила для фильтрации входящего трафика.

Вы не можете задать новое правило для контроля исходящего трафика через параметры задачи Управление сетевым экраном. Все правила сетевого экрана, заданные через Kaspersky Industrial CyberSecurity for Nodes 2.5, контролируют только входящий трафик.

Вы можете работать с правилами сетевого экрана следующих типов:

- Правила для приложений
- Правила для портов

Правила для приложений

Правила этого типа выборочно разрешают сетевые подключения для указанных приложений. Критерием срабатывания таких правил является путь к исполняемому файлу.

Вы можете управлять правилами для приложений:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила.
- изменять параметры заданных правил: указывать имя правила, путь к исполняемому файлу и область применения правила.

Правила для портов

Правила этого типа разрешают сетевые подключения для указанных портов и протоколов (TCP / UDP). Критериями срабатывания таких правил являются номер порта и тип протокола.

Вы можете управлять правилами для портов:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила.
- изменять параметры заданных правил: указывать имя правила, номер порта, тип протокола и область применения правила.

Правила для портов предполагают более широкую область действия, чем правила для приложений. Разрешая подключения с помощью правил для портов, вы снижаете уровень безопасности защищаемого компьютера.

Активация и выключение правил сетевого экрана

► *Чтобы активировать или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.
4. Откроется окно **Правила сетевого экрана**.
5. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.

6. 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. В окне Правила сетевого экрана нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Добавление правил сетевого экрана вручную

► *Чтобы добавить новое или изменить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, которое вы хотите добавить, выберите закладку **Приложения** или закладку **Порты** и выполните одно из следующих действий:
   - Чтобы изменить существующее правило, в списке правил выберите правило, параметры которого вы хотите настроить и нажмите на кнопку **Изменить**.
   - Чтобы создать новое правило, нажмите на кнопку **Добавить**.

     В зависимости от типа настраиваемого правила, откроется окно **Настроить правило для приложения** или окно **Настроить правило для порта**.
5. В открывшемся окне выполните следующие действия:
   - Если вы работаете с правилом для приложения, выполните следующие действия:
     a. В поле **Имя правила** укажите имя редактируемого правила.
     b. В поле **Путь к приложению** укажите путь к исполняемому файлу программы, подключения для которого вы хотите разрешить с помощью редактируемого правила.

        Вы можете задать путь вручную или с помощью кнопки **Обзор**.
     c. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

        Допускается указание IP-адресов только в формате IPv4.

- Если вы работаете с правилом для порта, выполните следующие действия:
  a. В поле **Имя правила** укажите имя редактируемого правила.
  b. В поле **Номер порта** укажите номер порта, для которого программа будет разрешать соединения.
  c. Выберите тип протокола (TCP / UDP), для которого программа будет разрешать соединения.
  d. В поле **Область применения правила** укажите сетевые адреса, в рамках которых будет выполнятся настраиваемое правило.

  > Допускается указание IP-адресов только в формате IPv4.

6. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **ОК**.
7. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Удаление правил сетевого экрана

> Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

► *Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Управление сетевым экраном**.
3. В панели результатов узла **Управление сетевым экраном** перейдите по ссылке **Правила сетевого экрана**.

   Откроется окно **Правила сетевого экрана**.
4. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Приложения** или закладку **Порты**.
5. В списке правил выберите правило, которое вы хотите удалить.
6. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
7. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи Управление сетевым экраном будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Диагностика системы

Этот раздел содержит информацию о задаче контроля файловых операций и возможностях анализа системного журнала операционной системы.

В этом разделе

Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Монитор целостности файлов.

В этом разделе

О задаче Мониторинг файловых операций

Задача Мониторинг файловых операций предназначена для отслеживания действий, выполненных с указанными файлами или папками, в областях мониторинга, заданных в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом компьютере. Вы также можете настроить отслеживание изменений файлов в периоды обрыва мониторинга.

Обрыв мониторинга – это период, когда область мониторинга временно выпадает из поля действия задачи, например из-за приостановки выполнения задачи или физического отсутствия запоминающего устройства на защищаемом компьютере. Kaspersky Industrial CyberSecurity for Nodes 2.5 сообщит об обнаружении файловых операций в области мониторинга, как только запоминающее устройство будет вновь подключено.

Приостановка выполнения задачи в заданной области мониторинга, вызванная переустановкой компонента Мониторинг файловых операций, не является обрывом мониторинга. В этом случае задача Мониторинг файловых операций не выполняется.

Требования к среде

Для запуска задачи Мониторинг файловых операций должны быть соблюдены следующие условия:

- На защищаемом компьютере установлено запоминающее устройство, поддерживающее файловые системы ReFS и NTFS.
- USN-журнал Windows должен быть включен. На основе опроса USN журнала компонент получает данные о файловых операциях.

> Если вы включили USN-журнал после того, как было создано правило для тома и запущена задача Мониторинга файловых операций, требуется перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

Исключения для области мониторинга

Вы можете создать исключения из области мониторинга. Исключения задаются для каждого отдельного правила и работают только для указанной области мониторинга. Вы можете задать неограниченное количество исключений для каждого правила.

> Исключения имеют более высокий приоритет, чем область мониторинга, и не контролируются задачей, даже если указанная папка или файл входят в область мониторинга. Если в параметрах одного из правил задана область мониторинга, которая является нижнеуровневой по отношению к папке, заданной в исключениях, такая область мониторинга не будет учитываться при выполнении задачи.

Для задания исключений вы можете использовать те же маски, что и для задания областей мониторинга.

О правилах мониторинга файловых операций

Задача Мониторинг файловых операций выполняется на основе правил мониторинга файловых операций. Вы можете настраивать условия срабатывания задачи и регулировать уровень важности событий для обнаруженных файловых операций, фиксируемых в журнале выполнения задачи, с помощью критериев срабатывания правила.

Правило мониторинга файловых операций задается для каждой указанной области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- Доверенные пользователи
- Маркеры файловых операций

Доверенные пользователи

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности события, формируя список доверенных пользователей в параметрах правила мониторинга файловых операций.

Недоверенный пользователь – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает файловую операцию, выполненную недоверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Критическое событие в журнале выполнения задачи.

Доверенный пользователь – пользователь или группа пользователей, которым разрешено выполнение файловых операций в указанной области мониторинга. Если Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает файловую операцию, выполненную доверенным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности Информационное событие в журнале выполнения задачи.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не может определить пользователя, выполнившего операции в период обрыва мониторинга. В этом случае статус пользователя определяется как неизвестный.

Неизвестный пользователь – данный статус присваивается пользователю в случае, когда Kaspersky Industrial CyberSecurity for Nodes 2.5 не может получить данные о пользователе вследствие прерывания задачи или сбоя драйвера синхронизации данных или USN-журнала. Если Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает файловую операцию, выполненную неизвестным пользователем, задача Мониторинг файловых операций фиксирует событие с уровнем важности *Предупреждение* в журнале выполнения задачи.

Маркеры файловых операций

В ходе выполнения задачи Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes 2.5 определяет, что над файлом было произведено действие, с помощью маркеров файловых операций.

Маркер файловой операции – это единичный признак, которым может быть охарактеризована файловая операция.

Каждая файловая операция может представлять собой одно действие или цепочку действий с файлами. Каждое такое действие приравнивается к маркеру файловой операции. Если в цепочке файловой операции был обнаружен маркер, указанный вами в качестве критерия срабатывания правила мониторинга, программа зафиксирует событие по факту совершения такой файловой операции.

Уровень важности фиксируемых событий не зависит от выбранных маркеров файловых операций или их количества.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см.таблицу ниже).

Таблица 30. Маркеры файловых операций

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
BASIC_INFO_CHANGE	изменены атрибуты или метки времени файла или папки	NTFS, ReFS
COMPRESSION_CHANGE	изменено сжатие файла или папки	NTFS, ReFS
DATA_EXTEND	размер файла или папки увеличен	NTFS, ReFS
DATA_OVERWRITE	перезаписаны данные в файле или папке	NTFS, ReFS
DATA_TRUNCATION	файл или папка усечены	NTFS, ReFS
EA_CHANGE	изменены расширенные атрибуты файла или папки	только NTFS
ENCRYPTION_CHANGE	изменен статус шифрования файла или папки	NTFS, ReFS
FILE_CREATE	файл или папка созданы впервые	NTFS, ReFS
FILE_DELETE	Файл или папка удалены, минуя корзину, с помощью команды SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	жесткая связь создана или удалена для файла или папки	только NTFS
INDEXABLE_CHANGE	изменен статус индексирования файла или папки	NTFS, ReFS
INTEGRITY_CHANGE	изменен атрибут целостности для именованного файлового потока	только ReFS
NAMED_DATA_EXTEND	размер именованного файлового потока увеличен	NTFS, ReFS
NAMED_DATA_OVERWRITE	именованный файловый поток перезаписан	NTFS, ReFS
NAMED_DATA_TRUNCATION	именованный файловый поток усечен	NTFS, ReFS
OBJECT_ID_CHANGE	изменен идентификатор файла или папки	NTFS, ReFS
RENAME_NEW_NAME	присвоено новое имя для файла или папки	NTFS, ReFS
REPARSE_POINT_CHANGE	создана новая или изменена существующая точка повторного анализа для файла или папки	NTFS, ReFS
SECURITY_CHANGE	изменены права доступа к файлу или папке	NTFS, ReFS
STREAM_CHANGE	создан новый или изменен существующий именованный файловый поток	NTFS, ReFS
TRANSACTED_CHANGE	именованный файловый поток изменен транзакцией TxF	только ReFS

Настройка параметров задачи Мониторинг файловых операций

Вы можете изменять параметры задачи Мониторинг файловых операций, заданные по умолчанию (см.таблицу ниже).

Таблица 31. Параметры задачи Мониторинг файловых операций по умолчанию

Параметр	Значение по умолчанию	Описание
Область мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.
Список доверенных пользователей	Не задано	Вы можете задать пользователей и/или группы пользователей, действия которых в указанных каталогах будут расцениваться компонентом как безопасные.
Контролировать файловые операции во время простоя задачи	Применяется	Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.
Учитывать исключенные области мониторинга	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes 2.5 будет пропускать области мониторинга, заданные в качестве исключений.
Расчет контрольной суммы	Не применяется	Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.
Учитывать маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Вы можете задать набор маркеров для характеристики файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Industrial CyberSecurity for Nodes 2.5 формирует событие аудита.
Расписание запуска задачи	Первый запуск не определен	Вы можете настроить параметры запуска задачи по расписанию.

► *Чтобы настроить параметры задачи Мониторинг файловых операций, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** снимите или установите флажок **Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга**.

   Флажок включает или выключает контроль над файловыми операциями, выбранными в параметрах задачи Мониторинг файловых операций, во время простоя задачи по любой причине (извлечение жесткого диска, остановка задачи пользователем, сбой программного обеспечения).

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет фиксировать события во всех областях мониторинга при прерывании задачи Мониторинг файловых операций.

   Если флажок снят, при прерывании задачи файловые операции в областях мониторинга не будут фиксироваться программой.

   По умолчанию флажок установлен.
5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Работа с расписанием задач" на стр. 62).
6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Настройка правил мониторинга

По умолчанию область мониторинга не задана; задача не контролирует выполнение файловых операций ни в одной директории.

► *Чтобы добавить область мониторинга, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Правила мониторинга**.

   Откроется окно **Мониторинг файловых операций**.

4. Добавьте область мониторинга одним из следующих способов:
   - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:
     a. В левой части окна нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Обзор папок**.

     b. В открывшемся окне выберите папку, операции в которой вы хотите контролировать, и нажмите кнопку **ОК**.

     c. Нажмите кнопку **Добавить**, чтобы программа Kaspersky Industrial CyberSecurity for Nodes 2.5 начала контролировать файловые операции в указанной области мониторинга.
   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:
     - <*.ext> - все файлы с расширением <ext> вне зависимости от их расположения;
     - <*\name.ext> - все файлы с именем name и расширением <ext> вне зависимости от их расположения;
     - <\dir*> - все файлы в директории <\dir>;
     - <\dir*\name.ext> - все файлы с именем name и расширением <ext> в директории <\dir> и всех ее поддиректориях.

   При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Industrial CyberSecurity for Nodes 2.5 не добавит указанную область мониторинга.

   В правой части окна на закладке **Параметры правила** отобразятся доверенные пользователи и маркеры файловых операций, выбранные для этой области мониторинга.
5. В списке добавленных областей мониторинга выберите область, для которой хотите настроить другие параметры.
6. Выберите закладку **Пользователи**.
7. Нажмите кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор: "Пользователи" или "Группы"**.
8. Выберите пользователей или группы пользователей, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 будет считать доверенными для выбранной области мониторинга.
9. Нажмите на кнопку **ОК**.

   По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 считает недоверенными всех пользователей, не указанных в списке доверенных (см. раздел "О правилах мониторинга файловых операций" на стр. 181), и формирует для них события с уровнем важности Критическое событие.
10. Выберите закладку **Маркеры файловых операций**.

11. Если требуется, выберите несколько маркеров файловых операций, выполнив следующие действия:
    a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
    b. В открывшемся списке доступных файловых операций (см. раздел "О правилах мониторинга файловых операций" на стр. 181) установите флажки напротив тех операций, которые вы хотите контролировать.

    По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует все доступные файловые операции, выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

12. Если вы хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes 2.5 рассчитывала контрольную сумму файлов после изменений, выполните следующие действия:
    a. В блоке **Контрольная сумма** установите флажок **Рассчитывать контрольную сумму измененного файла, если это возможно**.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 рассчитывает контрольную сумму измененного файла, в котором была обнаружена файловая операция, соответствующая хотя бы одному маркеру файловой операции.

       Если файловая операция обнаруживается сразу по нескольким маркерам, рассчитывается только финальная контрольная сумма файла после всех последовательных изменений.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не рассчитывает контрольную сумму измененных файлов.

       Программа не выполняет расчет контрольной суммы в следующих случаях:

       - если в результате файловой операции файл стал недоступен (например, изменены права доступа к файлу);
       - если файловая операция фиксируется для файла, который впоследствии был удален.

       По умолчанию флажок снят.

    b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из вариантов:
       - **Хеш MD5**.
       - **Хеш SHA256**.

13. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:
    a. Выберите закладку **Исключения**.
    b. Установите флажок **Учитывать исключенные области мониторинга**.

       Флажок включает или выключает применение исключений для папок, в которых не требуется мониторинг файловых операций.

       Если флажок установлен, при выполнении задачи Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes 2.5 будет пропускать области мониторинга, заданные в списке исключений.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 будет фиксировать события для всех заданных областей мониторинга.

       По умолчанию флажок снят, список исключений пуст.

c. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Обзор папок**.

d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.

e. Нажмите кнопку **Добавить**.

Указанная папка добавится в список исключенных областей.

> Вы также можете добавить исключения для области мониторинга вручную используя те же маски, что и для задания областей мониторинга.

14. Нажмите на кнопку **Сохранить**, чтобы применить новые параметры правил.

Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и параметрах задачи.

В этом разделе

О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Industrial CyberSecurity for Nodes 2.5 контролирует целостность защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках компьютерных атак.

Kaspersky Industrial CyberSecurity for Nodes 2.5 считывает данные журналов событий Windows и определяет нарушения в соответствии с правилами, заданными пользователем или параметрами эвристического анализатора, который применяется задачей для анализа журналов.

Предзаданные правила и эвристический анализ

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы с помощью предзаданных правил, осуществляющими анализ на основе встроенных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом компьютере, которая может являться признаком попытки атаки. Шаблоны определения аномальной активности заложены в доступных правилах в параметрах задачи.

Для задачи Анализ журналов доступно семь предзаданных правил. Вы можете включать и выключать применение любого правила. Вы не можете удалять существующие или создавать новые правила.

Вы можете настроить критерии срабатывания правил которые контролируют события для данных операций:

- Обработка подбора пароля

- Обработка сетевого входа

В параметрах задачи вы также можете настроить исключения. Эвристический анализатор не срабатывает, если вход в систему выполнен доверенным пользователем или с доверенного IP-адреса.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании правила, программа фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

Пользовательские правила задачи Анализ журналов

С помощью параметров правил задачи вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил задачи Анализ журналов содержит четыре правила. Вы можете включать и выключать применение данных правил, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

  Правило срабатывает при появлении новой записи в журнале событий Windows, если в параметрах события обнаружен идентификатор события, указанный для правила. Вы также можете добавлять и удалять идентификаторы для каждого заданного правила.

- Источник событий.

  Для каждого правила вы можете задать поджурнал журнала событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом поджурнале. Вы можете выбрать один из стандартных поджурналов (Приложение, Безопасность или Система), а также указать пользовательский поджурнал, указав его имя в поле выбора источника.

  Программа не выполняет проверок на фактическое наличие заданного поджурнала в журнале событий Windows.

При срабатывании правила Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует событие с уровнем важности Критическое событие в журнале выполнения задачи Анализ журналов.

По умолчанию задача Анализ журналов не учитывает пользовательские правила.

Перед запуском задачи Анализ журналов убедитесь, что политика аудита системы настроена верно. Более подробную информацию о настройке вы можете найти в данной статье https://technet.microsoft.com/en-us/library/cc952128.aspx.

Настройка параметров предзаданных правил задачи

► *Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Диагностика системы**.

2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Перейдите на закладку **Предзаданные правила**.
5. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Если этот флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет эвристический анализатор для обнаружения аномальной активности на защищаемом компьютере.

   Если этот флажок не установлен, то эвристический анализатор выключен, Kaspersky Industrial CyberSecurity for Nodes 2.5 использует предустановленные или пользовательские правила для обнаружения аномальной активности.

   По умолчанию флажок установлен.

   Для работы задачи должно быть выбрано хотя бы одно правило анализа журналов.
6. Из списка предзаданных правил, выберите правила, которые вы хотите применять для анализа журналов:
   - Обнаружена возможная попытка взлома пароля с помощью подбора.
   - 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.
   - Обнаружена подозрительная активность во время сетевого сеанса входа.
7. Чтобы настроить параметры выбранных правил, перейдите на закладку **Расширенные**.
8. В блоке **Обработка перебора пароля** укажите количество попыток и промежуток времени, в который выполнялись попытки, которые будут являться критериями срабатывания эвристического анализатора.
9. В блоке **Обработка сетевого входа** укажите начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Industrial CyberSecurity for Nodes 2.5 расценивает данное действие как аномальную активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Выбрать**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **OK**.

       Указанный пользователь добавится в список доверенных.
12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:
    a. Введите IP-адрес.

b. Нажмите на кнопку **Добавить**.

Указанный IP-адрес добавится в список доверенных.

13. Выберите закладку **Управление задачей**, чтобы настроить расписание запуска задачи.
14. Нажмите на кнопку **ОК**.

Параметры задачи Анализ журналов будут сохранены.

Настройка правил анализа журналов

Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Правила анализа журналов**.

Откроется окно **Правила анализа журналов**.

4. Снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

Если этот флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет пользовательские правила для анализа журналов в соответствии с настроенными параметрами каждого правила. Вы можете добавлять, удалять или изменять правила анализа журналов.

Если флажок снят, вы не можете добавлять или изменять пользовательские правила. Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет параметры правил по умолчанию.

По умолчанию флажок установлен. Активно только правило Обнаружено всплывающее окно приложения.

Вы можете контролировать применение предзаданных правил в списке правил. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

5. Чтобы создать новое пользовательское правило, выполните следующие действия:
   a. Введите имя нового правила.
   b. Нажмите на кнопку **Добавить**.

   Созданное правило добавится в общий список правил.
6. Чтобы настроить любое правило, выполните следующие действия:
   a. Выберите правило в списке нажатием левой кнопкой мыши.

   В правой области окна на закладке **Комментарий** отобразится общая информация о правиле.

   Комментарии для нового правила пусты.

   b. Выберите закладку **Параметры правила**.
   c. В блоке **Общие отредактируйте Имя** правила, если требуется.
   d. Выберите **Источник**.

7. В блоке **Идентификаторы событий** укажите идентификаторы записей, при обнаружении которых будет срабатывать правило:

   a. Введите числовое значение идентификатора.

   b. Нажмите кнопку **Добавить**.

      Указанный идентификатор правила добавится в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

   c. Нажмите на кнопку **Сохранить**.

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 компьютера.

В этом разделе

О задачах проверки по требованию

Kaspersky Industrial CyberSecurity for Nodes 2.5 однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы, оперативную память компьютера, а также объекты автозапуска.

В Kaspersky Industrial CyberSecurity for Nodes 2.5 предусмотрены следующие системные задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при запуске Kaspersky Industrial CyberSecurity for Nodes 2.5. Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет загрузочные секторы и главные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, программа заменяет возможно зараженный сектор резервной копией.
- Задача Проверка важных областей по умолчанию выполняется еженедельно по расписанию. Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и главные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы, которые содержатся в системных папках, например, в папке %windir%\system32. Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет параметры безопасности, значения которых соответствуют уровню Рекомендуемый (см. раздел "Выбор предустановленных уровней безопасности в задачах проверки по требованию" на стр. 210). Вы можете изменять параметры задачи Проверка важных областей.

- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз. Вы не можете изменять параметры задачи Проверка объектов на карантине.
- Задача Проверка целостности программы выполняется ежедневно. Она обеспечивает проверку модулей Kaspersky Industrial CyberSecurity for Nodes 2.5 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. Настройки расписания запуска задачи можно изменять.

Вы можете создавать пользовательские задачи проверки по требованию. Например, вы можете создать задачу проверки папок общего доступа на компьютере.

Kaspersky Industrial CyberSecurity for Nodes 2.5 может одновременно выполнять несколько задач проверки по требованию.

Статистика задач проверки по требованию

Пока выполняется задача проверки по требованию, вы можете просматривать информацию о количестве объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обработала с момента запуска задачи до текущего момента.

Эта информация будет доступна, даже если вы приостановите задачу. Вы можете просмотреть статистику задачи в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задаче Kaspersky Industrial CyberSecurity for Nodes 2.5 в журналах выполнения задач" на стр. 263).

► *Чтобы просмотреть статистику задачи проверки по требованию, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

В таблице ниже вы можете просмотреть информацию об объектах, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обработала с момента запуска задачи до текущего момента.

Таблица 32. Статистика задач проверки по требованию

Поле	Описание
Обнаружено	Количество объектов, которые обнаружила программа Kaspersky Industrial CyberSecurity for Nodes 2.5. Например, если программа Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаружила в пяти файлах одну вредоносную программу, значение в этом поле увеличится на единицу.
Зараженных и других обнаруженных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 признала зараженными, или обнаруженных объектов, которые не были исключены из области действия задач постоянной защиты или проверки по требованию и были определены как легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 признала возможно зараженными.
Объектов не вылечено	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 не вылечила по следующим причинам: • тип обнаруженного объекта не предполагает лечения; • при лечении возникла ошибка.
Объектов, не помещенных на карантин	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 попыталась поместить на карантин, но безуспешно, например, из-за отсутствия доступного пространства на диске.
Объектов не удалено	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 не смогла проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes 2.5 попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые вылечила программа Kaspersky Industrial CyberSecurity for Nodes 2.5.
Помещено на карантин	Количество объектов, которые поместила на карантин программа Kaspersky Industrial CyberSecurity for Nodes 2.5.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Industrial CyberSecurity for Nodes 2.5 сохранила в резервном хранилище.
Удалено объектов	Количество объектов, которые удалила программа Kaspersky Industrial CyberSecurity for Nodes 2.5.
Защищенных паролем объектов	Количество объектов (например, архивов), которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 пропустила, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 пропустила, так как их формат искажен.

Поле	Описание
Обработано объектов	Общее количество объектов, которые обработала программа Kaspersky Industrial CyberSecurity for Nodes 2.5.

Вы также можете посмотреть статистику задач проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

По завершении выполнения задачи проверки по требованию рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Настройка параметров задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать системные и пользовательские задачи проверки по требованию.

Таблица 33. Параметры задач проверки по требованию

Параметр	Значение	Как настроить
Область проверки	Применяется в системных и пользовательских задачах: • Проверка при старте операционной системы: весь компьютер, исключая папки общего доступа и объекты автозапуска. • Проверка важных областей: весь компьютер, исключая папки общего доступа и некоторые файлы операционной системы. • Пользовательские задачи проверки по требованию: весь компьютер.	Вы можете изменить область проверки. Вы не можете настроить область защиты для системных задач Проверка объектов на карантине и Проверка целостности программы.
Параметры безопасности	Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**	Для выбранных узлов в дереве или списке файловых ресурсов компьютера вы можете выполнить следующие действия: • выбрать другой предустановленный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла в шаблон, чтобы потом применить его для любого другого узла.

Параметр	Значение	Как настроить
Эвристический анализатор	Для задач Проверка важных областей и Проверка при старте операционной системы, а также для пользовательских задач проверки применяется с уровнем анализа **Средний**. Для задачи Проверка объектов на карантине применяется с уровнем анализа **Глубокий.**	Вы можете включать и выключать применение эвристического анализатора, регулировать уровень анализа. Вы не можете настроить уровень анализа для задачи Проверка объектов на карантине. Применение эвристического анализатора в задаче Проверка целостности программы не предусматривается.
Доверенная зона	Применяется	Единый список исключений, который вы можете применять в выбранных задачах.
Использование KSN	Применяется	Вы можете увеличить эффективность защиты компьютера с помощью использования инфраструктуры облачных служб Kaspersky Security Network.
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете изменять параметры запуска с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задач Проверка объектов на карантине и Проверка целостности программы.
Выполнение в фоновом режиме (низкий приоритет)	Не применяется	Вы можете настраивать приоритетность выполнения задач проверки по требованию.
Расписание запуска задачи	Применяется в системных задачах: • Проверка при старте операционной системы - **При запуске программы**; • Проверка важных областей - **Еженедельно**; • Проверка объектов на карантине - **После обновления баз программы**; • Проверка целостности программы - **При запуске программы**. Не применяется во вновь созданных пользовательских задачах.	Вы можете настраивать параметры запуска задачи по расписанию.
Регистрация выполнения проверки и обновление статуса защиты компьютера	Статус защиты компьютера обновляется еженедельно после выполнения задачи Проверка важных областей.	Вы можете настраивать параметры регистрации выполнения проверки важных областей следующими способами: • изменяя параметры расписания запуска задачи Проверка важных областей;

Параметр	Значение	Как настроить
		• изменяя область защиты задачи Проверка важных областей; • создавая пользовательские задачи проверки по требованию.

► *Чтобы настроить задачу проверки по требованию, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов узла на закладке **Обзор и управление** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**. Настройте следующие параметры задачи:

   - На закладке **Общие**:
     - **Использовать эвристический анализатор** (см. раздел "**Использование эвристического анализатора**" на стр. 80)
     - Выполнение задачи в фоновом режиме (см. раздел "Выполнение задачи проверки по требованию в фоновом режиме" на стр. 201).
     - Использование KSN (на стр. 202).
     - Применение Доверенной зоны (см. раздел "Включение и выключение применения доверенной зоны в задачах Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 55).
     - Регистрация выполнения задачи Проверка важных областей (см. раздел "Регистрация выполнения задачи Проверка важных областей" на стр. 202)
   - На закладках **Расписание** и **Дополнительно**:
     - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 62)
   - На закладке **Запуск с правами**:
     - Параметры запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 65)
4. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Изменения параметров задачи будут сохранены.
5. Если требуется, в панели результатов выбранного узла откройте закладку **Настройка области проверки**.

   Выполните следующие действия:

   - В дереве файловых ресурсов компьютера выберите узлы, которые хотите включить в область проверки.
   - Выберите один из предустановленных уровней безопасности (см. раздел "Выбор предустановленных уровней безопасности в задачах проверки по требованию" на стр. 210) или настройте параметры проверки вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 93).
6. В контекстном меню названия выбранной задачи выберите пункт **Сохранить задачу**.

Kaspersky Industrial CyberSecurity for Nodes 2.5 немедленно применит новые значения параметров в выполняющейся задаче. Данные о времени изменения параметров, а также значения параметров до и после их изменения будут сохранены в журнале выполнения задачи.

Применение эвристического анализатора

Вы можете использовать эвристический анализатор и настроить уровень анализа для задач Проверка по требованию и Постоянная защита файлов.

► *Чтобы настроить применение эвристического анализатора, выполните следующие действия:*

1. В зависимости от задачи:
   - Для задачи Проверка по требованию:
     a. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
     b. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
     c. В панели результатов перейдите по ссылке **Свойства**.
   - Для задачи Постоянная защита файлов:
     a. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита файлов**.
     b. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
2. Снимите или установите флажок **Использовать эвристический анализатор**.
3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

   Ползунок позволяет регулировать уровень эвристического анализа. Уровень детализации проверки обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

   Существуют следующие уровни детализации проверки:

   - **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее.
   - **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".

     Этот уровень выбран по умолчанию.
   - **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества

ложных срабатываний.

Ползунок активен, если установлен флажок **Использовать эвристический анализатор**.

4. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены. немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Выполнение задачи проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Industrial CyberSecurity for Nodes 2.5, имеют базовый приоритет **Средний**.

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, базовый приоритет **Низкий**. Понижение приоритета процесса увеличивает время выполнения задачи, но также может положительно повлиять на скорость выполнения процессов других активных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме. Вы можете установить максимальное количество процессов для фоновых задач проверки по требованию.

► *Чтобы изменить приоритет задачи проверки по требованию, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, приоритет которой вы хотите изменить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Установите или снимите флажок **Выполнять задачу в фоновом режиме**.

   Флажок изменяет приоритет задачи.

   Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему компьютера со стороны других задач Kaspersky Industrial CyberSecurity for Nodes 2.5 и программ. Как следствие, скорость выполнения задачи замедляется при увеличении нагрузки и увеличивается при уменьшении нагрузки.

   Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 и другие программы. В этом случае скорость выполнения задачи увеличивается.

   По умолчанию флажок снят.
5. 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.

Использование KSN

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network и запустить задачу.

► *Чтобы настроить использование KSN в задачах проверки по требованию, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Установите или снимите флажок **Использовать KSN для проверки**.

   Флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.

   Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

   Если флажок снят, задача постоянной защиты файлов не использует службы KSN.

   По умолчанию флажок установлен.

   Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи Использование KSN.
5. 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.

Регистрация выполнения Проверки важных областей

По умолчанию статус защиты компьютера отображается в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** и обновляется еженедельно после завершения задачи Проверка важных областей.

Время обновления статуса защиты компьютера привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**. Флажок установлен только для задачи Проверка важных областей и недоступен для редактирования.

Вы можете перепривязать задачу проверки по требованию к статусу защиты компьютера только из Kaspersky Security Center.

Область проверки в задачах проверки по требованию

Этот раздел содержит информацию о формировании и использовании области проверки в задачах проверки по требованию.

В этом разделе

Об области проверки

Вы можете настроить область проверки для задач Проверка при старте операционной системы и Проверка важных областей, а также для пользовательских задач проверки по требованию.

По умолчанию задачи проверки по требованию проверяют все объекты файловой системы компьютера. Если по требованиям к безопасности нет необходимости проверять все объекты файловой системы, вы можете ограничить область проверки.

В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 область проверки представляет собой список или дерево файловых ресурсов компьютера, которые программа может контролировать. По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.

► *Чтобы включить отображение файловых ресурсов компьютера в виде дерева,*

в раскрывающемся списке, расположенном в левом верхнем углу окна **Настройка области защиты**, выберите пункт **Показывать в виде дерева**.

Узлы в дереве или списке файловых ресурсов компьютера отображаются следующим образом:

 Узел включен в область проверки.

 Узел исключен из области проверки.

 По крайней мере один из узлов, вложенных в этот узел, исключен из области проверки, или параметры безопасности вложенных узлов отличаются от параметров безопасности этого узла (только для режима отображения в виде дерева).

Значок  отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области проверки для выбранного вложенного узла.

Имена виртуальных узлов области проверки отображаются шрифтом синего цвета.

Настройка параметров отображения сетевых файловых ресурсов

► *Чтобы выбрать способ отображения файловых ресурсов компьютера при настройке параметров области проверки, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 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 **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В левом верхнем углу открывшегося окна разверните раскрывающийся список. Выполните одно из следующих действий:
   - Выберите пункт **Показывать в виде дерева**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде дерева.
   - Выберите пункт **Показывать в виде списка**, если вы хотите, чтобы файловые ресурсы защищаемого компьютера отображались в виде списка.

   По умолчанию файловые ресурсы защищаемого компьютера отображаются в виде списка.
5. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут применены.

Предопределенные области проверки

Дерево или список файловых ресурсов компьютера отображается в панели результатов узла выбранной задачи проверки по требованию по ссылке Настроить область проверки.

Дерево или список файловых ресурсов отображает узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Industrial CyberSecurity for Nodes 2.5 предусмотрены следующие предопределенные области проверки:

- **Мой компьютер**. Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет весь компьютер.
- **Локальные жесткие диски**. Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты на жестких дисках компьютера. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.

- **Съемные диски**. Kaspersky Industrial CyberSecurity for Nodes 2.5 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.
- **Сетевое окружение**. Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, которую вы используете для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются под системной учетной записью.
- **Системная память**. Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.
- **Объекты автозапуска**. Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM. SYSTEM.INI, а также программные модули программ, которые автоматически запускаются при старте компьютера.
- **Папки общего доступа**. Вы можете включать в область проверки папки общего доступа на защищаемом компьютере.
- **Виртуальные диски**. Вы можете включать в область проверки динамические диски, папки и файлы, а также диски, которые монтируются на компьютер, например, общие диски кластера.

Предопределенные области проверки по умолчанию отображаются в дереве файловых ресурсов компьютера и доступны для добавления в список 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:
  - **Локальные жесткие диски**
  - **Съемные диски**
  - **Системная память**
- Задача Проверка важных областей:
  - **Локальные жесткие диски** (исключая папки Windows);
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
- Пользовательские задачи проверки по требованию:
  - **Локальные жесткие диски** (исключая папки Windows);
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
  - **Папки общего доступа**

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов компьютера в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5. Чтобы проверить объекты на псевдодиске, включите в область проверки папку на компьютере, с которой этот псевдодиск связан.
Подключенные сетевые диски также не отображаются в дереве файловых ресурсов компьютера. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Формирование области проверки

Если вы управляете Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере удаленно через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, установленную на рабочем месте администратора, вы должны входить в группу администраторов на защищаемом компьютере, чтобы просматривать папки на нем.

Названия параметров могут отличаться в разных операционных системах Windows.

Если вы измените область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, вы можете восстановить область проверки по умолчанию в этих задачах, выполнив восстановление Kaspersky Industrial CyberSecurity for Nodes 2.5 (**Пуск** > **Все программы** > **Kaspersky Industrial CyberSecurity for Nodes 2.5** > **Изменение или удаление Kaspersky Industrial CyberSecurity for Nodes**). В мастере установки установите флажок **Восстановить рекомендуемые параметры работы программы**.

Процедура формирования области проверки в задачах проверки по требованию зависит от типа отображения файловых ресурсов защищаемого компьютера (см. раздел "Настройка параметров отображения файловых ресурсов области защиты" на стр. 204). Вы можете настроить отображение файловых ресурсов в виде списка (применяется по умолчанию) или в виде дерева.

► *Чтобы сформировать область проверки, работая с деревом файловых ресурсов, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 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 **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В правой части открывшегося окна разверните дерево файловых ресурсов компьютера, чтобы отобразить все узлы.
5. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:

- если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с именем нужного типа дисков (например, чтобы включить все съемные диски на компьютере, установите флажок **Съемные диски**);
- если вы хотите включить в область защиты отдельный диск нужного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**.
- если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.

6. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

► *Чтобы сформировать область защиты, работая со списком файловых ресурсов, выполните следующие действия*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 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 **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область проверки**.
   c. В открывшемся окне **Добавление области проверки** выберите тип объекта, который вы хотите добавить в область проверки:
      - **Предопределенная область**, если вы хотите включить в область проверки одну из предопределнный областей на защищаемом компьютере. Затем в раскрывающемся списке выберите необходимую область.
      - **Диск, папка или сетевой объект**, если вы хотите включить в область проверки отдельный диск, папку или сетевой объект нужного типа. Затем выберите необходимый файл по кнопке **Обзор**.
      - **Файл**, если вы хотите включить в область проверки только отдельный файл на диске. Затем выберите необходимый файл по кнопке **Обзор**.

   Вы не можете добавить объект в область проверки, если он уже добавлен в качестве исключения из области защиты.
5. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В открывшемся окне **Добавление исключения** выберите тип объекта, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.

6. Чтобы изменить добавленную область проверки или исключение, в контекстном меню области, которую хотите изменить, выберите пункт **Изменить область**.
7. Чтобы скрыть отображение ранее добавленной области проверки или исключения в списке файловых ресурсов, в контекстном меню области, которую хотите скрыть, выберите пункт **Удалить из списка**.

   Область проверки исключается из области действия задачи проверки по требованию при ее удалении из списка файловых ресурсов.

8. Нажмите на кнопку **Сохранить**.

Окно Настройка области проверки будет закрыто. Настроенные параметры задачи будут сохранены.

Включение в область проверки сетевых объектов

Вы можете включать в область проверки сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы не можете сканировать сетевые папки при работе под системной учетной записью.

► *Чтобы добавить в область проверки сетевой объект, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. Выберите задачу **проверки по требованию**, в область проверки которой вы хотите добавить сетевой путь.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. В контекстном меню названия узла **Сетевое окружение** выполните следующие действия:
   - Выберите пункт **Добавить сетевую папку**, если вы хотите добавить сетевую папку в область проверки.
   - Выберите пункт **Добавить сетевой файл**, если вы хотите добавить сетевой файл в область проверки.
6. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **ENTER**.
7. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область проверки.
8. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
9. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Создание виртуальной области проверки

Вы можете включать в область проверки динамические диски, папки и файлы – создавать виртуальную область проверки.

Вы можете добавить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов (см. раздел "Настройка параметров отображения файловых ресурсов области защиты" на стр. 204).

► *Чтобы добавить в область проверки виртуальный диск, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 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 **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. В дереве файловых ресурсов компьютера откройте контекстное меню на узле **Виртуальные диски** и в списке доступных имен выберите имя для создаваемого виртуального диска.
6. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.
7. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

► *Чтобы добавить в область проверки виртуальную папку или виртуальный файл, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, в которой вы хотите создать виртуальную область проверки.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
5. В дереве файловых ресурсов компьютера откройте контекстное меню диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, если хотите добавить виртуальную папку в область защиты.
   - **Добавить виртуальный файл**, если хотите добавить виртуальный файл в область защиты.
6. В поле ввода задайте имя для папки или файла.

   Указывая имя файла, вы можете задать его маску с помощью специальных символов * и ?.
7. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область проверки.
8. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Параметры безопасности выбранного узла в задачах проверки по требованию

В выбранной задаче проверки по требованию вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области защиты или проверки, так и различными для разных узлов в дереве или списке файловых ресурсов компьютера.

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 или проверки одним из следующих способов:

- выбрать один из трех предустановленных уровней безопасности (**Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**);
- вручную изменить параметры безопасности для выбранных узлов в дереве или списке файловых ресурсов компьютера (уровень безопасности примет значение **Другой**).

Вы можете сохранить набор параметров узла в шаблон, чтобы потом применять этот шаблон для других узлов.

Выбор предустановленных уровней безопасности в задачах проверки по требованию

Для выбранного узла в дереве файловых ресурсов компьютера вы можете задать один из трех предустановленных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**. Каждый из этих уровней имеет свой набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, кроме использования Kaspersky Industrial CyberSecurity for Nodes 2.5 на компьютерах и рабочих станциях, принимаются дополнительные меры компьютерной безопасности, например сетевые экраны и политики безопасности для пользователей сети.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность защищаемых компьютеров. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты компьютеров в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если вы предъявляете повышенные требования к компьютерной безопасности в сети организации.

Таблица 34. Предустановленные уровни безопасности и соответствующие им значения

параметров безопасности

Параметры	Уровень безопасности		
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**
Проверка объектов	По формату	Все объекты.	Все объекты.
Проверка только новых и измененных файлов	Включена	Выключено	Выключено
Действия над зараженными и другими обнаруженными объектами	Лечить. Удалить, если не удалось вылечить.	Выполнять рекомендованное действие (Лечить. Удалить, если не удалось вылечить.)	Лечить. Удалить, если не удалось вылечить.
Действия над возможно зараженными объектами	Карантин	Выполнять рекомендованное действие (Поместить на карантин)	Карантин
Исключать файлы	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.).	60 сек.	Нет	Нет
Не проверять составные объекты размером более (МБ).	8 МБ	Нет	Нет
Альтернативные потоки NTFS	Да	Да	Да
Проверять загрузочные секторы дисков и MBR.	Да	Да	Да
Проверять составные объекты	• SFX-архивы* • упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• Архивы* • SFX-архивы* • упакованные объекты* • Вложенные OLE-объекты* * Все объекты	• Архивы* • SFX-архивы* • почтовые базы* • файлы почтовых форматов* • упакованные объекты* • Вложенные OLE-объекты* * Все объекты

Параметры безопасности: **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов** – не входят в набор параметров предустановленных уровней безопасности. Если вы измените состояние параметров **Использовать технологию iChecker**, **Использовать технологию iSwift**, или **Использовать эвристический анализатор**, выбранный вами предустановленный уровень безопасности не изменится.

► *Чтобы выбрать один из предустановленных уровней безопасности, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 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 **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В дереве или в списке файловых ресурсов компьютера выберите узел, для которого вы хотите выбрать предустановленный уровень безопасности.
5. Убедитесь, что выбранный узел включен в область проверки.
6. В правой части окна на закладке **Уровень безопасности** выберите уровень безопасности, который вы хотите применить.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.
7. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки. Эти параметры соответствуют значениям предустановленного уровня безопасности **Рекомендуемый**.

Вы можете изменять значения параметров безопасности по умолчанию, настроив их как едиными для всей области защиты, так и различными для разных узлов в дереве или списке файловых ресурсов компьютера.

При работе с деревом файловых ресурсов компьютера 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.

► *Чтобы настроить параметры безопасности вручную, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 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 **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.
4. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.

   Предопределенный шаблон с параметрами безопасности (см. раздел "О шаблонах параметров безопасности" на стр. 69) можно применить к выбранному узлу в области проверки.
5. Настройте нужные параметры безопасности выбранного узла в соответствии с вашими требованиями. Для этого выполните следующие действия:

- Общие параметры (см. раздел "Настройка общих параметров задачи" на стр. 213)
- Действия (см. раздел "Настройка действий" на стр. 215)
- Производительность (см. раздел "Настройка производительности" на стр. 217)

6. Нажмите кнопку **Сохранить** в окне **Настройка области проверки**.

Новые параметры области защиты будут сохранены.

Настройка общих параметров задачи

► *Чтобы настроить общие параметры безопасности задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "Настройка параметров безопасности вручную" на стр. 212).
2. Выберите закладку **Общие**.
3. В блоке **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:
   - **Объекты проверки**
     - **Все объекты.**

       Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет все объекты.
     - **Объекты, проверяемые по формату.**

       Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5.
     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах.**

       Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет только потенциально заражаемые файлы на основании формата файла.

       Список расширений составляется специалистами "Лаборатории Касперского". Он входит в состав баз Kaspersky Industrial CyberSecurity for Nodes 2.5.
     - **Объекты, проверяемые по указанному списку расширений.**

       Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы на основании расширения файла. Список расширений файлов, которые нужно проверять, вы можете задать вручную по кнопке **Изменить** в окне **Список расширений**.
   - **Проверять загрузочные секторы дисков и MBR.**

     Включение защиты загрузочных секторов дисков и главных загрузочных записей.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет загрузочные секторы и загрузочные надписи на жестких и съемных дисках компьютера.

     По умолчанию флажок установлен.
   - **Альтернативные потоки NTFS**

Проверка дополнительных потоков файлов и папок на дисках файловой системы NTFS.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет дополнительные потоки файлов и папок.

По умолчанию флажок установлен.

4. В блоке **Производительность** установите или снимите флажок **Проверять только новые и измененные файлы**.

   Флажок включает или выключает проверку и защиту файлов, признанных Kaspersky Industrial CyberSecurity for Nodes 2.5 новыми или измененными с момента последней проверки.

   Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет и защищает только файлы, признанные новыми или измененными с момента последней проверки.

   Если флажок снят, вы можете указать, какие файлы вы хотите проверять и защищать.

   По умолчанию флажок установлен для уровня безопасности **Максимальное быстродействие**. Если установлен уровень безопасности **Рекомендуемый** или **Максимальная защита**, то флажок снят.

> Для переключения между доступными вариантами при снятом флажке щелкните ссылку **Все** / **Только новые** для каждого типа составных объектов.

5. В блоке **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

   - **Все / Только новые архивы.**

     Проверка архивов ZIP, CAB, RAR, ARJ и других форматов.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет архивы.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

   - **Все / Только новые SFX-архивы.**

     Проверка самораспаковывающихся архивов.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет SFX-архивы.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает SFX-архивы при проверке.

     Значение по умолчанию зависит от выбранного уровня безопасности.

     Параметр активен, если снят флажок **Архивы**.

   - **Все / Только новые почтовые базы.**

     Проверка файлов почтовых баз Microsoft Outlook и Microsoft Outlook Express.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы почтовых баз.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает файлы почтовых баз при проверке.

Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые упакованные объекты.**

  Проверка исполняемых файлов, упакованных программами-упаковщиками двоичного кода, такими как UPX или ASPack.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет исполняемые файлы, упакованные программами-упаковщиками.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 при проверке пропускает исполняемые файлы, упакованные программами-упаковщиками.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые файлы почтовых форматов.**

  Проверка файлов почтовых форматов, например, сообщения форматов Microsoft Outlook и Microsoft Outlook Express.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы почтовых форматов.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает файлы почтовых форматов при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

- **Все / Только новые вложенные OLE-объекты.**

  Проверка встроенных в файл объектов (например, макрос Microsoft Word или вложение сообщения электронной почты).

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет встроенные в файл объекты.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает встроенные в файл объекты при проверке.

  Значение по умолчанию зависит от выбранного уровня безопасности.

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

► *Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "Настройка параметров безопасности вручную" на стр. 212).
2. Выберите закладку **Действия**.

3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**.

     Когда выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется событие *Обнаруженный объект не вылечен согласно пользовательским параметрам задачи*. В событии указана вся доступная информация об обнаруженном объекте, а также тот факт, что объект не был вылечен.

     Режим **Только сообщать** требуется отдельно настроить для каждой области защиты. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выберете этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически изменит уровень безопасности на **Пользовательский**.
   - **Лечить.**
   - **Лечить. Удалить, если не удалось вылечить.**
   - **Удалить**.
   - **Выполнять рекомендованное действие**.
4. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**.

     Когда выбран этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 не блокирует доступ к зараженному или другому обнаруженному объекту и не выполняет над ним никаких действий. В журнале выполнения задачи регистрируется событие *Обнаруженный объект не вылечен согласно пользовательским параметрам задачи*. В событии указана вся доступная информация об обнаруженном объекте, а также тот факт, что объект не был вылечен.

     Режим **Только сообщать** требуется отдельно настроить для каждой области защиты. Этот режим не используется по умолчанию ни на одном из уровней безопасности. Если вы выберете этот режим, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически изменит уровень безопасности на **Пользовательский**.
   - **Поместить на карантин**.
   - **Удалить**.
   - **Выполнять рекомендованное действие**.
5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

      Если флажок установлен, вы можете выбрать основное и дополнительное действие для каждого типа объектов, нажав на кнопку **Настройка**, расположенную рядом с флажком.

      Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 применяет действия, которые выбраны в блоках **Действия над зараженными и другими обнаруженными объектами** и **Действия над возможно зараженными объектами** соответственно указанным типам объектов.

      По умолчанию флажок снят.

a. Нажмите на кнопку **Настройка**.

b. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.

c. Нажмите на кнопку **OK**.

6. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл неизменяем**.

   Флажок включает или выключает форсированное удаление родительского составного файла при обнаружении вложенного вредоносного, возможно зараженного или другого обнаруживаемого объекта.

   Если флажок установлен и задача настроена на удаление зараженных или возможно зараженных объектов, Kaspersky Industrial CyberSecurity for Nodes 2.5 принудительно удаляет весь родительский составной файл при обнаружении вредоносного или другого вложенного объекта. Принудительное удаление составного объекта со всем его содержимым выполняется в случае, если программа не может удалить только вложенный обнаруженный объект (например, если составной объект неизменяем).

   Если флажок снят и задача настроена на удаление зараженных и возможно зараженных объектов, Kaspersky Industrial CyberSecurity for Nodes 2.5 не выполняет выбранное действие, если родительский объект неизменяем.

   По умолчанию установлен флажок для уровня безопасности **Максимальная защита** и сняты флажки **Рекомендуемый** и **Максимальное быстродействие**.

7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

► *Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:*

1. Откройте окно **Настройка области проверки** (см. раздел "Настройка параметров безопасности вручную" на стр. 212).
2. Выберите закладку **Производительность**.
3. В блоке **Исключения**:
   - Снимите или установите флажок **Исключать файлы**.

     Исключение файлов из проверки по имени файла или маске имени файла.

     Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке указанные объекты.

     Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет все объекты.

     По умолчанию флажок снят.

   - Снимите или установите флажок **Не обнаруживать**.

Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта. Вы можете найти список имен обнаруживаемых объектов на сайте Вирусной энциклопедии.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при проверке указанные объекты.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 обнаруживает все объекты, указанные в программе по умолчанию.

По умолчанию флажок снят.

- Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

4. В блоке **Дополнительные параметры**:

- **Останавливать проверку, если она длится более (сек.).**

  Ограничение времени проверки объекта. По умолчанию установлено значение 60 сек.

  Если флажок установлен, максимальная продолжительность проверки объекта ограничена указанным значением.

  Если флажок снят, максимальная продолжительность проверки не ограничена.

  По умолчанию флажок установлен.

- **Не проверять составные объекты размером более (МБ).**

  Исключение из проверки составных объектов больше указанного размера.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 пропускает при антивирусной проверке составные объекты, чей размер превышает установленное значение.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет составные объекты, не учитывая размер.

  По умолчанию флажок установлен для уровней безопасности **Рекомендуемый** и **Максимальное быстродействие**.

- **Использовать технологию iSwift.**

  Проверка только новых или измененных с момента последней проверки объектов файловой системы NTFS.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет только новые или изменившиеся с момента последней проверки объекты файловой системы NTFS.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет объекты файловой системы NTFS, не учитывая дату создания и изменения.

  По умолчанию флажок установлен.

- **Использовать технологию iChecker.**

  Проверка только новых или измененных с момента последней проверки файлов.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет только новые или изменившиеся с момента последней проверки файлы.

  Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет файлы, не учитывая дату создания и изменения.

По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Проверка съёмных дисков

Вы можете настроить проверку съёмных дисков, подключаемых по USB к защищаемому компьютеру.

Kaspersky Industrial CyberSecurity for Nodes 2.5 выполняет проверку съемного диска с помощью задачи проверки по требованию. Программа автоматически создает новую задачу Проверка по требованию в момент подключения съёмного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется с предустановленным уровнем безопасности, указанным для проверки съёмных дисков. Вы не можете настроить параметры временной задачи Проверка по требованию.

Kaspersky Industrial CyberSecurity for Nodes запускает проверку съёмных дисков, подключаемых по USB при их регистрации в операционной системе в качестве запоминающего устройства (USB Mass Storage Device). Программа не выполняет проверку съёмного диска, если его подключение было заблокировано задачей Контроль устройств. Программа не выполняет проверку MTP-подключаемых мобильных устройств.

Kaspersky Industrial CyberSecurity for Nodes 2.5 не блокирует доступ к съёмному диску на время проверки.

Результаты проверки каждого съёмного диска доступны в журнале выполнения задачи Проверка по требованию, созданной при подключении этого диска.

Вы можете изменять значения параметров компонента Проверка съёмных дисков (см.таблицу ниже).

Таблица 35. Параметры проверки съёмных дисков

Параметр	Значение по умолчанию	Описание
Проверять съёмные диски при их подключении по USB	Флажок снят	Вы можете включать или выключать проверку съёмных дисков при их подключении к защищаемому компьютеру.
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	1024 МБ	Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на съёмном диске. Kaspersky Industrial CyberSecurity for Nodes 2.5 не будет выполнять проверку съёмного диска, если объем содержащихся на нем данных превышает указанное значение.

Параметр	Значение по умолчанию	Описание
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 Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют предустановленным уровням безопасности в задачах проверки по требованию.

► *Чтобы настроить параметры проверки съёмных дисков при подключении, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Kaspersky Industrial CyberSecurity for Nodes** и выберите пункт **Настроить проверку съемных дисков**.

   Откроется окно **Проверка съёмных дисков**.

2. В блоке **Параметры проверки при подключении** выполните следующие действия:

   - Установите флажок **Проверять съёмные диски при их подключении по USB**, если вы хотите, чтобы Kaspersky Industrial CyberSecurity for Nodes автоматически выполнял проверку съёмных дисков при подключении.
   - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (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 съёмных дисков.

3. Нажмите на кнопку **OK**.

   Настроенные параметры будут сохранены и применены.

Создание задачи проверки по требованию

Вы можете создавать пользовательские задачи в узле **Проверка по требованию**. В других функциональных компонентах Kaspersky Industrial CyberSecurity for Nodes 2.5 создание пользовательских задач не предусмотрено.

► *Чтобы создать новую задачу проверки по требованию, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Проверка по требованию**.
2. Выберите пункт **Добавить задачу**.

   Откроется окно **Добавить задачу**.

3. Введите следующую информацию о задаче:

- **Имя** – название задачи, не более 100 символов, может содержать любые символы, кроме **% ? \ | / : * < > "**.

  Вы не можете сохранить новую задачу или перейти к настройке параметров новой задачи на закладках **Расписание**, **Дополнительно** и **Запуск с правами**, если не задано имя задачи.

- **Описание** – любая дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в окне свойств задачи.

4. Если требуется, настройте следующие параметры задачи:
   - На закладке **Общие**:
     - **Использовать эвристический анализатор**

       Флажок включает или выключает использование эвристического анализатора при проверке объектов.

       Если флажок установлен, эвристический анализатор включен.

       Если флажок снят, эвристический анализатор выключен.

       По умолчанию флажок установлен.

     - **Выполнять задачу в фоновом режиме.**

       Флажок изменяет приоритет задачи.

       Если флажок установлен, приоритет задачи в операционной системе снижается. Операционная система предоставляет ресурсы для выполнения задачи в зависимости от нагрузки на центральный процессор и файловую систему компьютера со стороны других задач Kaspersky Industrial CyberSecurity for Nodes 2.5 и программ. Как следствие, скорость выполнения задачи замедляется при увеличении нагрузки и увеличивается при уменьшении нагрузки.

       Если флажок снят, задача выполняется с тем же приоритетом, что и остальные задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 и другие программы. В этом случае скорость выполнения задачи увеличивается.

       По умолчанию флажок снят.

     - **Применять доверенную зону.**

       Флажок включает или выключает применение доверенной зоны в работе задачи.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes не учитывает файловые операции доверенных процессов при формировании области защиты в задаче Постоянная защита файлов.

       По умолчанию флажок установлен.

     - **Считать выполнение задачи проверкой важных областей.**

Флажок изменяет приоритет задачи: включает или выключает регистрацию события *Выполнена проверка важных областей* и обновление статуса защиты компьютера. Kaspersky Security Center оценивает безопасность компьютера (компьютеров) по показателям производительности задачи и присваивает статус *Проверка важных областей*. Флажок недоступен в свойствах локальных системных и пользовательских задач Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете изменять значение этого параметра только на стороне Kaspersky Security Center.

Если флажок установлен, Сервер администрирования регистрирует событие Выполнена проверка важных областей и обновляет статус защиты компьютера по результатам выполнения задачи. Задача проверки имеет высокий приоритет.

Если флажок снят, задача проверки выполняется с низким приоритетом.

Флажок установлен по умолчанию для задачи Проверка важных областей.

- **Использовать KSN для проверки.**

  Флажок включает или выключает использование облачных служб Kaspersky Security Network (KSN) в задаче.

  Если флажок установлен, программа использует данные, полученные от служб KSN, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний.

  Если флажок снят, задача постоянной защиты файлов не использует службы KSN.

  По умолчанию флажок установлен.

- На закладках **Расписание** и **Дополнительно**:
  - Параметры запуска задачи запуск расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 62)
- На закладке **Запуск с правами**:
  - Параметры запуск задачи с правами учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 65)

5. В окне **Параметры задачи** нажмите на кнопку **ОК**.

   Новая пользовательская задача проверки по требованию будет создана. Узел с названием новой задачи будет отображен в дереве Консоли. Операция регистрируется в журнале системного аудита (на стр. 259).

6. Если требуется, в панели результатов выбранного узла откройте закладку **Настройка области проверки**.

   Выполните следующие действия:

   - В дереве файловых ресурсов компьютера выберите узлы, которые хотите включить в область проверки.
   - Выберите один из предустановленных уровней безопасности (см. раздел "Выбор предустановленных уровней безопасности в задачах проверки по требованию" на стр. 210) или настройте параметры проверки вручную (см. раздел "Настройка параметров безопасности вручную" на стр. 93).

7. В контекстном меню названия выбранной задачи выберите пункт **Сохранить задачу**.

Пользовательская задача проверки по требованию будет создана. Настроенные параметры будут применены при последующем запуске задачи.

Удаление задачи

В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете удалять только пользовательские задачи проверки по требованию. Вы не можете удалять системные или групповые задачи.

► *Чтобы удалить задачу, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. Откройте контекстное меню названия пользовательской задачи, которую вы хотите удалить.
3. Выберите пункт **Удалить задачу**.

   Откроется окно подтверждения операции.
4. Нажмите на кнопку **Да**, чтобы подтвердить операцию удаления.

Задача будет удалена, операция удаления будет зарегистрирована в журнале системного аудита.

Переименование задачи

В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете переименовывать только пользовательские задачи. Вы не можете переименовывать системные или групповые задачи.

► *Чтобы переименовать задачу, выполните следующие действия:*

1. В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Проверка по требованию**.
2. Откройте контекстное меню названия пользовательской задачи, которую вы хотите переименовать.
3. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне введите новое имя задачи в поле **Имя**.
5. Нажмите на кнопку **OK**.

Задача будет переименована. Операция будет зарегистрирована в журнале системного аудита.

Обновление баз и модулей Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Industrial CyberSecurity for Nodes 2.5, копировании обновлений и откате обновлений баз Kaspersky Industrial CyberSecurity for Nodes 2.5, а также инструкции по настройке задач обновления баз и модулей программы.

В этом разделе

О задачах обновления

Kaspersky Industrial CyberSecurity for Nodes 2.5 предоставляет четыре задачи обновления системы: Обновление баз программы, Обновление модулей программы, Копирование обновлений и Откат обновления баз программы.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 соединяется с источником обновлений – одним из серверов обновлений "Лаборатории Касперского". Вы можете настраивать все задачи обновления (см. раздел "Настройка задач обновления" на стр. 230), кроме задачи Откат обновления баз программы. После того как вы измените параметры задачи, Kaspersky Industrial CyberSecurity for Nodes 2.5 применит их новые значения при следующем запуске задачи.

Вы не можете приостанавливать и возобновлять задачи обновления.

Обновление баз программы

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 копирует базы из источника обновлений на защищаемый компьютер и сразу переходит к их использованию в выполняющейся задаче постоянной защиты. Задачи проверки по требованию переходят к использованию обновленных баз программы при последующем их запуске.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 запускает задачу Обновление баз программы ежечасно.

Обновление модулей программы

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 проверяет доступность обновления модулей программы на источнике обновлений. Для применения установленных программных модулей требуется перезагрузка компьютера и / или перезапуск Kaspersky Industrial CyberSecurity for Nodes 2.5.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого компьютера). В ходе выполнения задачи программа проверяет наличие важных и плановых обновлений модулей Kaspersky Industrial CyberSecurity for Nodes 2.5, не копируя их.

Копирование обновлений

По умолчанию в ходе выполнения задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 загружает файлы обновлений баз и сохраняет их в указанную сетевую или локальную папку, не устанавливая их.

По умолчанию задача Копирование обновлений не выполняется.

Откат обновления баз программы

В ходе выполнения задачи Kaspersky Industrial CyberSecurity for Nodes 2.5 возвращается к использованию баз программы с ранее установленными обновлениями.

По умолчанию задача Откат обновления баз программы не выполняется.

Об обновлении программных модулей Kaspersky Industrial CyberSecurity for Nodes 2.5

"Лаборатория Касперского" может выпускать пакеты обновлений модулей Kaspersky Industrial CyberSecurity for Nodes 2.5. Пакеты обновлений делятся на *срочные* (или *критические*) и плановые. Срочные пакеты обновлений устраняют уязвимости и ошибки; плановые добавляют новые функции или улучшают существующие.

Срочные пакеты обновлений публикуются на серверах обновлений "Лаборатории Касперского". Вы можете настроить их автоматическую установку с помощью задачи Обновление модулей программы. По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого компьютера).

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматизированной установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете получать информацию о выходе плановых обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5 с помощью задачи Обновление модулей программы.

Вы можете загружать срочные обновления из интернета на каждый защищаемый компьютер или использовать один компьютер в качестве посредника, копируя обновления на него без их установки, а затем распределяя их на компьютеры защищаемой сети. Чтобы копировать и сохранять обновления без их установки, используйте задачу Копирование обновлений.

Перед тем как установить обновления модулей, Kaspersky Industrial CyberSecurity for Nodes 2.5 создает резервные копии модулей, установленных ранее. Если обновление модулей программы прервется или завершится с ошибкой, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически вернется к использованию ранее установленных программных модулей. Вы также можете откатить обновление модулей вручную до предыдущих установленных обновлений.

На время установки полученных обновлений служба Kaspersky Security автоматически останавливается, а затем снова запускается.

Об обновлении баз Kaspersky Industrial CyberSecurity for Nodes 2.5

Базы Kaspersky Industrial CyberSecurity for Nodes 2.5, хранящиеся на защищаемом компьютере, быстро становятся неактуальными. Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают сотни новых угроз, создают идентифицирующие их записи и включают их в обновления баз программы. Обновление баз представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента создания предыдущего обновления. Чтобы свести риск заражения компьютера к минимуму, регулярно получайте обновления баз.

По умолчанию, если базы Kaspersky Industrial CyberSecurity for Nodes 2.5 не обновляются в течение недели с момента создания последних установленных обновлений баз, возникает событие *Базы программы устарели.* Если базы программы не обновляются в течение двух недель, возникает событие *Базы программы сильно устарели*. Информация об актуальности баз (см. раздел "Просмотр состояния защиты и информации о Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 33) отображается в панели результатов узла **Kaspersky Industrial CyberSecurity for Nodes** дерева Консоли. Вы можете использовать общие параметры Kaspersky Industrial CyberSecurity for Nodes 2.5, чтобы указать другое количество дней до возникновения этих событий. Вы также можете настроить уведомления для администратора об этих событиях (см. раздел "Настройка уведомлений администратора и пользователей" на стр. 274).

Kaspersky Industrial CyberSecurity for Nodes загружает обновления баз и модулей программы с FTP или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или других источников обновлений.

Вы можете загружать обновления на каждый защищаемый компьютер или использовать один компьютер в качестве посредника, копируя обновления на него и затем распределяя их на компьютеры. Если вы используете программу Kaspersky Security Center для централизованного управления защитой компьютеров в организации, вы можете использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Вы можете запускать задачи обновления баз вручную или по расписанию (см. раздел "Настройка параметров расписания запуска задач" на стр. 62). По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 запускает задачу Обновление баз программы ежечасно.

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 2.5 вы можете сами откатить базы до ранее установленных обновлений (см. раздел "Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 236).

Схемы обновления баз и модулей антивирусных программ в организации

Ваш выбор источника обновлений в задачах обновления зависит от того, какую схему обновления баз и модулей антивирусных программ вы используете в организации.

Вы можете обновлять базы и модули Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемых компьютерах по следующим схемам:

- загружать обновления напрямую из интернета на каждый защищаемый компьютер (схема 1);
- загружать обновления из интернета на компьютер-посредник и распределять обновления на компьютеры с этого компьютера.

Посредником может служить любой компьютер, на котором установлена одна из следующих программ:

- Kaspersky Industrial CyberSecurity for Nodes 2.5 (один из защищаемых компьютеров) (схема 2);
- Сервер администрирования Kaspersky Security Center (схема 3).

Обновление через компьютер-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность компьютеров сети..

Перечисленные схемы обновлений описаны ниже.

Схема 1. Обновление напрямую из интернета

При использовании данного способа обновлений программа выходит из сертифицированного состояния.

► *Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5 напрямую из интернета,*

на каждом защищаемом компьютере в настройках параметров задач Обновление баз программы и Обновление модулей программы в качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".

Вы можете указать в качестве источника обновлений другие HTTP- или FTP-серверы, которые содержат папку с файлами обновлений.

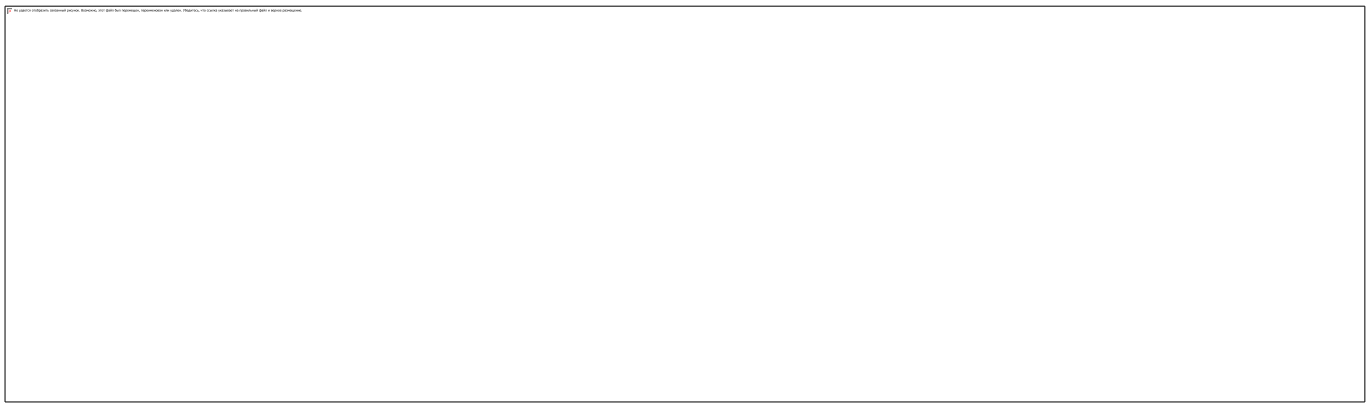


Схема 2. Обновление через один из защищаемых компьютеров

► *Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5 через один из защищаемых компьютеров, выполните следующие действия:*

1. Скопируйте обновления на выбранный защищаемый компьютер. Для этого выполните следующие действия:
   - На выбранном компьютере настройте параметры задачи Копирование обновлений:
     a. В качестве источника обновлений укажите компьютеры обновлений «Лаборатории Касперского».
     b. Укажите папку общего доступа в качестве папки, в которой будут сохранены обновления.

2. Распределите обновления на остальные защищаемые компьютеры. Для этого выполните следующие действия:

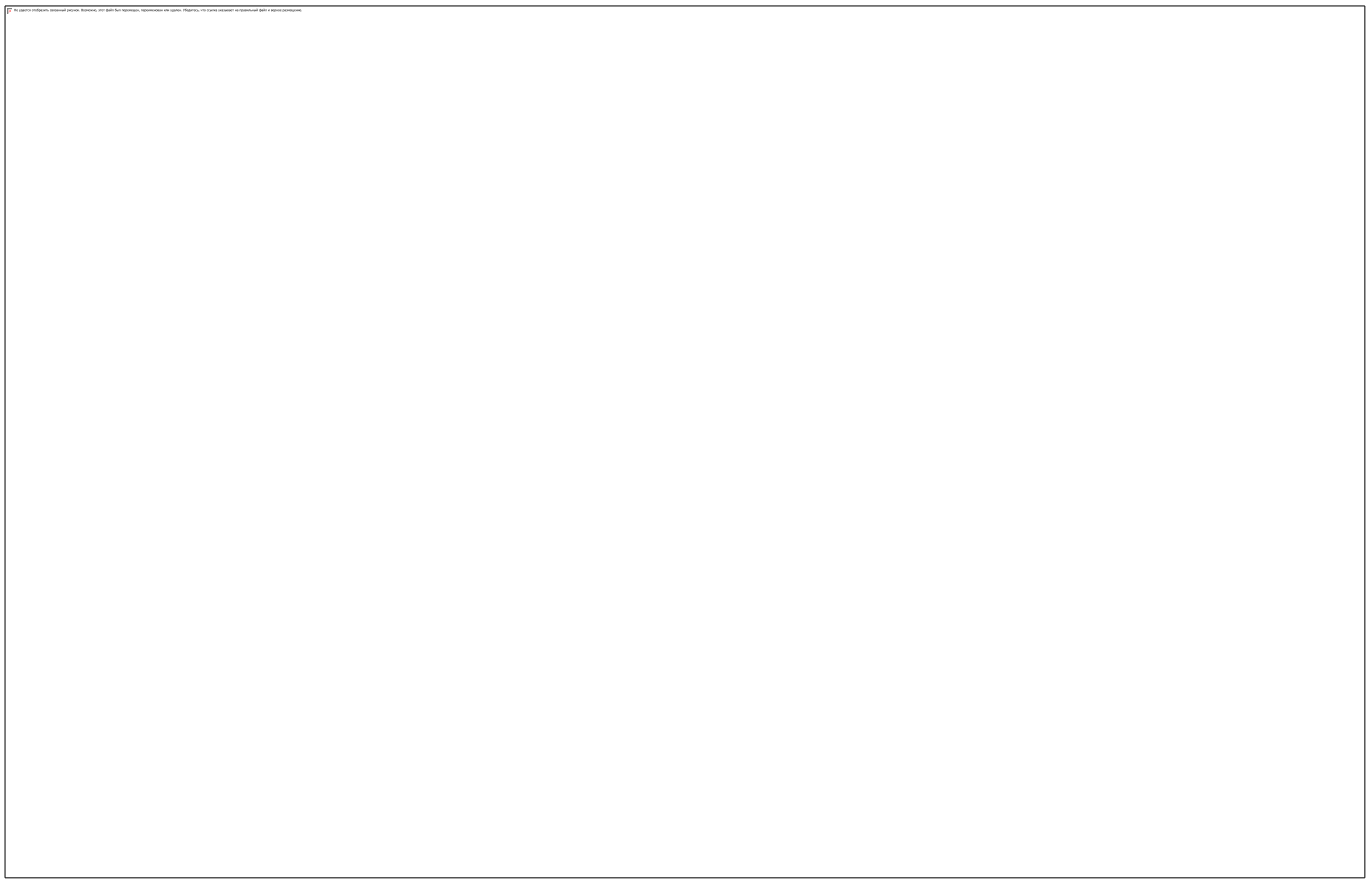
   - На каждом из защищаемых компьютеров настройте параметры задач Обновление баз программы и Обновление модулей программы (см. рис. ниже):

     a. В качестве источника обновлений укажите папку на диске компьютера-посредника, в которую вы скопировали обновления.

Kaspersky Industrial CyberSecurity for Nodes 2.5 будет получать обновления через один из защищаемых компьютеров.

Схема 3. Обновление через Сервер администрирования Kaspersky Security Center

Если вы используете программу Kaspersky Security Center для централизованного управления защитой компьютеров, вы можете загружать обновления через Сервер администрирования Kaspersky Security Center (см. рис. ниже).



► *Чтобы настроить получение обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5 через Сервер администрирования Kaspersky Security Center, выполните следующие действия:*

1. Загрузите обновления с сервера обновлений "Лаборатории Касперского" на Сервер администрирования Kaspersky Security Center. Для этого выполните следующие действия:
   - Настройте задачу Получение обновлений Сервером администрирования для указанного набора компьютеров:
     a. В качестве источника обновлений укажите серверы обновлений «Лаборатории Касперского».
2. Распределите обновления на защищаемые компьютеры. Для этого выполните одно из следующих действий:
   - Настройте на Сервере администрирования Kaspersky Security Center групповую задачу обновления для распределения обновлений на защищаемые компьютеры:
     a. В расписании задачи укажите частоту запуска **После получения обновлений Сервером администрирования**.

        Сервер администрирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым).

Вы не можете указывать частоту запуска задачи После получения обновлений Сервером администрирования в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

- Настройте на каждом из защищаемых компьютеров задачи Обновление баз программы и Обновление модулей программы:
  a. В качестве источника обновлений укажите Сервер администрирования Kaspersky Security Center.
  b. Если требуется, настройте расписание задачи.

При редких обновлениях антивирусных баз Kaspersky Industrial CyberSecurity for Nodes 2.5 (от одного раза в месяц до одного раза в год) вероятность обнаружения угроз снижается, повышается частота ложных срабатываний компонентов программы.

Kaspersky Industrial CyberSecurity for Nodes 2.5 будет получать обновления через Сервер администрирования Kaspersky Security Center.

Если вы планируете использовать Сервер администрирования Kaspersky Security Center для распределения обновлений, предварительно установите на каждом из защищаемых компьютеров программный компонент Агент администрирования, который входит в комплект поставки программы Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Industrial CyberSecurity for Nodes 2.5 на защищаемом компьютере. Подробная информация об Агенте администрирования и его настройке с помощью программы Kaspersky Security Center содержится в *Руководстве администратора Kaspersky Security Center*.

Настройка задач обновления

Этот раздел содержит инструкции по настройке задач обновления Kaspersky Industrial CyberSecurity for Nodes 2.5.

В этом разделе

Настройка параметров работы с источниками обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5

Для каждой задачи обновления, кроме задачи Откат обновления баз программы, вы можете указать один или несколько источников обновлений, добавить пользовательские источники обновлений и настроить параметры соединения с указанными источниками обновлений.

После изменения параметров задач обновления новые значения не применяются немедленно в выполняющихся задачах обновления. Настроенные параметры вступят в силу только при последующем запуске задач.

► *Чтобы указать тип источника обновлений, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В блоке **Источник обновлений** выберите тип источника обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5:

   - **Сервер администрирования Kaspersky Security Center**

     Kaspersky Industrial CyberSecurity for Nodes 2.5 использует в качестве источника обновления Сервер администрирования Kaspersky Security Center.

     Вы можете выбрать этот вариант, если в вашей сети управление программами "Лаборатории Касперского" выполняется с помощью системы удаленного управления Kaspersky Security Center и на защищаемом компьютере установлен Агент администрирования – компонент Kaspersky Security Center, обеспечивающий связь компьютеров с Сервером администрирования.

   - **Серверы обновлений "Лаборатории Касперского"**

     Kaspersky Industrial CyberSecurity for Nodes 2.5 использует в качестве источника обновлений интернет-сайты "Лаборатории Касперского", на которых публикуются обновления баз и программных модулей для всех программ "Лаборатории Касперского".

     Данный вариант выбран по умолчанию.

   - **Другие HTTP-,FTP-серверы и сетевые ресурсы**

     Kaspersky Industrial CyberSecurity for Nodes использует в качестве источника обновлений указанные администратором HTTP- или FTP-серверы, папки на компьютерах локальной сети.

     Вы можете сформировать список источников, которые содержат актуальный набор обновлений, нажав на ссылку **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

5. Если требуется, настройте дополнительные параметры для пользовательских источников обновления:

   a. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

      i. В открывшемся окне **Серверы обновлений** установите или снимите флажки рядом с пользовательскими источниками обновлений, чтобы начать или прекратить их использование.

      ii. Нажмите на кнопку **OK**.

   b. В блоке **Источник обновлений** на закладке **Общие** установите или снимите флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны** устанавливаете флажок.

      Флажок включает или выключает функцию использования серверов обновлений "Лаборатории Касперского" в качестве источника обновлений, если выбранные вами источники обновлений недоступны.

      Если флажок установлен, функция активна.

      По умолчанию флажок установлен.

      Вы можете установить флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**, когда выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

6. В окне **Параметры задачи** выберите закладку **Параметры соединения**, чтобы настроить параметры соединения с источником обновлений:

   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.

     Флажок включает / выключает использование параметров прокси-сервера, если обновление производится с серверов "Лаборатории Касперского" или установлен флажок Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны.

     Если флажок установлен, параметры прокси-сервера используются.

     Если флажок снят, параметры прокси-сервера не используются.

     По умолчанию флажок снят.

   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

     Флажок включает или выключает использование параметров прокси-сервера, если в качестве источника обновлений выбран вариант Другие HTTP-, FTP-серверы или сетевые ресурсы.

     Если флажок установлен, параметры прокси-сервера используются.

     По умолчанию флажок снят.

7. Нажмите на кнопку **OK**.

Настроенные параметры источника обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5 будут сохранены и применены при последующем запуске задачи.

Вы можете управлять списком пользовательских источников обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5.

► *Чтобы отредактировать список пользовательских источников обновлений программы, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

   Откроется окно **Серверы обновлений**.
5. Выполните следующие действия:
   - Чтобы добавить новый пользовательский источник обновления, в поле ввода укажите адрес папки с файлами обновлений на FTP- или HTTP-сервере; укажите локальную или сетевую папку в формате UNC (Universal Naming Convention). Нажмите на клавишу **ENTER**.

     По умолчанию добавленная папка используется в качестве источника обновлений.
   - Чтобы отключить использование пользовательского источника, снимите флажок рядом с источником в списке.
   - Чтобы включить использование пользовательского источника, установите флажок рядом с источником в списке.
   - Чтобы изменить очередность обращения Kaspersky Industrial CyberSecurity for Nodes 2.5 к пользовательским источникам, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, раньше или позже вы хотите его использовать.
   - Чтобы изменить путь к пользовательскому источнику, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **ENTER**.
   - Чтобы удалить пользовательский источник, выберите его в списке и нажмите на кнопку **Удалить**.

     Вы не можете удалить единственный пользовательский источник из списка.
6. Нажмите на кнопку **OK**.

Изменения в списке пользовательских источников обновления программы будут сохранены.

Оптимизация использования дисковой подсистемы при выполнении задачи Обновление баз программы

При выполнении задачи Обновление баз программы Kaspersky Industrial CyberSecurity for Nodes 2.5 размещает файлы обновлений на локальном диске компьютера. Вы можете снизить нагрузку на дисковую подсистему компьютера за счет размещения файлов обновлений на виртуальном диске в оперативной памяти в процессе выполнения задачи обновления.

Эта функция доступна для Microsoft Windows Vista®, Microsoft Windows Server 2008 и более поздних версиях операционных систем.

При использовании этой функции во время выполнения задачи Обновление баз программы в операционной системе может появиться дополнительный логический диск. Этот логический диск исчезает из операционной системы после завершения задачи.

► *Чтобы снизить нагрузку на дисковую подсистему компьютера при выполнении задачи Обновление баз программы, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление баз программы**.
3. В панели результатов узла **Обновление баз программы** перейдите по ссылке **Свойства**.
4. Откроется окно **Параметры задачи** на закладке **Общие**.
5. В блоке Оптимизация использования дисковой подсистемы настройте следующие параметры:
   - Снимите или установите флажок **Снизить нагрузку на дисковую подсистему**.

     Флажок включает или выключает функцию оптимизации дисковой подсистемы за счет размещения файлов обновления на виртуальном диске в оперативной памяти.

     Если флажок установлен, функция активна.

     По умолчанию флажок снят.
   - В поле **Объем оперативной памяти, используемый для оптимизации**, 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 512 МБ. Минимально допустимый объем оперативной памяти 400 МБ.
6. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Копирование обновлений

► *Чтобы настроить параметры задачи Копирование обновлений, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Обновление**.
2. Выберите вложенный узел **Копирование обновлений**.
3. В панели результатов узла **Копирование обновлений** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 231).

5. На закладке **Общие** в блоке **Параметры копирования обновлений** выполните следующие действия:
   - Укажите условия копирования обновлений программы:
     - **Копировать обновления баз программы**.

       Kaspersky Industrial CyberSecurity for Nodes загружает только обновления баз Kaspersky Industrial CyberSecurity for Nodes.

       Данный вариант выбран по умолчанию.
     - **Копировать критические обновления модулей программы**.

       Kaspersky Industrial CyberSecurity for Nodes 2.5 загружает только срочные обновления программных модулей Kaspersky Industrial CyberSecurity for Nodes 2.5.
     - **Копировать обновления баз программы и критические обновления модулей программы**.

       Kaspersky Industrial CyberSecurity for Nodes 2.5 загружает обновления баз и срочные обновления программных модулей Kaspersky Industrial CyberSecurity for Nodes 2.5.
   - Укажите локальную или сетевую папку, в которую Kaspersky Industrial CyberSecurity for Nodes 2.5 будет копировать полученные обновления.
6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 62).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуск задачи" на стр. 65).
8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Обновление модулей программы

► *Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление модулей программы**.
3. В панели результатов узла **Обновление модулей программы** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Настройка соединения** настройте параметры работы с источниками обновлений (см. раздел "Настройка параметров работы с источниками обновлений Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 231).
5. На закладке **Общие** в блоке **Параметры обновления** настройте параметры обновления модулей программы:
   - **Только проверять наличие доступных критических обновлений модулей программы.**

     Kaspersky Industrial CyberSecurity for Nodes выполняет уведомление об имеющихся на источнике срочных обновлениях программных модулей без скачивания обновлений. Уведомление производится, если оповещение о событиях этого типа настроено.

     Этот вариант выбран по умолчанию.

- **Копировать и устанавливать критические обновления модулей программы.**

  Kaspersky Industrial CyberSecurity for Nodes 2.5 копирует и устанавливает срочные обновления программных модулей.

- **Разрешать перезагрузку компьютера.**

  Перезагрузка операционной системы после установки обновлений, требующих перезагрузки.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes выполняет перезагрузку операционной системы после установки обновлений, требующих перезагрузки.

  Флажок активен, если выбран вариант **Копировать и устанавливать критические обновления модулей программы**.

  По умолчанию флажок снят.

- **Получать информацию о доступных плановых обновлениях модулей программы**

  Получение уведомлений обо всех имеющихся на источнике плановых обновлений программных модулях Kaspersky Industrial CyberSecurity for Nodes. Kaspersky Industrial CyberSecurity for Nodes выполняет уведомления в том случае, если настроено оповещение о событиях этого типа.

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes выполняет уведомление обо всех имеющихся на источнике плановых обновлениях программных модулей.

  По умолчанию флажок установлен.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 62). По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого компьютера).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 65).
8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете сами загружать их с веб-сайта "Лаборатории Касперского". Вы можете настроить уведомление администратора о событии *Доступно плановое обновление модулей программы*, в котором будет содержаться адрес страницы веб-сайта, с которой вы можете загрузить плановые обновления.

Откат обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5.

Перед применением обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5 создает резервные копии баз, которые использовались ранее. Если обновление прервалось или завершилось с ошибкой, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически возвращается к использованию баз с ранее установленными обновлениями.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу Откат обновления баз.

► *Чтобы запустить задачу Откат обновления баз,*

перейдите по ссылке Запустить в панели результатов узла **Откат обновления баз программы**.

Откат обновления программных модулей

Названия параметров могут отличаться в разных операционных системах Windows.

Перед применением обновления программных модулей Kaspersky Industrial CyberSecurity for Nodes 2.5 создает резервные копии модулей, используемых в текущий момент. Если обновление модулей прервалось или завершилось с ошибкой, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически возвращается к использованию модулей с ранее установленными обновлениями.

Чтобы откатить программные модули, используйте компонент панели управления Microsoft Windows **Установка и удаление программ**.

Статистика задач обновления

Пока выполняется задача обновления, вы можете просматривать в реальном времени информацию об объеме данных, полученных с момента запуска задачи по текущий момент, а также другую информацию о выполнении задачи.

После завершения или остановки задачи эту информацию можно просмотреть в журнале выполнения задачи.

► *Чтобы просмотреть статистику задачи обновления, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче, статистику которой вы хотите просмотреть.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Если вы просматриваете задачу Обновление баз программы или задачу Копирование обновлений, в блоке **Статистика** отображается объем данных, загруженных Kaspersky Industrial CyberSecurity for Nodes 2.5 на текущий момент (**Полученные данные**).

Если вы просматриваете задачу Обновление модулей программы, отображается информация, описанная в следующей таблице.

Таблица 36. Информация о задаче Обновление модулей программы

Поле	Описание
Полученные данные	Общий объем полученных данных
Доступно критических обновлений	Количество критических обновлений, доступных для установки
Доступно плановых обновлений	Количество плановых обновлений, доступных для установки
Ошибок применения обновлений	Если значение этого поля отличается от нуля, обновление не было применено. Вы можете просмотреть название обновления, при применении которого возникла ошибка, в журнале выполнения задачи (см. раздел "Просмотр статистики и информации о задаче Kaspersky Industrial CyberSecurity for Nodes 2.5 в журналах выполнения задач" на стр. 263).

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.

В этом разделе

Изолирование возможно зараженных объектов. Карантин

Этот раздел содержит информацию об изолировании возможно зараженных объектов, то есть о помещении этих объектов на карантин, и настройке параметров карантина.

В этом разделе

Об изолировании возможно зараженных объектов

Kaspersky Industrial CyberSecurity for Nodes 2.5 переносит объекты, которые он признает возможно зараженными, из исходного местоположения на *карантин*. В целях безопасности объекты на карантине хранятся в зашифрованном виде.

Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

► *Чтобы просмотреть объекты на карантине, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.

Информация об объектах, помещенных на карантин, отобразится в панели результатов выбранного узла.

► *Чтобы найти нужный объект в списке объектов на карантине,*

отсортируйте объекты (см. раздел "Сортировка объектов на карантине" на стр. 240) или отфильтруйте их (см. раздел "Фильтрация объектов на карантине" на стр. 240).

Сортировка объектов на карантине

По умолчанию объекты в списке объектов на карантине отсортированы по дате помещения в обратном хронологическом порядке. Чтобы найти нужный объект, вы можете отсортировать объекты по содержимому столбцов с информацией об объектах. Результат сортировки сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 с сохранением в MSC-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать объекты, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты в списке.

Объекты в списке будут отсортированы по выбранному параметру.

Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, вы можете отфильтровать объекты в списке – отобразить только те объекты, которые удовлетворяют заданным вами критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы закроете и снова откроете узел Карантин или если вы закроете Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 с сохранением в MSC-файл и снова откроете ее из этого файла.

► *Чтобы задать один или несколько фильтров, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В контекстном меню названия узла выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

4. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите поле, с которым будет сравниваться значение фильтра.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в списке **Название поля**.
   c. В поле **Значение поля** введите или выберите в списке значение фильтра.
   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите шаги a-d для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

   - 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**.
   - Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
   - Чтобы изменить фильтр, выберите фильтр из списка в окне **Параметры фильтра**. Затем измените нужные значения в полях **Имя поля**, **Оператор** или **Значение поля** и нажмите кнопку **Заменить**.

5. После добавления всех фильтров нажмите на кнопку **Применить**.

Созданные фильтры будут сохранены.

► *Чтобы снова отобразить все объекты в списке объектов на карантине,*

в контекстном меню названия узла **Карантин** выберите пункт **Снять фильтр**.

Проверка объектов на карантине

По умолчанию после каждого обновления баз Kaspersky Industrial CyberSecurity for Nodes 2.5 выполняет системную задачу Проверка объектов на карантине. Параметры задачи приводятся в таблице ниже. Вы не можете изменять параметры задачи Проверка объектов на карантине.

Вы можете настраивать расписание запуска задачи (см. раздел "Настройка параметров расписания запуска задач" на стр. 62), запускать ее вручную, а также изменять права учетной записи (см. раздел "Указание учетной записи для запуска задачи" на стр. 65), под управлением которой запускается задача.

Проверив объекты на карантине после обновления баз, Kaspersky Industrial CyberSecurity for Nodes 2.5 может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Kaspersky Industrial CyberSecurity for Nodes 2.5 может признать зараженными и выполнить над ними действия, предусмотренные параметрами задачи Проверка объектов на карантине: лечить или удалять, если лечение невозможно.

Таблица 37. Параметры задачи Проверка объектов на карантине

Параметр задачи Проверка объектов на карантине	Значение
Область проверки	Папка карантина
Параметры безопасности	Единые для всей области проверки; их значения приводятся в следующей таблице.

Таблица 38. Параметры безопасности в задаче Проверка объектов на карантине

Параметр безопасности	Значение
Проверка объектов	Все объекты области проверки
Оптимизация	Выключено
Действие над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Пропускать
Исключать объекты	Нет
Не обнаруживать	Нет
Останавливать проверку, если длится более (сек.)	Не задано
Не проверять составные объекты размером более (МБ).	Не задано
Альтернативные потоки NTFS	Включена
Загрузочные секторы дисков MBR.	Выключено
Использовать технологию iChecker	Выключено
Использовать технологию iSwift	Выключено
Проверять составные объекты.	• Архивы* • SFX-архивы* • упакованные объекты* • Вложенные OLE-объекты* * Проверка только новых и измененных файлов выключена.
Проверка подписи Microsoft у файлов	Не выполняется
Использовать эвристический анализатор	Включено с уровнем анализа **Глубокий**
доверенная зона;	Не применяется

Восстановление содержимого карантина

Kaspersky Industrial CyberSecurity for Nodes 2.5 помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемый компьютер от их возможного вредоносного действия.

Вы можете восстановить любой объект из карантина. Это может потребоваться в следующих случаях:

- если после проверки карантина с применением обновленных баз статус объекта изменился на **Ложное срабатывание** или **Вылечен**;
- если вы считаете объект безопасным для компьютера и хотите его использовать. Чтобы Kaspersky Industrial CyberSecurity for Nodes 2.5 не изолировал этот объект при последующих проверках, вы можете исключить объект из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите объект в качестве значения параметра безопасности **Исключать файлы** (по имени файла) или **Не обнаруживать** в этих задачах либо добавьте его в Доверенную зону (см. раздел "Настройка Доверенной зоны" на стр. 53).

При восстановлении объекта вы можете выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановления на защищаемом компьютере или в указанной вами папке на компьютере, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, или на другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом компьютере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами карантина.

Восстановление объектов из карантина может привести к заражению компьютера.

Вы можете восстановить объект, сохранив его копию в папке карантина, чтобы использовать ее в дальнейшем, например, чтобы еще раз проверить объект после обновления баз.

Если объект, помещенный на карантин, входит в составной объект (например, в архив), Kaspersky Industrial CyberSecurity for Nodes 2.5 не включает его снова в составной объект при восстановлении, а сохраняет отдельно, в указанной папке.

Вы можете восстановить один или несколько объектов.

► *Чтобы восстановить объекты из карантина, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. В панели результатов узла **Карантин** 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 клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на одном из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.
4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект. (Название файла отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке выбранных).

   Выполните одно из следующих действий:
   - чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**;
   - чтобы восстановить объект в папке, которую вы задали в качестве папки для восстановления, в параметрах выберите **Восстановить в папку, используемую по умолчанию**.
   - чтобы сохранить объект в другой папке на компьютере, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, или в сетевую папку, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

5. Если вы хотите сохранить копию объекта в папке карантина после его восстановления, снимите флажок **Удалить объекты из хранилища после восстановления**.
6. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное вами местоположение: если вы выбрали **Восстановить в исходную папку**, каждый из объектов будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе** – все объекты будут сохранены в одну указанную папку.
7. Нажмите на кнопку **OK**.

   Kaspersky Industrial CyberSecurity for Nodes начнет восстанавливать первый из выбранных вами объектов.
8. 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 сохранить восстановленный объект вместо существующего;
      - **Переименовать**, чтобы сохранить восстановленный объект под другим именем. В поле ввода введите новое имя файла объекта и полный путь к нему;
      - **Переименовать, добавив суффикс**, чтобы переименовать 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 **Заменить** или **Переименовать**, добавив суффикс к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. (Если вы установили значение **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен).

   c. Нажмите на кнопку **OK**.

   Файл будет восстановлен. Информация об операции используемую будет зарегистрирована в журнале системного аудита.

   Если вы не выбрали вариант **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В нем вы можете указать местоположение, в которое будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Помещение объектов на карантин

Вы можете вручную помещать файлы на карантин.

► *Чтобы поместить файл на карантин, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню названия узла **Карантин**.
2. Выберите пункт **Добавить**.
3. В окне **Открыть** укажите файл, который вы хотите поместить на карантин.
4. Нажмите на кнопку **OK**.

   Kaspersky Industrial CyberSecurity for Nodes 2.5 поместит указанный файл на карантин.

Удаление объектов с карантина

Согласно параметрам задачи Проверка объектов на карантине, Kaspersky Industrial CyberSecurity for Nodes 2.5 автоматически удаляет из папки карантина объекты, статус которых при проверке карантина с использованием обновленных баз изменился на *Зараженный* и которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 не смогла вылечить. Остальные объекты Kaspersky Industrial CyberSecurity for Nodes 2.5 не удаляет.

Вы можете вручную удалить из карантина один или несколько объектов.

► *Чтобы удалить из карантина один или несколько объектов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. Выполните одно из следующих действий:
   - чтобы удалить один объект, в контекстно меню названия объекта выберите пункт **Удалить**.
   - чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на любом из выбранных объектов и выберите пункт **Удалить.**
4. В открывшемся окне нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные объекты будут удалены из карантина.

Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"

Если поведение какого-нибудь файла дает вам основание подозревать в нем наличие угрозы, а Kaspersky Industrial CyberSecurity for Nodes 2.5 признает этот файл незараженным, то, возможно, вы встретились с новой, неизвестной угрозой, описание которой еще не добавлено в базы. Вы можете отправить этот файл на исследование в "Лабораторию Касперского". Вирусные аналитики "Лаборатории Касперского" проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись и алгоритм лечения в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Industrial CyberSecurity for Nodes 2.5 признает его зараженным и сможет его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы из карантина. Файлы, находящиеся на карантине, хранятся в зашифрованном виде и при пересылке не удаляются антивирусной программой, установленной на почтовом сервере.

Вы не можете отправлять объекты из карантина на исследование в "Лабораторию Касперского" после окончания срока действия лицензии.

► *Чтобы отправить файл на исследование в "Лабораторию Касперского", выполните следующие действия:*

1. Если файл не находится на карантине, предварительно **поместите его на карантин**.
2. В узле **Карантин**, в списке объектов на карантине, откройте контекстное меню файла, который вы хотите отправить на исследование в "Лабораторию Касперского", и выберите пункт **Отправить объект на исследование**.
3. В открывшемся окне подтверждения операции нажмите на кнопку **Да**, если действительно хотите отправить выбранный объект на исследование.
4. Если на компьютере, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, настроен почтовый клиент, будет создано новое сообщение электронной почты. Просмотрите его, а затем нажмите на кнопку **Отправить**.

   Поле **Получатель** сообщения содержит адрес электронной почты "Лаборатории Касперского" newvirus@kaspersky.com. Поле Тема содержит текст "Объект карантина".

   Текст сообщения содержит следующую информацию: "Этот файл будет отправлен на анализ в "Лабораторию Касперского". В тело сообщения вы можете включить любую дополнительную информацию о файле: почему он показался вам возможно зараженным или опасным, как он себя ведет или как влияет на систему.

   В сообщение вложен архив <имя объекта>.cab. Он содержит файл <uuid>.klq с зашифрованным объектом (где uuid – уникальный идентификатор объекта в Kaspersky Industrial CyberSecurity for Nodes 2.5), файл <uuid>.txt с информацией, полученной Kaspersky Industrial CyberSecurity for Nodes 2.5 об объекте, а также файл Sysinfo.txt, который содержит следующую информацию о Kaspersky Industrial CyberSecurity for Nodes 2.5 и операционной системе на компьютере:

   - название и версию операционной системы;
   - название и версию Kaspersky Industrial CyberSecurity for Nodes 2.5;
   - дата выпуска последних установленных обновлений баз;
   - номер активного ключа.

   Эта информация нужна вирусным аналитикам "Лаборатории Касперского", чтобы быстрее и эффективнее проанализировать файл. Однако если вы не хотите передавать ее, вы можете удалить файл Sysinfo.txt из архива.

Если почтовый клиент не установлен на компьютере, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, программа предложит сохранить выбранный зашифрованный объект в файл. Этот файл вы можете переслать в "Лабораторию Касперского" самостоятельно.

► *Чтобы сохранить зашифрованный объект в файл, выполните следующие действия:*

1. В открывшемся окне с приглашением сохранить объект нажмите на кнопку **Да**.
2. Выберите папку на диске защищаемого компьютера или сетевую папку, в которую вы хотите сохранить файл с объектом.

Объект будет сохранен в файл формата CAB.

Настройка параметров карантина

Вы можете настраивать параметры карантина. Новые параметры карантина применяются сразу после сохранения.

► *Чтобы настроить параметры карантина, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Откройте контекстное меню названия вложенного узла **Карантин**.
3. Выберите пункт **Свойства**.
4. В окне **Параметры карантина** настройте нужные параметры карантина в соответствии с вашими требованиями:
   - В блоке **Параметры карантина**:
     - **Папка карантина**

       Путь к папке карантина в формате UNC (Universal Naming Convention).

       По умолчанию установлен путь C:\ProgramData\Kaspersky Industrial CyberSecurity for Nodes\2.5\Quarantine\.

     - **Максимальный размер карантина**

       Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в карантине. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует событие Превышен максимальный размер карантина и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

       Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 отслеживает суммарный размер размещенных в карантине объектов.

       Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не отслеживает суммарный размер объектов в карантине.

       По умолчанию флажок снят.

     - **Порог доступного пространства.**

       Флажок включает или выключает отслеживание минимального размера свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует 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 2.5 отслеживает размер свободного места в резервном хранилище.

       Флажок Порог доступного пространства (МБ) активен, если установлен флажок Максимальный размер резервного хранилища (МБ).

       По умолчанию флажок установлен.

     Если объем объектов на карантине превышает значение максимального размера карантина или превышает порог доступного пространства, Kaspersky Industrial CyberSecurity for Nodes 2.5 уведомит вас об этом, не переставая помещать объекты на карантин.

   - В блоке **Параметры восстановления объектов**:
     - **Папка, в которую восстанавливаются объекты.**
5. Нажмите на кнопку **ОК**.

Настроенные параметры карантина будут сохранены.

Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – статистику карантина.

► *Чтобы просмотреть статистику карантина,*

в контекстном меню названия узла **Карантин** в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите пункт **Статистика**.

В окне **Статистика** отображается информация о количестве объектов на карантине в текущий момент (см. таблицу ниже):

Поле	Описание
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Industrial CyberSecurity for Nodes 2.5 признала возможно зараженными.
Текущий размер карантина	Общий объем данных в папке карантина.
Ложных срабатываний	Количество объектов, которые получили статус *Ложное срабатывание*, так как при проверке карантина с применением обновленных баз были признаны незараженными.
Вылечено объектов	Количество объектов, которые после проверки карантина получили статус *Вылеченный*.
Всего объектов	Общее количество объектов на карантине.

Резервное копирование объектов. Резервное хранилище

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также инструкции по настройке параметров резервного хранилища.

В этом разделе

О резервном копировании объектов перед лечением или удалением

Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет зашифрованные копии объектов со статусами *зараженный* или *возможно зараженный* в *резервное хранилище* перед тем, как выполнить лечение или удаление этих объектов.

Если объект является частью составного объекта (например, входит в архив), Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Industrial CyberSecurity for Nodes 2.5 признал зараженным один из объектов в составе почтовой базы, он сохраняет копию всей почтовой базы.

Если объект, который Kaspersky Industrial CyberSecurity for Nodes 2.5 копирует в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске вашего компьютера.

Вы можете восстанавливать файлы из резервного хранилища, как в исходную папку, так и в другую папку на защищаемом компьютере или другом компьютере в локальной сети организации. Вы можете восстановить файл из резервного хранилища, например, если исходный зараженный или возможно зараженный файл содержал важную информацию, но при лечении этого файла программа Kaspersky Industrial CyberSecurity for Nodes 2.5 не смогла сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению компьютера.

Просмотр объектов в резервном хранилище

Вы можете просматривать объекты в папке резервного хранилища только через Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, в узле **Резервное хранилище**. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

► *Чтобы просмотреть объекты в резервном хранилище,*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

Информация об объектах, помещенных в резервное хранилище, отобразится в панели результатов выбранного узла.

► *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 сохранения в обратном хронологическом порядке. Чтобы найти нужный файл, вы можете отсортировать файлы по содержимому любой графы в панели результатов.

Результат сортировки сохранится, если вы закроете и снова откроете узел Резервное хранилище или если вы закроете Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 с сохранением в MSC-файл и снова откроете ее из этого файла.

► *Чтобы отсортировать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. В списке файлов в **резервном хранилище** 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 – отобразить в узле **Резервное хранилище** только те файлы, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

Результат фильтрации сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5 с сохранением в MSC-файл и снова откроете ее из этого файла.

► *Чтобы отфильтровать файлы в резервном хранилище, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

2. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите поле, со значениями которого будет сравниваться указанное вами значение фильтра при отборе.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут быть различными в зависимости от того, какое значение вы выберите в поле **Название поля**.

   c. В поле **Значение поля** введите или выберите значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

   - 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**.

- Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы отредактировать фильтр, выберите его в списке фильтров в окне **Параметры фильтра**, измените нужные значения в полях **Название поля**, **Оператор** или **Значение поля** и нажмите на кнопку **Заменить**.

После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке отобразятся только файлы, отобранные согласно заданным фильтрам.

► *Чтобы снова отобразить все файлы в списке файлов в резервном хранилище,*

в контекстном меню узла **Резервное хранилище** выберите пункт **Снять фильтр**.

Восстановление файлов из резервного хранилища

Kaspersky Industrial CyberSecurity for Nodes 2.5 хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемый компьютер от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный файл, который оказался зараженным, содержал важную информацию, при лечении файла программа Kaspersky Industrial CyberSecurity for Nodes 2.5 не смогла сохранить его целостность, и в результате информация в файле стала недоступной;
- если вы считаете файл безопасным для компьютера и хотите его использовать. Чтобы Kaspersky Industrial CyberSecurity for Nodes 2.5 не признавал файл зараженным или возможно зараженным при последующих проверках, вы можете исключить его из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите файл в качестве параметра **Исключать файлы** или **Не обнаруживать** этих задач.

Восстановление файлов из резервного хранилища может привести к заражению компьютера.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходную папку (по умолчанию), в специальную папку для восстановленных объектов на защищаемом компьютере или в указанную вами папку на компьютере, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, или на другом компьютере в сети.

Папка для восстановления предназначена для хранения восстановленных объектов на защищаемом компьютере. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами резервного хранилища (см. раздел "Настройка параметров резервного хранилища" на стр. 253).

По умолчанию, когда Kaspersky Industrial CyberSecurity for Nodes 2.5 восстанавливает файл, он сохраняет его копию в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

3. 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 клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню на одном из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.

4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект. (Название файла отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке выбранных).

   Выполните одно из следующих действий:

   - чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**;
   - чтобы восстановить объект в папке, которую вы задали в качестве папки для восстановления, в параметрах выберите **Восстановить в папку, используемую по умолчанию**.
   - чтобы сохранить объект в другой папке на компьютере, на котором установлена Консоль Kaspersky Industrial CyberSecurity for Nodes 2.5, или в сетевую папку, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, 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 **Удалять 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**.

   Все выбранные объекты будут восстановлены и сохранены в указанное вами местоположение: если вы выбрали **Восстановить в исходную папку**, каждый из объектов будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе** – все объекты будут сохранены в одну указанную папку.

7. Нажмите на кнопку **OK**.

   Kaspersky Industrial CyberSecurity for Nodes начнет восстанавливать первый из выбранных вами объектов.

8. 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 сохранить восстановленный объект вместо существующего;
      - **Переименовать**, чтобы сохранить восстановленный объект под другим именем. В поле ввода введите новое имя файла объекта и полный путь к нему;
      - **Переименовать, добавив суффикс**, чтобы переименовать 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 **Заменить** или **Переименовать**, добавив суффикс к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. (Если вы установили значение **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен).

c. Нажмите на кнопку **OK**.

Файл будет восстановлен. Информация об операции используемую будет зарегистрирована в журнале системного аудита.

Если вы не выбрали вариант **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В нем вы можете указать местоположение, в которое будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Удаление файлов из резервного хранилища

► *Чтобы удалить из резервного хранилища один или несколько файлов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. Выполните одно из следующих действий:
   - чтобы удалить один объект, в контекстно меню названия объекта выберите пункт **Удалить**.
   - **чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавишу** Ctrl **или клавишу** Shift**, затем откройте контекстное меню на любом из выбранных объектов и выберите пункт** Удалить.
4. **В открывшемся окне нажмите на кнопку** Да, чтобы подтвердить операцию.

Выбранные файлы будут удалены из резервного хранилища.

Настройка параметров резервного хранилища

► *Чтобы настроить параметры резервного хранилища, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Откройте контекстное меню названия вложенного узла **Резервное хранилище**.
3. Выберите пункт **Свойства**.
4. В окне **Свойства резервного хранилища** настройте нужные параметры резервного хранилища в соответствии с вашими требованиями:

   В блоке **Параметры резервного хранилища**:

   - **Папка резервного хранилища.**

     Путь к папке резервного хранилища в формате UNC (Universal Naming Convention).

     По умолчанию установлен путь C:\ProgramData\Kaspersky Industrial CyberSecurity for Nodes\2.5\Backup\.

   - **Максимальный размер хранилища (МБ)**

Флажок включает или выключает функцию, которая отслеживает суммарный размер объектов, размещенных в папке резервного хранилища. В случае превышения заданного значения (по умолчанию 200 МБ) Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует событие Превышен максимальный размер резервного хранилища и выполняет уведомление в соответствии с параметрами уведомлений о событиях данного типа.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 отслеживает суммарный размер размещенных в резервном хранилище объектов.

Если флажок снят, Kaspersky Industrial CyberSecurity for Nodes 2.5 не отслеживает суммарный размер объектов в резервном хранилище.

По умолчанию флажок снят.

- **Порог доступного пространства (МБ).**

  Флажок включает или выключает отслеживание минимального размера свободного места в резервном хранилище (по умолчанию 50 МБ). Если размер свободного места становится меньше установленного, Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует 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 2.5 отслеживает размер свободного места в резервном хранилище.

  Флажок Порог доступного пространства (МБ) активен, если установлен флажок Максимальный размер резервного хранилища (МБ).

  По умолчанию флажок установлен.

Если объем объектов в резервном хранилище превышает значение максимального размера резервного хранилища или превышает порог доступного пространства, Kaspersky Industrial CyberSecurity for Nodes 2.5 уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

В блоке **Параметры восстановления объектов**:

- **Папка, в которую восстанавливаются объекты.**

  Путь к папке, в которую восстанавливаются объекты в формате UNC (Universal Naming Convention).

  Путь по умолчанию: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\2.5\Restored\.

5. Нажмите на кнопку **OK**.

Настроенные параметры резервного хранилища будут сохранены.

Статистика резервного хранилища

Вы можете просматривать информацию о состоянии резервного хранилища в текущий момент: статистику резервного хранилища.

► *Чтобы просмотреть статистику резервного хранилища,*

в контекстном меню названия узла **Резервное хранилище** в дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 выберите пункт **Статистика**. Откроется окно **Статистика резервного хранилища**.

В окне **Статистика резервного хранилища** отображается информация о состоянии резервного хранилища в текущий момент (см. таблицу ниже).

Таблица 39. 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

Блокирование доступа к сетевым файловым ресурсам. Заблокированные узлы

В этом разделе описано, как заблокировать недоверенные компьютеры и настроить параметры хранилища заблокированных компьютеров.

В этом разделе

О блокировании доступа к сетевым файловым ресурсам

Хранилище заблокированных узлов устанавливается по умолчанию, если установлен любой из следующих компонентов: Постоянная защита файлов, Защита от шифрования. Задачи отслеживают попытки удаленных компьютеров получить доступ к общим сетевым папкам защищаемого компьютера или сетевого хранилища в соответствии со списком недоверенных компьютеров. Информация обо всех недоверенных компьютерах со всех защищаемых компьютеров отправляется в Kaspersky Security Center. Kaspersky Industrial CyberSecurity for Nodes 2.5 блокирует доступ к общим сетевым папкам компьютера или общим папкам сетевого хранилища для всех узлов в хранилище заблокированных узлов.

Хранилище заблокированных узлов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Если в ходе выполнения задачи Постоянная защита файлов со стороны компьютера, обращающегося к сетевым файловым ресурсам, выявлена вредоносная активность и в параметрах задачи Постоянная защита файлов установлен флажок **Вносить компьютеры, с которых ведется вредоносная активность, в список недоверенных.**
- Если в ходе выполнения задачи Защита от шифрования со стороны компьютера, обращающегося к сетевым файловым ресурсам, выявлена активность вредоносного шифрования.

После обнаружения вредоносной активности или попытки шифрования задача отправляет информацию об атакующем узле в хранилище заблокированных узлов, и программа создает критическое событие блокировки узла. Любые попытки данного узла получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет недоверенные компьютеры из хранилища через 30 минут после добавления. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка недоверенных. Вы можете указать период, после которого заблокированные узлы автоматически разблокируются.

Обратите внимание, что в случае наложения запрета доступа к управлению хранилищами какому-либо пользователю, хранилище Заблокированных узлов останется доступным. Настройки хранилища Заблокированных узлов не могут быть изменены только если пользователь не имеет **прав на изменение** для управления Kaspersky Industrial CyberSecurity for Nodes 2.5.

Включение блокирования доступа к сетевым файловым ресурсам

Чтобы добавить компьютеры, проявляющие вредоносную активность или попытки шифрования, в хранилище заблокированных узлов и заблокировать этим компьютерам доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов.
- Защита от шифрования

► *Чтобы настроить задачу Постоянная защита файлов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В блоке **Интеграция с другими компонентами** установите флажок **Вносить компьютеры, с которых ведется вредоносная активность, в список недоверенных**, если вы хотите, чтобы программа Kaspersky Industrial CyberSecurity for Nodes 2.5 блокировала доступ к сетевым файловым ресурсам для компьютеров, со стороны которых в ходе работы задачи Постоянная защита файлов обнаружена вредоносная активность.
5. Если задача не была запущена, откройте закладку **Расписание**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В выпадающем списке выберите частоту запуска **При запуске задачи**.
6. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

► *Чтобы настроить задачу Защита от шифрования, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от шифрования**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Если задача не была запущена, откройте закладку **Расписание**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В выпадающем списке выберите частоту запуска **При запуске задачи**.
5. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Настройка параметров хранилища заблокированных узлов

► *Чтобы настроить хранилище заблокированных узлов, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Заблокированные узлы**.
3. Выберите пункт меню **Свойства**.

   Откроется окно **Параметры хранилища заблокированных узлов**.
4. Откроется окно Параметры хранилища заблокированных узлов.
5. Нажмите на кнопку **ОК**.
6. Чтобы восстановить доступ для всех заблокированных узлов, выполните следующие действия:
   a. Откройте контекстное меню вложенного узла **Заблокированные узлы**.
   b. Выберите пункт **Разблокировать все**.

      Все узлы будут удалены из списка и разблокированы.
7. Чтобы удалить несколько узлов из списка заблокированных, выполните следующие действия:
   a. Выберите один или несколько узлов в списке недоверенных в панели результатов.
   b. Откройте контекстное меню вложенного узла **Заблокированные узлы**.
   c. Выберите пункт **Разблокировать выбранные**.

      Выбранные узлы будут разблокированы.

Запись событий. Журналы Kaspersky Industrial CyberSecurity for Nodes 2.5

Этот раздел содержит информацию о работе с журналами Kaspersky Industrial CyberSecurity for Nodes 2.5: журналом системного аудита, журналами выполнения задач и журналом событий.

В этом разделе

Способы записи событий Kaspersky Industrial CyberSecurity for Nodes 2.5

События Kaspersky Industrial CyberSecurity for Nodes 2.5 делятся на две группы:

- события, связанные с обработкой объектов в задачах Kaspersky Industrial CyberSecurity for Nodes 2.5;
- события, связанные с управлением Kaspersky Industrial CyberSecurity for Nodes 2.5, например: запуск программы, создание или удаление задач, запуск задач, изменение параметров задач.

Kaspersky Industrial CyberSecurity for Nodes 2.5 использует следующие способы для записи событий:

- **Журналы выполнения задач**. Журнал выполнения задачи содержит информацию о параметрах задачи, текущем состоянии задачи и событиях, возникших за время ее выполнения.
- **Журнал системного аудита**. Журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Industrial CyberSecurity for Nodes 2.5.
- **Журнал событий**. Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Industrial CyberSecurity for Nodes 2.5. Журнал событий доступен в Просмотре событий Microsoft Windows.
- **Журнал безопасности**. Журнал безопасности содержит информацию о событиях, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом компьютере.

Если в работе Kaspersky Industrial CyberSecurity for Nodes 2.5 возникла проблема (например, Kaspersky Industrial CyberSecurity for Nodes 2.5 или отдельная задача завершается аварийно) и вы хотите диагностировать ее, вы можете создать файл трассировки и файл дампа Kaspersky Industrial CyberSecurity for Nodes 2.5 и отправить файлы с этой информацией на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Industrial CyberSecurity for Nodes 2.5 не отправляет файлы трассировки и дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Industrial CyberSecurity for Nodes 2.5 записывает информацию в файлы трассировки и дампа в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Industrial CyberSecurity for Nodes 2.5. Вы можете настроить права доступа (см. раздел "Права доступа к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5" на стр. 43) и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

Журнал системного аудита

Kaspersky Industrial CyberSecurity for Nodes 2.5 ведет системный аудит событий, связанных с управлением Kaspersky Industrial CyberSecurity for Nodes 2.5. Программа сохраняет информацию, например, о запуске программы, запуске и остановке задач Kaspersky Industrial CyberSecurity for Nodes 2.5, изменении параметров задач, создании и удалении задач проверки по требованию. Записи об этих событиях отображаются в панели результатов при выборе узла **Журнал системного аудита** в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете указать папку, в которой Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

Сортировка событий в журнале системного аудита

По умолчанию события отображаются в журнале системного аудита в обратном хронологическом порядке.

Вы можете отсортировать события по содержимому любой графы, кроме графы **Событие**.

► *Чтобы отсортировать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журнал системного аудита**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в списке событий.

Результат сортировки сохранится до следующего просмотра журнала системного аудита.

Фильтрация событий в журнале системного аудита

Вы можете отобразить в журнале системного аудита записи только о тех событиях, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журнале системного аудита, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой выполняется фильтрация событий.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от пункта, 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 **Параметры фильтра**.
4. Если требуется, выполните одно из следующих действий:
   - Если вы хотите объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Если вы хотите объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в журнале системного аудита.

   В списке событий журнала системного аудита отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журнала системного аудита.

► *Чтобы отключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Снять фильтр**.

   В списке событий журнала системного аудита отобразятся все события.

Удаление событий из журнала системного аудита

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете вручную удалить все события из журнала системного аудита.

► *Чтобы удалить события из журнала системного аудита, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Очистить**.
3. Выполните одно из следующих действий:
   - Если вы хотите перед удалением событий из журнала системного аудита сохранить содержимое журнала в файл в формате CSV или TXT, в окне подтверждения удаления нажмите на кнопку **Да**. В открывшемся окне укажите имя и местоположение файла.
   - Если вы не хотите сохранить содержимое журнала в файл, в окне подтверждения удаления нажмите на кнопку **Нет**.

Журнал системного аудита будет очищен.

Журналы выполнения задач

Этот раздел содержит информацию о журналах выполнения задач Kaspersky Industrial CyberSecurity for Nodes 2.5 и инструкции по работе с ними.

В этом разделе

О журналах выполнения задач

Информация о выполнении задач Kaspersky Industrial CyberSecurity for Nodes 2.5 отображается в панели результатов при выборе узла **Журналы выполнения задач** в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5.

В журнале выполнения каждой задачи вы можете просмотреть статистику выполнения задачи, информацию о каждом объекте, который был обработан программой с момента запуска задачи по текущий момент, а также параметры задачи.

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете указать папку, в которой Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет файлы журналов выполнения задач, отличную от папки, установленной по умолчанию. Также вы можете выбрать события, записи о которых Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в журналах выполнения задач.

Просмотр списка событий в журналах выполнения задач

► *Чтобы просмотреть список событий в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.

   Список событий, сохраненных в журналах выполнения задач Kaspersky Industrial CyberSecurity for Nodes 2.5, отобразится в панели результатов.

Вы можете отсортировать события по содержимому любой графы или применить фильтр.

Сортировка событий в журналах выполнения задач

По умолчанию события отображаются в журналах выполнения задач в обратном хронологическом порядке. Вы можете отсортировать события по содержимому любой графы.

► *Чтобы отсортировать события в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в журналах выполнения задач Kaspersky Industrial CyberSecurity for Nodes 2.5.

Результат сортировки сохранится до следующего просмотра журналов выполнения задач.

Фильтрация событий в журналах выполнения задач

Вы можете отобразить в списке событий журналов выполнения задач только записи о тех событиях, которые удовлетворяют заданным вами условиям фильтрации (фильтрам).

► *Чтобы отфильтровать события в журналах выполнения задач, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой выполняется фильтрация событий.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от пункта, 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 **Параметры фильтра**.
4. Если требуется, выполните одно из следующих действий:
   - Если вы хотите объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Если вы хотите объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в списке событий журналов выполнения задач.

В списке событий журналов выполнения задач отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журналов выполнения задач.

► *Чтобы отключить действие фильтра, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Снять фильтр**.

В списке событий журналов выполнения задач отобразятся все события.

Просмотр статистики и информации о задачах Kaspersky Industrial CyberSecurity for Nodes 2.5 в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска по текущий момент, а также статистику выполнения задач и параметры задач.

► *Чтобы просмотреть статистику и информацию о задаче Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
   - двойным щелчком мыши на событии, которое возникло в задаче, журнал которой вы хотите просмотреть;
   - откройте контекстное меню события, которое возникло в задаче, журнал которой вы хотите просмотреть, и выберите пункт **Просмотреть журнал**.

4. В открывшемся окне отображается следующая информация:
   - на закладке **Статистика** отображается время запуска и завершения задачи и ее статистика;
   - на закладке **События** отображается список событий, зафиксированных при выполнении задачи;
   - на закладке **Параметры** отображаются параметры задачи.
5. Если требуется, нажмите на кнопку **Фильтр**, чтобы отфильтровать события в журнале выполнения задачи.
6. Если требуется, нажмите на кнопку **Экспорт**, чтобы экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.
7. Нажмите на кнопку **Закрыть**.

Окно **Журнал выполнения** будет закрыто.

Экспорт информации из журнала выполнения задачи

Вы можете экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

► *Чтобы экспортировать информацию из журнала выполнения задачи, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:
   - двойным щелчком мыши на событии, которое возникло в задаче, журнал которой вы хотите просмотреть;
   - откройте контекстное меню события, которое возникло в задаче, журнал которой вы хотите просмотреть, и выберите пункт **Просмотреть журнал**.
4. В нижней части окна **Журнал выполнения нажмите на кнопку** Экспорт.

   Откроется окно **Сохранить как**.
5. Укажите имя, местоположение, тип и кодировку файла, в который вы хотите экспортировать информацию из журнала выполнения задачи.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

Удаление событий из журналов выполнения задач

По умолчанию Kaspersky Industrial CyberSecurity for Nodes 2.5 хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете вручную удалить все события из журналов выполнения задач, завершившихся на данный момент.

События из журналов задач, выполняющих в данный момент и журналов, используемых другими пользователями, удалены не будут.

► *Чтобы удалить события из журналов выполнения задач, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. Выполните одно из следующих действий:
   - Если вы хотите удалить события из всех журналов выполнения задач, завершившихся на данный момент, откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Очистить**.
   - Если вы хотите очистить журнал выполнения отдельной задачи, в панели результатов откройте контекстное меню события, которое возникло в задаче, журнал выполнения которой вы хотите очистить, и выберите пункт **Удалить**.
   - Если вы хотите очистить журналы выполнения нескольких задач, выполните следующие действия:
     a. В панели результатов с помощью клавишей **Ctrl** или **Shift**, выберите события, которые возникли в задачах, журналы выполнения которых вы хотите очистить.
     b. Откройте контекстное меню любого выбранного события и выберите пункт **Удалить**.
4. В окне подтверждения удаления нажмите на кнопку **Да**, чтобы подтвердить удаление.

Выбранные журналы выполнения задач будут очищены. Удаление событий из журналов выполнения задач будет зарегистрировано в журнале системного аудита.

Журнал безопасности

Kaspersky Industrial CyberSecurity for Nodes 2.5 ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом компьютере. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач постоянной защиты компьютера и проверки по требованию, задач Мониторинг файловых операций, Контроль запуска программ и Контроль устройств).

Вы можете очистить журнал безопасности, так же как и журнал системного аудита (см. раздел "Удаление событий из журнала системного аудита" на стр. 260). При этом Kaspersky Industrial CyberSecurity for Nodes 2.5 фиксирует событие системного аудита об очистке журнала безопасности.

Просмотр журнала событий Kaspersky Industrial CyberSecurity for Nodes 2.5 в оснастке "Просмотр событий"

С помощью оснастки Просмотр событий для Microsoft Management Console вы можете просматривать журнал событий Kaspersky Industrial CyberSecurity for Nodes 2.5. В нем Kaspersky Industrial CyberSecurity for Nodes 2.5 регистрирует события, которые нужны для диагностики сбоев в работе Kaspersky Industrial CyberSecurity for Nodes 2.5.

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 события всех уровней важности; наименее подробным является уровень Критические события, при котором регистрируются только критические события. По умолчанию для всех компонентов кроме компонента Обновление установлен уровень детализации Важные события (регистрируются только важные и критические события); для компонента Обновление установлен уровень Информационные события.

► *Чтобы просмотреть журнал событий Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

   Откроется окно 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 компьютер, на котором установлена программа Kaspersky Industrial CyberSecurity for Nodes 2.5, и нажмите кнопку **ОК**.

5. В окне **Добавление и удаление оснасток** нажмите на кнопку **ОК**.

   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 2.5.**

Откроется журнал событий Kaspersky Industrial CyberSecurity for Nodes 2.5.

Настройка параметров журналов в Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5

Вы можете настраивать следующие параметры журналов Kaspersky Industrial CyberSecurity for Nodes 2.5:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита.

- местоположение папки, в которой Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет файлы журналов выполнения задач и журнала системного аудита;
- пороги формирования событий *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей компьютера давно не выполнялась*.
- события, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Industrial CyberSecurity for Nodes 2.5 в оснастке Просмотр событий.
- параметры публикации событий аудита и событий выполнения задач по протоколу syslog на syslog-сервер.

► *Чтобы настроить параметры журналов Kaspersky Industrial CyberSecurity for Nodes 2.5, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. В окне **Параметры журналов и уведомлений** настройте параметры журналов в соответствии с вашими требованиями. Для этого выполните следующие действия:

   - На закладке **Общие**, если требуется, выберите события, которые Kaspersky Industrial CyberSecurity for Nodes 2.5 сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Industrial CyberSecurity for Nodes 2.5 в оснастке Просмотр событий. Для этого выполните следующие действия:

     - В списке **Компонент** выберите функциональный компонент Kaspersky Industrial CyberSecurity for Nodes 2.5, уровень детализации событий которого вы хотите указать.

     > Для компонентов Постоянная защита файлов, проверки по требованию и обновления предусмотрена запись событий в журналы выполнения задач и журнал событий. Для этих компонентов таблица списка событий содержит графы **Журналы** и **Журнал событий**. Для компонентов Карантин и Резервное хранилище события записываются в журнал системного аудита и журнал событий. Для этих компонентов таблица списка событий содержит графы **Аудит** и **Журнал событий**.

     - В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного функционального компонента.

       В таблице списка событий ниже установлены флажки рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.

     - Если вы хотите вручную включить запись отдельных событий для выбранного функционального компонента, выполните следующие действия:

     a. В списке **Уровень важности** выберите **Другой**.

     b. В таблице списка событий установите флажки рядом с теми событиями, запись которых в журналы выполнения задач, журнал системного аудита и журнал событий вы хотите включить.

   - На закладке **Дополнительно** настройте параметры хранения журналов и пороги формирования событий о статусе защиты компьютера:

     - В блоке **Хранение журналов**:

- **Папка журналов**

  Путь к папке с журналами в формате UNC (Universal Naming Convention).

  Путь по умолчанию: Путь по умолчанию: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Reports\.

- **Удалять журналы выполнения задач и событий старше чем (дни)**

  Флажок включает / выключает функцию, которая удаляет журналы с результатами выполнения завершенных задач и события, опубликованные в журналах выполняющихся задач, по истечении заданного периода (по умолчанию, 30 дней).

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет журналы о результатах выполнения завершенных задач и события, опубликованные в журналах выполняющихся задач, по истечении заданного периода.

  По умолчанию флажок установлен.

- **Удалять события журнала аудита старше чем (дни)**

  Флажок включает / выключает функцию, которая удаляет события, зарегистрированные в журнале аудита, по истечении заданного периода (по умолчанию, 60 дней).

  Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes 2.5 удаляет события, зарегистрированные в журнале аудита, по истечении заданного периода.

  По умолчанию флажок установлен.

- В блоке **Пороги формирования событий**:
  - количество дней, после которого будут возникать события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей компьютера давно не выполнялась*;.

Таблица 40. Пороги формирования событий

Параметр	Пороги формирования событий.
Описание	Вы можете указать пороги формирования событий следующих трех типов: Базы программы устарели и Базы программы сильно устарели. Событие возникает, если базы Kaspersky Industrial CyberSecurity for Nodes 2.5 не обновляются в течение указанного параметром количества дней с момента создания последних установленных обновлений баз. Вы можете настроить уведомление администратора по этим событиям. Проверка важных областей давно не выполнялась. Событие возникает, если в течение указанного количества дней не выполняется ни одна из задач, отмеченных флажком Считать выполнение задачи проверкой важных областей.
Возможные значения	Количество дней от 1 до 365.
Значение по умолчанию	Базы программы устарели – 7 дней; Базы программы сильно устарели – 14 дней; Проверка важных областей давно не выполнялась – 30 дней.

- На закладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач (см. раздел "Настройка параметров интеграции с SIEM" на стр. 269) на syslog-сервере.

3. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Об интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и снизить риск деградации системы в результате увеличения объемов журналов программы, вы можете настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он собирает и анализирует полученные события, а также выполняет другие действия в рамках управления журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: этот режим предполагает, что все события выполнения задач, публикация которых настроенная в параметрах журналов, а также все события системного аудита продолжают храниться на локальном компьютере даже после отправки в SIEM.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемый компьютер.

- Удалять локальные копии событий: этот режим предполагает, что все события, зарегистрированные в ходе работы программы и опубликованные в SIEM, будут удалены с локального компьютера.

  Программа никогда не удаляет локальные версии журнала нарушений безопасности

Kaspersky Industrial CyberSecurity for Nodes 2.5 может конвертировать события в журналах программы в форматы, поддерживаемые syslog-компьютером, для передачи событий и их успешного распознавания на стороне SIEM. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Рекомендуется выбирать формат событий на основе конфигурации используемой SIEM.

Параметры надежности

Вы можете снизить риск неудачной отправки событий в SIEM задав параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если подключение к основному syslog-серверу или его использование недоступны.

Также Kaspersky Industrial CyberSecurity for Nodes 2.5 уведомляет вас о неудачной попытке подключения к SIEM и об ошибках отправки событий в SIEM с помощью событий системного аудита.

Настройка параметров интеграции с SIEM

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и отключать интеграцию с SIEM, а также настраивать параметры функциональности (см. таблицу ниже).

Таблица 41. Параметры интеграции с SIEM

Параметр	Значение по умолчанию	Описание
Отправлять события по протоколу syslog на внешний syslog-сервер	Не применяется	Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.
Удалять локальные копии событий при записи на внешний syslog-сервер	Не применяется	Вы можете настраивать параметры хранения локальных копий журналов, после их отправки в SIEM с помощью установки или снятия флажка.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует свои события перед их отправкой на syslog-сервер для лучшего распознавания этих событий на стороне SIEM.
Протокол подключения	TCP	Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UPD или TCP с помощью выпадающего списка.
Параметры подключения к основному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.
Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен	Не применяется	Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.
Параметры подключения к дополнительному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

► *Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.
3. Выберите закладку **Интеграция с SIEM**.

4. В блоке **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

   Флажок включает или отключает использование функциональности отправки публикуемых событий на внешний syslog-сервер.

   Если флажок установлен, программа выполняет отправку публикуемых событий в SIEM в соответствии с настроенными параметрами интеграции с SIEM.

   Если флажок снят, программа не выполняет интеграцию с SIEM. Вы не можете настраивать параметры интеграции SIEM, если флажок снят.

   По умолчанию флажок снят.

5. Если требуется, в блоке **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

   Флажок включает или отключает удаление локальных копий журналов по их отправке в SIEM.

   Если флажок установлен, программа удаляет локальные копии событий после того, как они были успешно опубликованы в SIEM. Рекомендуется использовать этот режим на маломощных компьютерах.

   Если флажок снят, программа только отправляет события в SIEM. Копии журналов продолжают храниться локально.

   По умолчанию флажок снят.

> Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

6. В блоке **Формат событий** укажите формат, в который вы хотите конвертировать события по работе программы для их отправки в SIEM.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

7. В блоке **Параметры соединения**:

   - Укажите протокол подключения к SIEM.
   - Укажите параметры соединения с основным syslog-сервером.

     Вы можете указать IP-адрес только в формате IPv4.

   - Если требуется, установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер недоступна.

     - Укажите параметры подключения к зеркальному syslog-серверу. **IP-адрес** и **Порт**.

       Поля **IP-адрес** и **Порт** для зеркального syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

       Вы можете указать IP-адрес только в формате IPv4.

8. Нажмите на кнопку **OK**.

   Настроенные параметры интеграции с SIEM будут применены.

Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Industrial CyberSecurity for Nodes 2.5 о событиях программы и состоянии защиты компьютера, а также инструкцию по настройке уведомлений.

В этом разделе

Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому компьютеру, о событиях, связанных с работой Kaspersky Industrial CyberSecurity for Nodes 2.5 и состоянием антивирусной защиты компьютера.

Программа обеспечивает выполнение следующих задач:

- администратор может получать информацию о событиях выбранных типов;
- пользователи локальной сети, которые обращаются к защищаемому компьютеру, и терминальные пользователи компьютера могут получать информацию о событиях типа *Обнаружен объект*, возникших в задаче Постоянная защита файлов.

В Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 вы можете активировать уведомления администратора или пользователей несколькими способами:

- Способы уведомления пользователей:
  a. Средства службы терминалов.

     Вы можете применять этот способ для оповещения терминальных пользователей, если защищаемый компьютер является терминальным.

  b. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.
- Способы уведомления администраторов:
  a. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.

  b. Запуск исполняемого файла.

     Этот способ запускает по событию исполняемый файл, который хранится на локальном диске защищаемого компьютера.

  c. Отправка по электронной почте.

     Этот способ использует для передачи сообщений электронную почту.

Вы можете создавать текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется предустановленный текст сообщений.

Настройка уведомлений администратора и пользователей

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений, а также составление текста сообщения.

► *Чтобы настроить уведомления о событиях, выполните следующие действия:*

1. В дереве Консоли Kaspersky Industrial CyberSecurity for Nodes 2.5 откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. На закладке **Уведомления** укажите способы уведомлений:

   a. В списке **Тип события** выберите событие, для которого вы хотите выбрать способ уведомления.

   b. В группе параметров **Уведомление администраторов** или **Уведомление пользователей** установите флажок рядом со способами уведомлений, которые вы хотите использовать.

   > Вы можете настроить уведомления пользователей только для события **Обнаружен объект**.

3. Если вы хотите составить текст сообщения, выполните следующие действия:

   a. Нажмите на кнопку **Текст сообщения**.

   b. В открывшемся окне введите текст, который будет отображаться в сообщении о событии.

   > Вы можете составить один текст сообщения для нескольких типов событий: после того как вы выбрали способ уведомлений для одного типа событий, выберите, используя клавишу **Ctrl** или клавишу **Shift**, остальные типы событий, для которых вы хотите составить такой же текст сообщения, перед тем как нажать на кнопку **Текст сообщения**.

   c. Чтобы добавить поля с информацией о событии, нажмите на кнопку **Макрос** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   d. Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

4. Если вы хотите настроить параметры для способов уведомлений администраторов о выбранном событии, в окне **Уведомления** нажмите на кнопку **Настройка** и в окне **Дополнительные параметры** выполните настройку выбранных способов. Для этого выполните следующие действия:

   a. Для уведомлений по электронной почте откройте закладку **Электронная почта** и в соответствующих полях укажите адреса электронной почты получателей (разделяйте адреса символом "точка с запятой"), имя или сетевой адрес SMTP-сервера, а также его порт. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** вы также можете включать переменные с информацией о событии (см. таблицу ниже).

      Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, в группе **Параметры аутентификации** установите флажок **Использовать SMTP-аутентификацию** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

b. Для уведомлений средствами **службы сообщений** на закладке **Служба сообщений**, составьте список компьютеров-получателей уведомлений: для каждого компьютера, который вы хотите добавить, нажмите на кнопку **Добавить** и в поле ввода введите его сетевое имя.

c. Для запуска исполняемого файла на закладке **Исполняемый файл** выберите на локальном диске защищаемого компьютера файл, который будет выполняться на компьютере по событию, или введите полный путь к нему. 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.

   Если вы хотите ограничить количество уведомлений по событиям одного типа в единицу времени, на закладке **Дополнительно** установите флажок **Не отправлять одно и то же уведомление чаще** и укажите нужное количество раз и единицу времени.

5. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

Таблица 42. 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 обнаруженного объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Industrial CyberSecurity for Nodes 2.5 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 2.5 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 компьютера пользователя, который обратился к объекту на компьютере.
%USER_NAME%	В задаче Постоянная защита файлов имя пользователя, который обратился к объекту на компьютере.
%FROM_COMPUTER%	Имя защищаемого компьютера, с которого поступило уведомление.
%EVENT_REASON%	Причина возникновения события (некоторые события не имеют этого поля).
%ERROR_CODE%	Код ошибки (применяется только для события "внутренняя ошибка задачи").
%TASK_NAME%	Имя задачи (имеется только у событий, связанных с выполнением задач).

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В программе Kaspersky Security Center, находящейся в открытом сегменте сети, настроить задачу загрузки обновлений в хранилище.
2. Убедиться в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые машины с установленными программами, базы для которых необходимо обновить.
3. Запустить задачу. В процессе загрузки обновлений с открытых серверов «Лаборатории Касперского» Kaspersky Security Center проведет проверку контроля целостности обновлений, прежде чем добавит их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.

Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления с указанием перенесенного хранилища как источника обновлений. При загрузке обновлений из хранилища, программы еще раз проведут контроль целостности загружаемых обновлений.

Если вам недоступны серверы обновлений "Лаборатории Касперского" (например, нет доступа к интернету), обратитесь в Службу технической поддержки "Лаборатории Касперского" для получения обновлений программы на дисках.

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (http://www.bdu.fstec.ru, https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- На форуме "Лаборатории Касперского" (https://forum.kaspersky.com).

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 279).

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону.
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем защиты компьютеров от угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, “Лаборатория Касперского” – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей (“IDC Endpoint Tracker 2014).

"Лаборатория Касперского" основана в России в 1997 году. Сегодня “Лаборатория Касперского” – это международная группа компаний с 38 офисами в 33 стране мира. В компании работает более 3 000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: среди них Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu и ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, “Лаборатория Касперского” стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей, а количество организаций, являющихся ее клиентами, превышает 270 000.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru
Вирусная лаборатория:	https://newvirus.kaspersky.ru/ (для проверки подозрительных файлов и веб-сайтов)
Веб-форум "Лаборатории Касперского":	https://forum.kaspersky.ru

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Internet Explorer, Excel, Outlook, Windows, Windows Server и Windows Vista – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 43. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
операционная система, промышленная инфраструктура, промышленная сеть	среда функционирования
защищаемый компьютер	объект воздействия
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь
уведомления пользователей и администратора	сигналы тревоги

Глоссарий

K

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе данных "Лаборатории Касперского" с постоянно обновляемой информацией о репутации файлов, интернет-ресурсов и программного обеспечения. Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

O

OLE-объект

Объект, прикрепленный к другому файлу или вложенный в другой файл путем использования технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft Office Excel®, встроенная в документ Microsoft Office Word.

S

SIEM

Технология, которая обеспечивает анализ событий безопасности, исходящих от различных сетевых устройств и приложений.

A

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать вредоносный код в проверяемых объектах. Антивирусные базы создаются специалистами "Лаборатории Касперского" и обновляются каждый час.

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

З

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка компьютера и Обновление баз программы.

Зараженный объект

Объект, часть кода которого полностью совпадает с частью кода известной вредоносной программы. "Лаборатория Касперского" не рекомендует обрабатывать такие объекты.

К

Карантин

Папка, в которую программа "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Локальная задача

Задача, определенная и работающая на отдельном клиентском компьютере.

М

Маска файла

Представление имени файла с помощью специальных символов. Стандартными специальными символами, используемыми в масках файлов, являются * и ?, где * представляет любое количество символов, а ? представляет любой отдельный символ.

О

Обновление

Процедура замены/добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Объекты автозапуска

Набор программ, необходимых для запуска и правильной работы операционной системы и установленного на компьютере программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

П

Параметры задачи

Параметры программы, специфические для каждого типа задач.

Подозрительный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный "Лаборатории Касперского". Подозрительные объекты обнаруживаются с помощью эвристического анализатора.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на устройствах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект (на чтение, запись и исполнение) и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы, или возможно зараженные объекты обрабатываются в соответствии с параметрами задачи (лечатся, удаляются или помещаются на карантин).

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe и dll. Риск проникновения вредоносного кода в такие файлы весьма высок.

Р

Резервное хранилище:

Специальное хранилище для резервных копий файлов, которые создаются перед попыткой дезинфекции или удаления.

С

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Его также можно использовать для управления этими программами.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Срок действия лицензии

Период, в течение которого у вас есть доступ к функциям программы и право использовать дополнительные службы. Службы, которые вы можете использовать, зависят от типа лицензии.

У

Уровень безопасности

Уровень безопасности представляет собой предварительно заданный набор параметров компонентов программы.

Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют четыре уровня важности:

- Критическое событие.
- Ошибка.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

Э

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы "Лаборатории Касперского". Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

Приложение. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированном конфигурации на другие значения, выводит программу из безопасного состояния.

Таблица 44. Параметры и их безопасные значения для программы в сертифицированной конфигурации

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Параметры установки		
Компонент Управление сетевым экраном	Выбор компонентов для установки на защищаемый компьютер.	Не установлен (по умолчанию)
Компонент Контроль устройств	Выбор компонентов для установки на защищаемый компьютер.	Не установлен (флажок снят)
Компонент Постоянная защита	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Компонент Контроль запуска программ	Выбор компонентов для установки на защищаемый компьютер.	Установлен (по умолчанию)
Настройки прав доступа и функциональных компонентов		
Служба Kaspersky Security	Основная служба Kaspersky Security; управляет задачами и рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 2.5. • **Запущена** • **Остановлена**	Запущена
Права на управление программой	Доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5: • **Разрешить** • **Запретить**	Учетные записи пользователей- администраторов безопасности должны быть добавлены в группу KICS Administrators. Для всех пользователей и групп, кроме KICS Administrators и SYSTEM, установлены флажки **Запретить**.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Служба Kaspersky Security	Основная служба Kaspersky Security; управляет задачами и рабочими процессами Kaspersky Industrial CyberSecurity for Nodes 2.5. • **Запущена** • **Остановлена**	Запущена
Права на управление программой	Доступ к функциям Kaspersky Industrial CyberSecurity for Nodes 2.5: • **Разрешить** • **Запретить**	Учетные записи пользователей - администраторов безопасности должны быть добавлены в группу KICS Administrators. Для всех пользователей и групп, кроме KICS Administrators и SYSTEM, установлены флажки **Запретить**.
Права на управление службой	Доступ к функциям службы Kaspersky Security: • **Разрешить** • **Запретить**	Учетные записи пользователей – администраторов безопасности должны быть добавлены в группу KICS Administrators. Для всех пользователей и групп, кроме KICS Administrators и SYSTEM, установлены флажки **Запретить**.
Задача Постоянная защита файлов	Антивирусная проверка файлов на защищаемом сервере при обращении к этим файлам. • **Выполняется** • **Остановлена**	Выполняется
Лицензирование	Активация программы с помощью ключа.	Добавлен файл ключа. По окончании срока действия ключа программа выходит из сертифицированного состояния.
Использовать Локальный KSN	Взаимодействие с Глобальным или Локальным KSN, настраеваемое в Kaspersky Security Center.	Запускать задачу Использование KSN следует только при использовании Локального KSN (флажок **Настроить Локальный KSN** установлен), в том числе при отсутствии управления программой через Kaspersky Security Center.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Параметры задач Постоянная защита / проверка по требованию		
Архивы	Проверка архивов в указанной области защиты в параметрах задачи Постоянной защиты файлов. • **Применяется** (флажок установлен). • **Не применяется** (флажок снят).	Применяется (флажок установлен).
Загрузочные секторы дисков и MBR	Проверять загрузочные секторы и загрузочные надписи на жестких и съемных дисках сервера. • **Применяется** (флажок установлен). • **Не применяется** (флажок снят).	Применяется (флажок установлен).
Область защиты	Папки и файлы находящиеся под защитой задач Постоянная защита и Проверка по требованию. • Любые локальные и сетевые папки.	По умолчанию. Исключение папок из области защиты, установленной по умолчанию, ведет к выходу из сертифицируемого состояния.
Пропускать для любого типа объектов	Действия при обнаружении объектов: • **Лечить** • **Удалять** • **Помещать на карантин** • **Пропускать**	Не выбрано. При выборе действия **Пропускать** для любого типа объектов, программа выходит из сертифицированного состояния.
Объекты, проверяемые по указанному списку расширений	На закладке **Общие**, выберите объекты, которые необходимо защищать: • **Все объекты** • **Объекты, проверяемые по формату** • **Объекты, проверяемые по списку расширений, указанному в антивирусных базах** • **Объекты, проверяемые по указанному списку расширений**	Флажок снят. Наполнение списка расширений объектов вручную ведет к выходу программы из сертифицированного состояния.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Исключать файлы	Исключение файлов из проверки по имени файла или маске имени файла: • Применяется (флажок установлен). • Не применяется (флажок снят).	Не применяется (Флажок снят).
Не обнаруживать	Исключение обнаруживаемых объектов из проверки по имени или маске имени обнаруживаемого объекта: • Применяется (флажок установлен). • Не применяется (флажок снят).	Не применяется (Флажок снят).
Использовать эвристический анализатор	Применение эвристического анализатора: • Применяется (флажок установлен). • Не применяется (флажок снят).	Применяется (флажок установлен). Снятие флажка ведет к выходу программы из сертифицированного состояния.
Параметры задач обновления		
Серверы обновлений «Лаборатории Касперского» на компьютере-ретрансляторе (Задача Копирование обновлений)	Источник обновлений баз программы: • **Сервер администрирования Kaspersky Security Center.** • **Серверы обновлений «Лаборатории Касперского».** • **Другие HTTP-, FTP-серверы или сетевые ресурсы.**	На компьютере-ретрансляторе выбран вариант **Серверы обновлений «Лаборатории Касперского»**. Для работы программы в сертифицированной конфигурации, задачи обновления должны осуществляться через один из защищаемых компьютеров сети.
Копировать обновления программы (Задача Копирование обновлений)	Укажите условия копирования обновлений программы: • **Копировать обновления программы.** • **Копировать критические обновления модулей программы.** • **Копировать обновления баз программы и критические обновления модулей программы.**	Выбран вариант **Копировать обновления программы**. Kaspersky Industrial CyberSecurity for Nodes 2.5 загружает только обновления баз Kaspersky Security.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Другие HTTP-, FTP-серверы или сетевые ресурсы на серверах-ресиверах.	Источник обновлений баз программы: • **Сервер администрирования Kaspersky Security Center** • **Серверы обновлений «Лаборатории Касперского»** • **Другие HTTP-, FTP-серверы или сетевые ресурсы**	На серверах-ресиверах выбран вариант **Другие HTTP-, FTP-серверы или сетевые ресурсы**. В качестве источника должна быть указана сетевая папка, настроенная в качестве папки локального источника обновлений в задаче Копирование обновлений на компьютере-ретрансляторе.
Использовать серверы обновлений «Лаборатории Касперского», если серверы, указанные пользователем, недоступны на серверах-ресиверах. (Задача Обновление баз программы)	При выборе источника обновления **Другие HTTP-, FTP-серверы или сетевые ресурсы**, активируется функция использования серверов обновлений «Лаборатории Касперского». • **Применяется** (флажок установлен). • **Не применяется** (флажок снят).	Не применяется (флажок снят). Обновление через сервера обновлений «Лаборатории Касперского» запрещено.
Частота запуска задачи Обновление баз программы	Промежуток времени, через которое задача осуществляет проверку наличия обновлений: • **Ежечасно** • **Ежесуточно** • **Еженедельно** • **При запуске программы** • **После получения обновлений Сервером администрирования**	**Ежечасно** (по умолчанию). Снижение частоты запусков задачи, установленного по умолчанию ведет к выходу программы из сертифицированного состояния.

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Настройка параметров аудита		
События для компонентов постоянной защиты, проверки по требованию, KSN, лицензирования и обновлений баз программы.	Регистрация событий в параметрах журналов. • **Все события** • **Набор событий по умолчанию**	Для компонентов **Постоянная защита**, **Проверка по требованию**, **Использование KSN**, **Лицензирование** и задачи **Обновление баз программы** установлены оповещения о событиях по умолчанию.
Удалять события в журналах выполнения задач старше, чем (сут.)	Очистка журнала выполнения задач через заданный прометужок времени.	**30** сут. (по умолчанию). Уменьшение количества дней хранения событий в журнале ведет к выходу программы из сертифицированного состояния.
Удалять события в журнале системного аудита старше, чем (сут.)	Очистка журнала системного аудита через заданный прометужок времени.	**60** сут. (по умолчанию). Уменьшение количества дней хранения событий в журнале ведет к выходу программы из сертифицированного состояния.
Пороги формирования событий	Промежуток времени, через который возникают события: • **Базы программы устарели.** • **Базы программы сильно устарели.** • **Проверка важных областей компьютера давно не выполнялась**.	По умолчанию выставлены следующие значения: **7** (сут) **14** (сут) **30** (сут) Уменьшение порога формирования событий ведет к выходу программы из сертифицированного состояния.
Настройка сигналов тревоги		
Путем запуска исполняемого файла	Способы уведомления администраторов: • **Средствами службы сообщений**; • **Путем запуска исполняемого файла**; • **По электронной почте**.	Флажок **Путем запуска исполняемого файла** установлен для событий: • *Обнаружен объект* • *Объект не вылечен* • *Объект не удален* • *Запуск программы запрещен* • *Запуск программы запрещен по прецеденту* • *Объект не помещен на карантин* • *Объект не помещен в резервное хранилище*

Название параметра	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Данные сигнала тревоги	Переменные в составе сообщения сигнала тревоги.	Переменные **Тип обнаруженного объекта** (%VIRUS_TYPE%), **Обнаружено** (%VIRUS_NAME%) и **Событие** (%EVENT_TYPE%) присутствуют в сообщении сигнала тревоги.